Citrix DaaS

Contents

Visão geral

November 21, 2023

Introdução

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) oferece virtualização que oferece ao pessoal de TI o controle de máquinas virtuais, aplicativos e segurança, fornecendo também acesso em qualquer lugar para qualquer dispositivo. Os usuários podem usar aplicativos e áreas de trabalho independentemente da interface e do sistema operacional do dispositivo.

Usando o Citrix DaaS, você pode fornecer aplicativos e áreas virtuais seguras para qualquer dispositivo, deixando a maior parte da instalação, configuração e atualizações para a Citrix. Você mantém controle total sobre aplicativos, políticas e usuários, oferecendo a melhor experiência do usuário em qualquer dispositivo.

O Citrix DaaS permite que você gerencie cargas de trabalho de data center local e nuvem pública juntas em uma implantação híbrida. Você pode se conectar a nuvens públicas Microsoft Azure, Amazon Web Services (AWS) e Google Cloud, além de hipervisores locais, como Citrix Hypervisor, Microsoft Hyper-V, Nutanix AHV e VMware vSphere. A abordagem híbrida e multinuvem oferece a flexibilidade de implantar diferentes aplicativos em diferentes locais de recursos em todo o mundo.

O Citrix DaaS oferece várias maneiras de fornecer aplicativos e áreas de trabalho.

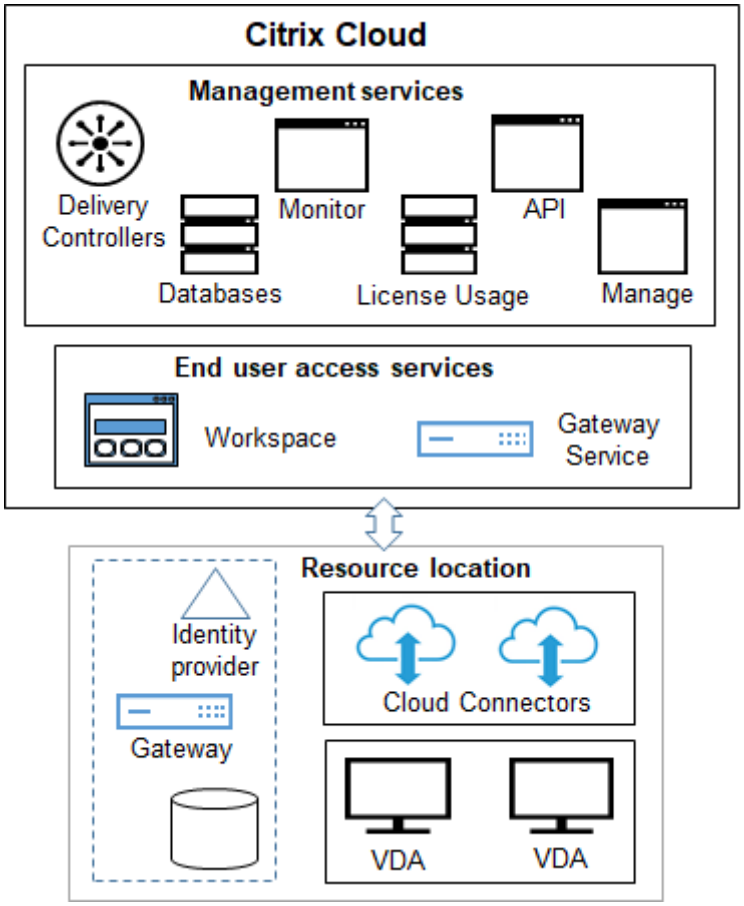
- Métodos de entrega descreve as principais formas, com casos de uso e prós/contras.
- Modelos de entrega lista mais opções e oferece comparações de modelos VDI.

Citrix Managed Azure simplifica ainda mais a implantação de aplicativos e áreas de trabalho virtuais. Com o Citrix Managed Azure, o 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 da Citrix trabalham em uma implantação de produção do Citrix DaaS (também conhecida como site).



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

Componentes e serviços gerenciados pela Citrix

- **Delivery Controllers:** O Citrix DaaS fornece a funcionalidade para balancear a carga de aplicativos e áreas de trabalho, 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:** Os dados de configuração, monitoramento e registro de configuração do site são armazenados pelo serviço de nuvem, eliminando o requisito de banco de dados SQL

do produto Citrix Virtual Apps and Desktops local.

- **Licenciamento:** Gerencia licenças e fornece estatísticas de uso.
- **Interfaces de gerenciamento:** Consulte Interfaces de gerenciamento. Muitas tarefas também estão disponíveis nas APIs de serviço.
- **Interface Monitor:** A interface Monitor permite que as equipes de suporte de TI e help desk monitorem um ambiente, solucionem problemas antes que eles se tornem críticos e executem tarefas de suporte para usuários finais. Os dados exibidos são:
  - Dados de sessão em tempo real do Broker Service no Controlador, que inclui 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. Recomendamos dois ou mais Cloud Connectors para redundância.

  - Quando usar Full Configuration 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 do Azure, a Citrix cria o local do recurso e os Cloud Connectors para você quando você cria um catálogo.

  Depois que os Cloud Connectors são instalados, a Citrix os gerencia e atualiza. As únicas tarefas tratadas pelo cliente são atualizações e patches do Windows do Cloud Connector.

Interfaces de gerenciamento

Na guia **Manage** do Citrix DaaS, você pode selecionar as seguintes interfaces.

Full Configuration

Na interface **Manage > Full Configuration**:

- Obtenha uma visão geral da implantação do Citrix DaaS e dos recursos mais recentes na página inicial.
- Crie e gerencie conexões com hosts.

- Crie e gerencie catálogos de máquinas que contêm aplicativos e áreas de trabalho que você entrega aos usuários.
- Crie e gerencie grupos de entrega e, opcionalmente, grupos de aplicativos.
- Crie e gerencie políticas da Citrix que afetam o uso e o comportamento das tecnologias e recursos HDX, além do gerenciamento no nível do site. Isso inclui configurações de política para sessões, transporte adaptável, dispositivos, gráficos, multimídia, redirecionamento de conteúdo e VDAs.
- Personalize a administração delegada para criar administradores baseados em funções que têm escopos de autoridade específicos.
- Gerencie o recurso de Autoscale para gerenciar proativamente máquinas que fornecem aplicativos e áreas de trabalho.
- Balanceamento da carga das máquinas
- Execute verificações de integridade em seus VDAs para identificar possíveis problemas e corrigir sugestões.
- Exiba o conteúdo do log de configuração para ver quando ocorreram alterações de configuração e outras atividades administrativas e quem as iniciou.

Quick Deploy

Na interface **Manage > Quick Deploy**, você pode implantar e gerenciar facilmente cargas de trabalho do Microsoft Azure que usam uma assinatura do Citrix Managed Azure ou sua própria assinatura do Azure. Para obter mais informações, consulte Quick Deploy e Citrix Managed Azure. No Quick Deploy, você pode:

- Criar e gerenciar catálogos.
- Criar e personalizar imagens, seja de várias imagens preparadas pela Citrix ou de imagens importadas de sua assinatura do Azure.

Para obter mais informações, consulte Quick Deploy.

Environment Management

A partir da interface **Environment Management**, você pode usar o gerenciamento inteligente de recursos e as tecnologias do Profile Management para oferecer o melhor desempenho possível, logon na área de trabalho e ótimos tempos de resposta de aplicativos. Para obter mais informações, consulte Workspace Environment Management.

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 dispositivo virtual Citrix Gateway ou VPX é um dispositivo VPN SSL implantado na DMZ. Ele fornece um único ponto seguro de acesso através do firewall corporativo.

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

- **Active Directory:** O Active Directory é usado para autenticação e autorização. Ele autentica os usuários e garante que tenham 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 compatíveis são: Active Directory local, Active Directory mais token, Azure Active Directory, Citrix Gateway e Okta. Para obter mais informações, consulte:

  - Workspace Identity
  - Identity and access management

- **Virtual Delivery Agents (VDAs):** Cada máquina física ou virtual que fornece recursos (aplicativos e áreas de trabalho) deve ter um Citrix VDA instalado. Os VDAs estabelecem e gerenciam a conexão entre a máquina na qual ele está instalado e o dispositivo do usuário e aplicam políticas configuradas para a sessão.

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

  Estão disponíveis vários tipos de VDA:

  - Os VDAs para sistemas operacionais Windows multissessão permitem que vários usuários se conectem à máquina simultaneamente. Esse tipo de VDA geralmente é instalado em servidores Windows.

  - Os sistemas operacionais de sessão única VDAs para Windows permitem que um usuário se conecte a uma máquina por vez. Esse tipo de VDA geralmente é usado para VDI.

    Uma versão principal desse tipo de VDA está disponível para uso com o recurso Remote PC Access. Ele contém um subconjunto dos recursos no VDA completo de sessão única.

  - Os VDAs do Linux oferecem suporte a aplicativos e áreas de trabalho virtuais com base em uma distribuição RHEL, CentOS, SUSE ou Ubuntu.

  Em toda a documentação deste serviço, “VDA”geralmente se refere ao agente e à máquina na qual ele está instalado.

- **Hipervisores e serviços em nuvem:** Na maioria dos sites de produção, as instâncias do aplicativo e da área de trabalho (cargas de trabalho) que você disponibiliza (publica) para seus usuários são "hospedadas"por um hipervisor ou serviço de nuvem compatível. (O recurso Remote PC Access geralmente é usado com máquinas físicas. Portanto, ele não usa hipervisores ou serviços de nuvem para provisionamento de máquinas.)

  - Usando a interface Full Configuration, você cria uma conexão com um hipervisor de host ou serviço de nuvem compatível. Em seguida, em Full Configuration, você usa uma imagem (criada por meio desse host) para criar um catálogo de máquinas que contêm as instâncias do aplicativo e da área de trabalho. Em seguida, você cria um grupo de entrega. A Citrix fornece muitas ferramentas para simplificar e facilitar a forma como esses hosts de sessão são criados 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 do Citrix Managed Azure também elimina a necessidade de gerenciar o host.

  As instâncias do aplicativo e da área de trabalho que você publica podem ser locais, hospedadas em nuvens públicas ou em uma mistura híbrida de ambas.

- **Citrix StoreFront:** O Citrix StoreFront é o antecessor do Citrix Workspace hospedado na nuvem. Ele é usado como interface da web para acesso a aplicativos e áreas de trabalho.

  Opcionalmente, você pode instalar servidores StoreFront em locais de recursos. Ter lojas locais pode ajudar a fornecer aplicativos e áreas de trabalho durante interrupções de rede. O recurso Local Host Cache requer um StoreFront gerenciado pelo cliente em cada local de recurso.

  Consulte O acesso do usuário para obter considerações sobre o uso do StoreFront em um ambiente de serviço.

Objetos que você configura para fornecer áreas de trabalho e aplicativos

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

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

  - O endereço e as credenciais para acessar o host
  - O método de armazenamento que deve ser usado e as máquinas que devem ser 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 o Citrix Managed Azure, a Citrix também gerencia a hospedagem.

- **Catálogo:** Nas interfaces Full Configuration e Monitor, os catálogos são chamados de "machine catalogs"(catálogos de máquinas).
  Um catálogo é uma coleção de máquinas virtuais ou físicas que têm o mesmo tipo de sistema operacional (por exemplo, multissessão do Windows, sessão única do Ubuntu).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **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 áreas de trabalho que os usuários podem acessar por meio do Workspace.

  Ao usar o Quick Deploy, um grupo de entrega é criado automaticamente. (Ele aparece somente na interface Full Configuration.)

- **Grupo de aplicativos:** Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos que são compartilhados entre diferentes grupos de entrega ou usados por um subconjunto de usuários dentro de grupos de entrega. Os grupos de aplicativos são opcionais.

Citrix Managed Azure

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

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

- Implantar máquinas de sistema operacional Windows de sessão única e de várias sessões ou máquinas com sistema operacional Linux, a partir de várias versões suportadas.
- Escolha em uma lista selecionada de tipos de computação e opções de armazenamento em regiões selecionadas.
- Provisione cargas de trabalho persistentes ou não persistentes nessas máquinas.
- Escolha entre várias imagens fornecidas pela Citrix que tenham o VDA mais recente instalado. Então, a partir da interface da 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.

Mesmo que a Citrix gerencie a capacidade do Azure, se você quiser se comunicar com os recursos existentes em sua própria assinatura do Azure, poderá usar o emparelhamento VNet do Azure para conectar recursos. Você também pode usar o Citrix SD-WAN para se conectar diretamente aos seus recursos locais.

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

Como pedir o Citrix Managed Azure

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

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

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

Resumo dos benefícios do Citrix Managed Azure

O uso do Citrix Managed Azure oferece vários benefícios:

- O caminho mais rápido para os benefícios da nuvem híbrida.
- Descarrega o gerenciamento de TI da infraestrutura. Oferece uma experiência de administração que coloca a TI no controle sem os desafios de gerenciamento e manutenção.
- Permite que você dimensione 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 de 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 verdadeiro modelo de Infraestrutura como Serviço (IaaS) baseado em consumo.
- Várias tecnologias estão disponíveis para criar conexões com suas próprias redes locais (como o emparelhamento do Azure VNet e a SD-WAN). Isso permite que os usuários acessem os recursos da 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 da Citrix.

Entrega de aplicativos e áreas de trabalho aos usuários

Citrix Workspace

Os assinantes (usuários) acessam suas áreas de trabalho e aplicativos por meio do Citrix Workspace.

Depois de instalar e configurar o Citrix DaaS, você receberá o link do URL de um espaço de trabalho. O URL do espaço de trabalho é publicado em dois locais:

- No console do Citrix Cloud, selecione **Workspace Configuration** no menu no canto superior esquerdo. A guia **Access** contém a URL do Workspace.
- Na página **Welcome** do Citrix DaaS, o URL do espaço de trabalho aparece na parte inferior da página.

Teste e compartilhe o link de URL da área de trabalho com seus assinantes (usuários) para dar a eles acesso aos aplicativos e áreas de trabalho. Seus assinantes podem acessar o URL do espaço de trabalho sem nenhuma configuração adicional.

Você configura espaços de trabalho do Citrix Cloud.

- Especifique quais serviços estão integrados ao Citrix Workspace.
- Personalize o URL que seus assinantes usam para acessar o espaço de trabalho.
- Personalize a aparência dos espaços de trabalho dos assinantes, como logotipos, cores e preferências.

- Especifique como os assinantes se autenticam em seu espaço de trabalho, como, por exemplo, por meio o Active Directory ou do Azure Active Directory.
- Especifique a conectividade externa para locais de recursos usados por seus assinantes.

Para obter mais informações, consulte Citrix Workspace.

Aplicativo Citrix Workspace

Do lado do usuário, o aplicativo Citrix Workspace é instalado em dispositivos do usuário e outros pontos de extremidade, como áreas de trabalho virtuais. O aplicativo Citrix Workspace fornece aos usuários acesso seguro e de autoatendimento a documentos, aplicativos e áreas de trabalho 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 por meio 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.

Contrato de nível de serviço

O Citrix DaaS foi concebido usando as melhores práticas do setor para alcançar a escala da nuvem e um alto grau de disponibilidade de serviço.

Para obter detalhes completos sobre o compromisso da Citrix com a disponibilidade dos serviços do Citrix Cloud, consulte o Contrato de nível de serviço.

O desempenho contra esse objetivo pode ser monitorado continuamente em https://status.cloud.com.

Limitações

O cálculo dessa Meta de Nível de Serviço não incluirá a perda de disponibilidade das seguintes causas:

- Falha do cliente em seguir os requisitos de configuração do Citrix DaaS documentados na documentação do produto em https://docs.citrix.com.
- Causado por qualquer componente não gerenciado pela Citrix, incluindo, sem limitação, máquinas físicas e virtuais controladas pelo cliente, sistemas operacionais instalados e mantidos pelo cliente, equipamentos de rede instalados e controlados pelo cliente ou outro

hardware; configurações de segurança definidas e controladas pelo cliente, grupo políticas e outras políticas de configuração; falhas do provedor de nuvem pública, falhas do provedor de serviços de Internet ou outras externas ao controle Citrix.
- Interrupção do serviço devido a razões além do controle da Citrix, incluindo desastres naturais, guerra ou atos de terrorismo, atuação do governo.

Mais informações

- Diagramas do Citrix DaaS
- Arquitetura de referência e métodos de implantação do Citrix DaaS
- Visão técnica geral da segurança
- Portas de rede
- Notas para terceiros
- Requisitos do sistema
- Recursos
  - Uma introdução às tecnologias HDX, além de detalhes sobre dispositivos, gráficos e multimídia.
  - Remote PC Access: permitir que os usuários façam logon remotamente de qualquer lugar para um PC físico no escritório. Você pode configurar Remote PC Access a partir da Full Configuration ou da Quick Deploy.
  - Publish content: publique um aplicativo que seja simplesmente um URL ou caminho UNC para um recurso.
  - Server VDI: forneça uma área de trabalho a partir de um sistema operacional de servidor para um único usuário.
- Para o Citrix DaaS Standard para Azure, consulte a documentação exclusiva do produto.
- Para saber mais sobre a disponibilidade de recursos nos produtos e edições do Citrix DaaS, consulte a matriz de recursos do Citrix DaaS.
- A Citrix Cloud Learning Series oferece um curso educacional para você começar a trabalhar com o Citrix Cloud e seus serviços. Você pode visualizar sequencialmente todos os módulos, desde apresentações até serviços de planejamento e construção. Você também pode escolher módulos separadamente ou segmentos específicos de tarefas dentro de um módulo. Veja a Cloud Learning Series.

Introdução

Para saber como configurar sua implantação, comece com Plan and build a deployment. Esse resumo o orienta pelas principais etapas do processo e fornece links para mais informações e procedimentos detalhados.

Novidades

December 20, 2023

A Citrix tem como meta entregar novos recursos e atualizações do produto aos clientes do Citrix DaaS quando disponíveis. As novas versões fornecem mais valor, portanto, não há motivo para esperar quando as atualizações lançadas. As atualizações contínuas do Citrix DaaS são lançadas aproximadamente a cada três semanas.

Esse processo é transparente para você. As atualizações iniciais são aplicadas somente nos sites internos da Citrix e depois são aplicadas gradualmente aos ambientes do cliente. O fornecimento de atualizações de forma incremental, em lotes, ajuda a garantir a qualidade do produto e a maximizar a disponibilidade.

Para obter detalhes sobre o Acordo de Nível de Serviço para dimensionamento de nuvem e disponibilidade de serviço, consulte Acordo de Nível de Serviço. Para monitorar interrupções de serviço e manutenção programada, consulte o Service Health Dashboard.

Virtual Delivery Agents (VDAs)

Os VDAs para computadores Windows geralmente são lançados simultaneamente com o produto Citrix Virtual Apps and Desktops.

- Para obter informações sobre novos recursos de VDA e HDX, consulte os artigos Novidades e Problemas conhecidos da versão atual do Citrix Virtual Apps and Desktops.
- Para obter informações sobre plataformas e recursos de VDA que não são mais suportados, consulte Substituição. Esse artigo também inclui plataformas e recursos que perderam o suporte em uma versão futura (como os sistemas operacionais que suportam a instalação do VDA).

> **Importante:**
>
> Se o componente Personal vDisk (PvD) já tiver sido 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 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.

Novembro 2023

Recursos novos e aprimorados

Limites de configuração modificados. A tabela a seguir descreve as modificações feitas nos limites da configuração do DaaS para melhorar o desempenho e oferecer economia.

Recurso	Limite antigo	Novo limite
Domínios do Active Directory	85	100
Catálogos	1000	2000
Grupos de entrega	1000	2000
Local de recursos	85	100
Locais de 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 lançar uma nova VM, fazendo dela uma opção mais eficiente para reter VMs em ciclos de energia. Em resposta a essa mudança, combinamos as opções **Retain VMs across power cycles** e **Retain system disk during power cycles** em uma única opção: **Retain VM and system disk during power cycles**. Isso significa que quando você seleciona essa opção para reduzir o tempo de reinicialização da VM retendo os discos do sistema, suas VMs também são retidas.

Novo recurso em Full Configuration para filtrar tamanhos de máquinas com base na *propriedade Encryption at Host* em perfis de máquina (específicos de VMs do Azure). Depois de escolher um perfil de máquina com a opção *Encryption at Host* ativada durante o gerenciamento ou a criação do catálogo de máquinas do Azure, somente os tamanhos de máquina que suportam o recurso são exibidos.

Restrição das ações de backup e restauração à função Full Administrator. Aprimoramos o controle de acesso para as ações de backup e restauração. Somente usuários com a função Full Administrator agora podem acessar o nó **Backup + Restore**, prevenindo ações não autorizadas.

Armazenamento de dados em cache para o nó de pesquisa. Introduzimos o cache de dados para o nó **Search** do Citrix DaaS. Esse aprimoramento melhora o desempenho da pesquisa e a lista a seguir mostra os casos de uso que facilitam suas tarefas regulares:

- Exibição rápida dos resultados da pesquisa depois que eles são restaurados pela primeira vez.
- Retém os resultados de paginação depois de sair e voltar para o nó de **pesquisa**.

Informações de imagem na página de catálogos de máquinas. Agora você pode visualizar as seguintes informações da imagem por meio de **Template Properties** do catálogo de máquinas:

- Sistema operacional
- Machine Identity Service
- Armazenamento de Machine Creation Services
- Caminho de arquivo de `pagefile.sys` para implantações do Azure

Esse aprimoramento fornece 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 fornecer uma experiência de pesquisa rápida, Full Configuration permite um recurso que fixa seus filtros de pesquisa. Os pinos de filtro permitem que você mantenha os filtros de pesquisa usados com frequência acessíveis na página. Esse aprimoramento está disponível nos painéis de pesquisa dos seguintes nós:

- **Pesquisa**
- **Catálogos de máquinas**
- **Grupos de entrega**
- **Aplicativos**

Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Suporte para associar metadados aos logs de configuração. Usando esse aprimoramento, agora você pode anexar metadados aos logs de configuração associando um par `name-value` às operações de alto nível. Para obter mais informações, consulte Associar metadados aos logs de configuração.

Ignora recursos órfãos com marcação tag específica. Em ambientes Azure, um recurso gerenciado pelo cliente marcado com todas as tags Citrix é detectado como um recurso órfão. Com esse 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. Depois de criar várias VMs usando o MCS, o SCCM (System Center Configuration Manager) exibia somente uma VM em seu console devido à duplicação de GUIDs. Agora, esse problema foi resolvido com a adição de uma etapa na preparação da imagem. Essa etapa exclui os certificados existentes e as informações do GUID na imagem mestre. A etapa está habilitada por padrão.

Reparo das informações de identidade das contas ativas do computador. Com esse recurso, você pode redefinir as informações de identidade de contas de computador ativas que tenham problemas

relacionados à identidade. Você pode optar por redefinir somente a senha da máquina e as chaves confiáveis ou redefinir todas as configurações do disco de identidade. A implementação é aplicável a catálogos de máquinas persistentes e não persistentes. Atualmente, o recurso é suportado somente para ambientes de virtualização do Azure e VMware. Para obter mais informações, consulte Reparar as informações de identidade de contas de computador ativas.

Obter criptografia nas informações do host associadas a um perfil de máquina. Nos ambientes do Azure, com esse recurso, agora você pode saber se a criptografia no host está habilitada para uma entrada de perfil de máquina (especificação de modelo ou VM) usando comandos do PowerShell. Para obter mais informações, consulte Recuperar criptografia nas informações do host de um perfil de máquina.

Reparo dos certificados de usuário das identidades de máquina híbridas ingressadas no Azure AD. Com esse recurso, você pode usar o comando Powershell para reparar os certificados de usuário de identidades de máquinas híbridas ingressadas no Azure AD se eles forem corrompidos ou expirarem. Para obter mais informações, consulte Criar catálogos ingressados no Azure Active Directory híbrido.

Você pode executar o comando `Get-ProvScheme` para obter informações sobre a data de expiração do certificado do usuário de um catálogo de máquinas ingressado no Azure AD híbrido.

Suporte para VMs confidenciais do Azure (prévia). VMs de computação confidencial do Azure garante que sua área de trabalho virtual seja criptografada na memória e protegida durante o uso. Com esse recurso, agora você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho do perfil da máquina para criar esse catálogo. Você pode usar as especificações do modelo VM e ARM como uma entrada de perfil de máquina. Para obter mais informações, consulte VMs confidenciais do Azure (prévia).

Suporte para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina no ambiente AWS. No ambiente da AWS, agora você pode usar um modelo de inicialização ou VM como entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina. As novas VMs adicionadas ao catálogo obtêm os valores de propriedades do perfil da máquina. Para obter mais informações, consulte Converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina.

Suporte para o plug-in HPE Moonshot gerenciado pela Citrix (prévia). 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 no chassi HPE Moonshot. O plug-in era baseado em APIs legadas que dificultavam os projetos de infraestrutura do MCS. Com essa função, foi introduzido um plug-in HPE Moonshot gerenciado pela Citrix (HPE Moonshot). Com esse plug-in, você pode criar conexões com seu chassi HPE Moonshot, criar catálogos e gerenciar

a energia das máquinas no catálogo usando a interface Full Configuration e os comandos do PowerShell. Para obter mais informações, consulte:

- Ambientes de virtualização do HPE Moonshot (prévia)
- Conexão com o HPE Moonshot (prévia)
- Criar um catálogo de máquinas do HPE Moonshot (prévia)
- Gerenciar um catálogo do HPE Moonshot (prévia)

Capacidade de alterar a memória e o tamanho do cache do disco. Com esse recurso, agora você pode alterar o tamanho da memória e do cache de disco do cache de write-back (quando MCSIO está ativado) usando um comando do PowerShell sem criar um novo catálogo de máquinas. Essa implementação ajuda você a ter a configuração de cache otimizada que é adequada às suas necessidades comerciais. Esse 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 criar um catálogo habilitado por chave de criptografia gerenciado pelo cliente. Em ambientes Azure, agora você pode criar um catálogo do Citrix Provisioning habilitado com a chave de criptografia gerenciada pelo cliente (CMEK) usando a interface Full Configuration e os comandos do PowerShell. Para obter mais informações, consulte Criar um catálogo ativado por chave de criptografia gerenciada pelo cliente.

Capacidade de copiar marcações em todos os recursos no Azure. Com esse recurso, no ambiente do Azure, agora você pode copiar marcações especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do sistema operacional, 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 especificação de modelo de ARM ou VM. Para obter mais informações, consulte Copiar marcações em todos os recursos.

O estado da sessão é atualizado para desconectado após a suspensão da máquina. Anteriormente, depois que você suspendia uma VM, a sessão ainda era exibida como **Ativa**. Com esse aprimoramento, depois que você suspender uma VM, o estado da sessão associada agora é mostrado como **Desconectado**.

Suporte para a criação de VMs da AWS que suportam a hibernação. Agora você pode criar catálogos de máquinas que oferecem suporte à hibernação de VMs em seus ambientes da AWS, aprimorando 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 esse recurso. Para obter mais informações, consulte Gerenciamento de energia de VMs da AWS.

Suporte para configurar métodos de balanceamento de carga no nível do grupo de entrega (prévia). Esse recurso permite que você escolha o método **Vertical Load Balancing** em um nível de grupo de entrega. Com esse recurso, cada máquina é alinhada ao índice de carga máximo antes que a próxima máquina seja ligada. AutoScale e Vertical Load Balancing determinam quando a próxima máquina será ligada. Esse recurso atinge a utilização máxima de cada máquina e economiza custos com nuvens públicas. Esse recurso oferece mais flexibilidade no gerenciamento das estratégias de balanceamento de carga das máquinas.

Você pode configurar um grupo de entrega para herdar o método de balanceamento de carga das configurações no nível do site ou substituir o método de balanceamento de carga no nível do site e, em seu lugar, escolher um dos métodos de balanceamento de carga vertical ou horizontal. Para obter mais informações, consulte a Etapa 2. Balanceamento de carga.

Suporte para VMs com capacidade de hibernação no Azure (prévia). Em ambientes Azure, você pode criar um catálogo de máquinas MCS que aceite a hibernação. Usando esse recurso, você pode suspender uma VM e depois se reconectar ao estado anterior da VM quando um usuário fizer login novamente. Para obter mais informações, consulte Criar VMs com capacidade de hibernação (prévia).

Guia de introdução ao DaaS. Lançamos um novo guia para agilizar e simplificar a implantação e a configuração do DaaS para administradores novos e experientes. Ele oferece os seguintes benefícios principais:

- **Fácil de começar.** Usando uma abordagem passo a passo tendo questionários como base, este guia ajuda novos administradores a configurar suas implantações rapidamente. As informações de ajuda contextual em todo o guia ajudam a entender os conceitos e a terminologia essenciais.
- **Simplifique configurações complexas.** Este guia inclui configurações pré-definidas, quando aplicável, e fornece acesso à interface de usuário Full Configuration para a 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 (prévia).

Atribuir letras de unidade a discos de cache de write-back usando Full Configuration. Anteriormente, você só podia atribuir uma letra de unidade específica ao disco de cache de write-back usando um cmdlet PowerShell. Agora você pode realizar a mesma tarefa usando Full Configuration. Para obter mais informações, consulte Criar catálogos de máquinas.

Suporte para alterar várias propriedades de máquina do Azure usando Full Configuration. Nas máquinas do Azure provisionadas por Machine Creation Services, agora você pode alterar as seguintes configurações de propriedade usando Full Configuration:

- Tipo de armazenamento
- ID do grupo do host

- Configurações da Galeria de Computação do Azure

Quando você altera qualquer uma dessas configurações, Full Configuration identifica automaticamente as configurações relacionadas e fornece sincronização automática ou mensagens de aviso solicitando que você selecione novamente as configurações relacionadas. Esse recurso garante mudanças consistentes nas configurações associadas, evitando possíveis erros de configuração. Para obter mais informações, consulte Editar um catálogo.

Usar pools de identidades existentes para criar identidades para máquinas provisionadas por MCS. Ao criar catálogos ingressados no AD ou adicionar máquinas a eles usando Full Configuration, agora você pode usar um pool de identidades existentes para alocar identidades de máquinas. Esse recurso permite que você aplique um esquema consistente de nomenclatura de conta de máquina entre vários catálogos. Para obter mais informações, consulte Identidades de máquina.

Topologia da sessão. A exibição Session Topology é a próxima etapa para aprimorar os fluxos de trabalho de solução de problemas em Monitor. A exibição Session Topology fornece uma representação visual do caminho da sessão de sessões HDX conectadas. Você pode acessar a exibição da topologia em **User Details > Session Performance**.

A exibição Session Topology de 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 de ICA e ICA RTT são exibidas para a sessão quando ela está em um estado conectado.

Use a exibição Session Topology 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 2023

Recursos novos e aprimorados

Refinar as 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 do Autoscale e dados de uso da máquina da semana anterior. Com esse gráfico, você pode obter insights sobre a eficiência das configurações do Autoscale:

- **Not cost-effective**. O desperdício financeiro existe devido ao excesso de provisionamento de capacidade.
- **Poor user experience**. A experiência do usuário é afetada negativamente devido ao subprovisionamento da capacidade.
- **Good balance between user experience and cost**. A capacidade provisionada está alinhada com o uso histórico.

Para obter mais informações, consulte Analisar a eficiência das configurações do AutoScale.

Suporte a várias NICs para VMs do Azure. Com Full Configuration, agora você pode criar VMs do Azure com várias NICs. A contagem máxima de NICs de uma VM é determinada pela configuração do tamanho da máquina, enquanto a 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 das métricas de desempenho da sessão. O Monitor introduziu a nova guia **User Details > Session Performance** com fluxos de trabalho aprimorados para a solução de problemas, começando com a capacidade de correlacionar métricas em tempo real para identificar problemas nas sessões do usuário. Session Experience 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. Esse recurso ajuda a reduzir o tempo médio de resolução, permitindo que você correlacione várias métricas de desempenho em uma exibição simples. Para obter mais informações, consulte o artigo Problemas de usuário.

Suporte à versão VDA na página de configurações da política de criação/edição. Como parte da criação de uma política e ao definir as configurações, o sistema oferece a opção de visualizar o tipo das configurações. Você pode visualizar os seguintes tipos de configurações:

- All settings –Exibir todas as configurações de todas as versões do VDA
- Current settings only –Exibir configurações somente para as versões atuais do VDA
- Legacy settings only –Exibir configurações somente para as versões do VDA preteridas

Para obter mais informações, consulte Criar políticas

Limite de visibilidade do aplicativo suportado somente para contas do Active Directory. A capacidade de limitar a visibilidade do aplicativo está disponível somente para as contas de usuário do Active Directory, não para as contas do Azure Active Directory e Okta. Observe que, para auxiliar esse recurso, no fluxo de trabalho de configuração do aplicativo, na página Select Users or Groups, as opções **Azure Active Directory** e **Okta** no campo **Select Identity type** estão desativadas.

Nova opção de interface do usuário para excluir registros de VM somente do banco de dados do site Citrix. Quando a exclusão do catálogo e da VM falha devido a um hipervisor inacessível, agora você pode optar por excluir somente os registros da VM do banco de dados do site da Citrix, deixando as VMs intactas no host. Para obter mais informações, consulte Excluir um catálogo.

Suporte para criar catálogos de máquinas vazios para máquinas não provisionadas pelo MCS. A criação de catálogos de máquinas vazios agora se estende a máquinas não provisionadas pelo MCS, incluindo:

- Máquinas virtuais ou blade provisionadas usando outras tecnologias diferentes de Machine Creation Services.

- Máquinas físicas sem gerenciamento de energia pelo Citrix DaaS
- Máquinas de acesso ao PC remoto

Com esse recurso, agora você pode criar catálogos de máquinas sem a necessidade de adicionar máquinas a eles durante a criação do catálogo.

Aprimoramentos de 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 selecionar um nó, somente as imagens desse nó serão 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 pressionada a tecla CTRL e clicando no nó. Para obter mais informações, consulte Imagem mestre.

Ligar atribuído ao pico do AutoScale. Quando áreas de trabalho persistentes são ligadas, mas permanecem sem uso ou se nenhum usuário faz login, os administradores podem definir o tempo de espera para realizar ações como suspender, desligar ou nenhuma ação.

Para máquinas atribuídas, as quais estão ligadas, mas nenhuma sessão foi conectada a elas dentro do horário definido após o início do horário de pico, você pode adicionar uma política ao nível do grupo de entrega para desligar a máquina.

Para máquinas atribuídas, as quais estão em estado de continuação, mas nenhuma sessão foi conectada a elas dentro do horário definido após o início do horário de pico, você pode adicionar uma política ao nível do grupo de entrega para suspender a máquina.

Esse recurso é útil se houver um usuário final que está no PTO, não está conectado ou se uma empresa tem um fim de semana 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 com SO de sessão única e Grupos de entrega estáticos com SO de sessão única

Monitorar várias instâncias do Citrix DaaS (prévia). 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 suporte técnico em todas as instâncias configuradas do DaaS a partir de um único console do Monitor. Para obter mais informações sobre a configuração necessária para agregar as instâncias do serviço spoke a um hub, consulte Agregar várias instâncias de serviço do Citrix Virtual Apps and Desktops. O Monitor suporta agregar até quatro locatários do DaaS (spokes) sob um único locatário do DaaS (hub).
Para ter um monitoramento unificado de todos os locatários do DaaS, use a enumeração bidirecional das instâncias hub e spoke. Para obter mais informações, consulte Pesquisa agregada em várias instâncias de DaaS (prévia).

Suporte para vSAN 8.0. Agora você pode usar o MCS para provisionar VMs no ambiente vSAN 8.0.

Preservar as configurações da NIC em VMs provisionadas. Anteriormente, as configurações da NIC da imagem mestre não eram mantidas nas VMs provisionadas. Por exemplo, se você definisse as configurações de DNS na imagem mestre, as VMs provisionadas não manteriam as configurações de DNS definidas da imagem mestre. Com esse recurso, as VMs provisionadas agora podem reter as configurações da NIC da imagem mestre. As configurações são mantidas mesmo após uma atualização do Windows. O driver de filtro é instalado automaticamente se você fizer uma nova instalação do VDA versão 2308 ou posterior em uma máquina com Hyper-V implantado 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 marcar a caixa de seleção **Citrix HyperV Filter Driver** na página **Additional Components** ao atualizar o VDA. Para obter mais informações, consulte Instalar componentes adicionais.

Esse 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 esse recurso, agora você pode detectar os recursos órfãos em sua implantação do Azure, permitindo o gerenciamento eficiente de recursos. Depois que os recursos órfãos são identificados, você pode tomar outras medidas, gerando mais produtividade e redução de custos. Para obter mais informações, consulte Detectar recursos órfãos do Azure em sua implantação.

Novo status de atualização da imagem. Ao monitorar os status de atualização de imagens dos catálogos em Full Configuration, agora você pode exibir o novo status **Preparing image**, além dos já existentes: **Fully updated**, **Partially updated** e **Pending update**. Para obter mais informações, consulte Alterar a imagem mestre.

Comandos do PowerShell para criar marcações automáticas (prévia). Com esse recurso, agora você pode criar marcações automaticamente usando o comando do PowerShell. Para obter mais informações, consulte Marcações automáticas.

O sinal de notificação é exibido para o usuário ou grupo de entrega. Ao criar ou modificar uma política e definir as configurações, se todos os grupos de entrega estiverem desativados, o sistema exibirá um aviso: None of the elements in this filter is enabled. Se pelo menos um grupo de entrega estiver ativado, o sistema não exibirá o sinal de aviso. Para obter mais informações, consulte Configurações de política.

Setembro 2023

Recursos novos e aprimorados

Comandos do PowerShell para gerenciar o Cache de host local (LHC). Agora você pode usar os comandos do PowerShell para gerenciar o LHC nos Citrix Cloud Connectors. Para obter mais informações, consulte Comandos do PowerShell de Cache de host local.

Suporte para criar catálogos de máquinas vazios. Em Full Configuration, agora você pode criar um catálogo de máquinas sem a criação imediata da VM. Com esse recurso, você pode adiar a criação da VM até que os hosts de back-end estejam totalmente preparados ou o provisionamento da VM esteja concluído, obtendo mais flexibilidade na criação de catálogos. Atualmente, esse recurso se aplica somente 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. Esse aprimoramento melhora a experiência do usuário reduzindo os tempos de carregamento da página quando você navega até o nó **Home**.

Aprimoramentos de pesquisa para aplicativos. Aprimoramos a funcionalidade de pesquisa no nó **Applications** para se alinhar ao novo design introduzido no nó **Search**. Esse novo recurso melhora sua experiência de pesquisa de aplicativos e mantém uma experiência de pesquisa consistente no DaaS. A palavra-chave **Application Name** na expressão do filtro foi renomeada para **Name**, mas mantem seu significado original. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Gerenciamento aprimorado do escopo: mostrando objetos na exibição da pasta. Nas páginas de criação e gerenciamento do escopo, os catálogos de máquinas, grupos de entrega e grupos de aplicativos agora são exibidos em estruturas de pastas que se alinham com o gerenciamento deles no DaaS. Essa exibição de pastas simplifica o processo de seleção de objetos para a criação e o gerenciamento do escopo, tornando suas escolhas mais intuitivas e diretas. Para obter mais informações, consulte Criar e gerenciar escopos.

Foi removida a opção Leave user management to Citrix Cloud. Ao criar um grupo de entrega em Manage > Full Configuration, na página Users, o suporte a essa opção foi removido. Para grupos de entrega em que as atribuições de usuários foram realizadas por meio do Citrix Cloud, continue gerenciando as atribuições de usuários na biblioteca do Citrix Cloud.

Removida a opção Azure Germany. Alinhado ao encerramento do Microsoft Cloud Deutschland em 29 de outubro de 2021, removemos a opção **Azure Germany** da página de criação de conexão do host.

Alertas de serviços proativos em Full Configuration. Os alertas vêm em dois níveis: alertas de todo o site mostrados na página Home (ícone de bandeira) e alertas relacionados à zona exibidos na guia

Troubleshoot de cada zona. Atualmente, esse recurso fornece avisos e alertas proativos para garantir que o seu cache de host local e as zonas estejam configurados corretamente para que, quando ocorrer uma interrupção, o cache do host local funcione e seus usuários não sejam afetados. Para obter mais informações, consulte Alertas de integridade do serviço e Zonas.

Agosto 2023

Recursos novos e aprimorados

Full Configuration: suporte para provisionar VMs da AWS e do GCP usando perfis de máquina. Ao provisionar VMs da AWS ou do GCP usando Machine Creation Services (MCS), agora você pode selecionar uma VM existente como perfil da máquina, permitindo que as VMs do catálogo herdem as configurações da VM selecionada.

- Para VMs do GCP, as configurações herdadas incluem ID do conjunto de criptografia de disco, tamanho da máquina, tipo de armazenamento e zona.
- Para VMs da AWS, as configurações herdadas variam de acordo com o estágio:
  - Durante a criação do catálogo: tamanho da máquina, tipo de locação, grupo de segurança e 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.

Nova funcionalidade de pesquisa nos nós de catálogos de máquinas e grupos de entrega. Agora você pode pesquisar e localizar diretamente catálogos de máquinas e grupos de entrega nos nós **Machine Catalogs** e **Delivery Groups** A funcionalidade de pesquisa nesses nós fornece a mesma interface do nó de **pesquisa**, fornecendo uma excelente experiência de pesquisa em todo o DaaS. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Visualize o status do dispositivo do ponto de extremidade no Session Launch Diagnostics usando a postura do dispositivo. O recurso Session Launch Diagnostics no Monitor ajuda a restringir o componente e o estágio exatos em que ocorreu uma falha na sessão. Isso ajuda a identificar o motivo exato de uma falha no início de uma sessão e a tomar a ação recomendada.

Como próxima etapa para tornar essa verificação abrangente a todos os componentes envolvidos na sequência de início da sessão, agora você pode visualizar os resultados da varredura do dispositivo do ponto de extremidade. Clique em **Endpoint Device** na lista de componentes para exibir o status de varredura da postura do dispositivo. O serviço Device Posture faz a varredura do dispositivo do ponto de extremidade para verificar sua conformidade com base nas políticas definidas pelo administrador.

Certifique-se de que o serviço Device Posture esteja configurado com DaaS conforme descrito no artigo sobre a postura do dispositivo. Os erros registrados no log pelo Device Posture estão descritos em Device Posture Error Logs.

Para obter mais informações, consulte Etapas para diagnosticar a falha no início da sessão.

Novas opções em Full Configuration para rotear solicitações de API para o Azure e o GCP por meio dos Citrix Cloud Connectors. Anteriormente, as solicitações de API para o Azure e o GCP só podiam ser roteadas através de pontos de extremidade públicos. Com uma nova opção em **Full Configuration > Add Connection and Resources**, agora você pode optar por uma abordagem mais segura roteando-as através dos Citrix Cloud Connectors. Para obter mais informações, consulte Criar uma entidade de serviço e uma conexão usando Full Configuration.

Aprimoramentos em pesquisa e filtro. Fizemos os seguintes aprimoramentos para melhorar sua experiência de pesquisa:

- **Pesquisa simplificada**: a realização de uma pesquisa sem filtros agora remove as recomendações de pesquisa, proporcionando uma experiência de pesquisa clara e direta.
- **Atualização do operador AND/OR**: as opções "Match all (operador AND)"e "Match any (operador OR)"agora estão disponíveis no painel de filtros, acessíveis com um único clique no ícone de filtros.
- **Configuração agilizada do filtro**: agora você pode especificar e aplicar vários filtros sem entraves com o painel de filtros.
- **Interface mais clara**: a capacidade de "fixar o filtro"foi removida, reduzindo o excesso de informações na interface do usuário e tornando sua experiência de pesquisa mais intuitiva.
- **Adição rápida de filtros**: depois de aplicar filtros, agora você pode usar o sinal de adição 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 ir para **Manage filter sets**.

Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Suporte de atualização de VDA para catálogos de máquinas criados pelo Azure Quick Deployment. Em Full Configuration, agora você pode habilitar o **VDA Upgrade** para catálogos de máquinas criados por meio do Azure Quick Deploy e realizar o **Upgrade VDA** neles para atualizações imediatas ou programadas. Para obter mais informações, consulte Atualizar VDAs usando a interface Full Configuration.

Capacidade de redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS no SCVMM. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. O recurso automatiza o processo de redefinição do disco do sistema operacional. Por exemplo, ele ajuda na redefinição da VM para o seu status inicial de catálogo de área de

trabalho de desenvolvimento persistente criado usando o MCS. Atualmente, esse recurso é aplicável aos ambientes de virtualização do Azure, Citrix Hypervisor, SCVMM e VMware. Para obter mais informações sobre como usar o comando do PowerShell para redefinir o disco do sistema operacional, consulte Redefinir disco do sistema operacional.

Atualize as propriedades de VMs individuais. Agora você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistentes usando um comando do PowerShell. Essa implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, esse recurso é aplicável somente ao ambiente do Azure. Para obter mais informações, consulte Atualizar propriedades de VMs individuais.

Restrinja o upload e o download de discos gerenciados. De acordo com a política do Azure, você não pode carregar ou baixar mais de cinco discos ou instantâneos ao mesmo tempo com o mesmo objeto de acesso ao disco. Com esse recurso, o limite de cinco uploads ou downloads simultâneos não é aplicado se você:

- Configurar `ProxyHypervisorTrafficThroughConnector` em `CustomProperties` e
- Não configurar a política do Azure para criar Acessos ao disco automaticamente para que cada novo disco use pontos de extremidade privados.

Suporte para atribuir uma letra de unidade específica ao disco de cache de write-back MCS I/O. Anteriormente, o sistema operacional Windows atribuía automaticamente uma letra de unidade ao disco de cache de write-back MCS I/O. Com esse recurso, agora você pode atribuir uma letra de unidade específica ao disco de cache de write-back MCS I/O. Essa implementação ajuda a evitar conflitos entre a letra da unidade de qualquer aplicativo que você usa e a letra da unidade do disco de cache de write-back MCS I/O. Esse recurso é aplicável somente ao sistema operacional Windows. Para obter mais informações, consulte Atribuir uma letra de unidade específica ao disco de cache de write-back MCS I/O.

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 fonte da entrada do perfil da máquina é uma VM. O perfil da 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.

Suporte para criar um catálogo de VMs habilitado com a Amazon Elastic Graphics. Usando o fluxo de trabalho baseado em perfil de máquina, agora você pode criar um catálogo de VMs habilitadas com o acelerador da Amazon Elastic Graphics. Você pode usar uma VM ou um modelo de execução como uma entrada de perfil de máquina. Para obter mais informações, consulte Criar um catálogo de VMs habilitadas com o acelerador do Elastic Graphics.

Tentativa de recriar o catálogo após uma falha. Quando a criação do catálogo falhar, agora você pode tentar criar o catálogo novamente. Para garantir a criação bem-sucedida, verifique as infor-

mações de solução de problemas e resolva os problemas. As informações descrevem os problemas encontrados e fornecem recomendações para resolvê-los. Catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, acesse a guia **Troubleshoot** de cada catálogo. Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Permissão para gerenciar conjuntos de configurações. Para permitir um controle mais preciso sobre o gerenciamento do conjunto de configurações do WEM, introduzimos uma nova permissão chamada **Manage configuration sets** no conjunto de permissões **Machine catalogs**. Essa permissão concede acesso exclusivo aos usuários que podem realizar tarefas como vincular ou desvincular um conjunto de configurações e alternar para um conjunto de configurações diferente para os catálogos. Para obter mais informações, consulte Gerenciar o conjunto de configurações para um catálogo.

Nova opção em Full Configuration para permitir eliminar dispositivos obsoletos ingressados no Azure AD. Introduzimos uma opção em Full Configuration para simplificar a eliminação de dispositivos obsoletos ingressados no Azure AD no Citrix DaaS. Anteriormente, era necessário executar um script personalizado do PowerShell para realizar a tarefa. A ativação dessa opção concede às conexões do host a permissão para eliminar automaticamente os dispositivos obsoletos ingressados no Azure AD. Para obter mais informações, consulte Conexões de host do Azure.

Monitore o status de atualização de imagens para catálogos usando Full Configuration. Agora você pode monitorar os status de atualização de imagens de catálogos de máquinas não persistentes usando uma nova coluna, **Image Update**. Essa coluna indica se as imagens de um catálogo estão **totalmente atualizadas**, **parcialmente atualizadas** ou com **atualização pendente**.

Para mostrar a coluna na tabela de **catálogos de máquinas**, siga estas etapas:

1. No nó **Machine Catalogs**, selecione o ícone **Columns to Display** na barra de ações.
2. Selecione **Machine Catalog > Image Status**.
3. Clique em **Salvar**.

A exibição da coluna **Image update** pode prejudicar o desempenho do console. Recomendamos exibi-lo somente quando necessário.

Ambiente seguro para tráfego gerenciado do GCP. Com esse recurso, agora você pode permitir somente o acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aumenta a segurança para manipular dados confidenciais. Para fazer isso, adicione `ProxyHypervisorTrafficThroughConnector` em `CustomProperties` no caso de uma implantação do Citrix Cloud. Se você estiver usando um pool de workers privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter mais informações, consulte Criar um ambiente seguro para o tráfego gerenciado do GCP.

Julho 2023

Recursos novos e aprimorados

Suporte para obter uma lista de recursos órfãos no Azure. Nos ambientes do 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 criar máquinas multissessão persistentes usando Full Configuration. Ao criar um catálogo de máquinas multissessão, agora você pode especificar se deseja torná-las persistentes. Para máquinas multissessão persistentes, lembre-se de que as alterações feitas pelos usuários nas áreas de trabalho são salvas e ficam acessíveis a todos os usuários autorizados. Para obter mais informações, consulte Criar catálogos de máquinas.

Novo recurso em Full Configuration para filtrar o inventário da AWS AMI. Ao selecionar modelos de máquina durante a criação do catálogo da AWS, agora você pode filtrar o inventário da AWS AMI 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 itens são carregados à medida que você rola a lista.

Suporte para excluir dispositivos do Azure AD. Com esse recurso, dispositivos obsoletos do Azure AD podem ser excluídos de forma consistente, atribuindo-se a função Cloud Device Administrator à entidade 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 Criar catálogos ingressados no Azure Active Directory.

Suporte para perfil de máquina no ambiente da 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 iniciar a versão do modelo e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume do EBS, tipo de instância, otimização do EBS, Elastic Graphics e outras configurações compatíveis da AWS. Ao editar o catálogo, o perfil de máquina das máquinas provisionadas pode ser alterado fornecendo uma VM ou um modelo de inicialização diferente. Para obter mais informações, consulte Criar um catálogo usando um perfil de máquina.

O limite de exportação dos resultados da pesquisa foi estendido de 10.000 para 30.000. Estendemos o limite de exportação dos resultados da pesquisa. Antes restrito a 10.000 itens, agora você

pode exportar até 30.000 itens para um arquivo CSV. Para obter mais informações, consulte Exportar resultados da 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 **Refresh** no canto superior direito. Observe que a opção **Refresh** não está disponível para catálogos da AWS. A opção **Refresh** também está disponível para perfis de máquina e grupos de hosts nos catálogos do Azure.

Junho 2023

Recursos novos e aprimorados

Suporte para obter propriedades personalizadas da entrada do perfil da máquina no GCP. Anteriormente, em ambientes do GCP, ao criar um catálogo de máquinas MCS usando uma entrada de perfil de máquina, você precisava especificar explicitamente as propriedades personalizadas. A ação forçou um esforço extra. Com esse recurso, agora você pode derivar as seguintes propriedades personalizadas sem defini-las explicitamente:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Quando você executa os comandos `New-ProvScheme` e `Set-ProvScheme` e não especifica 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 entrará em vigor.

Remover tags em ambientes da AWS. Anteriormente, os comandos `Remove-ProvVM` e `Remove-ProvScheme` do PowerShell 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 precisava gerenciar individualmente as VMs e os catálogos de máquinas que não eram totalmente removidos de todos os recursos. Com esse recurso, você pode usar:

- O parâmetro `Remove-ProvVM` com `ForgetVM` para remover VMs e tags de uma única VM ou uma lista de VMs de um catálogo de máquinas.
- O parâmetro `Remove-ProvScheme` com `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e recursos de um catálogo de máquinas.

Essa implementação ajuda na:

- Identificação de recursos vazados
- Remoção do custo adicional de manter os recursos que não são necessários

Esse recurso é aplicável somente a VMs persistentes. Para obter mais informações, consulte Remover tags.

Capacidade de obter erros históricos e avisos associados a um catálogo de máquinas MCS. Anteriormente, você só recebia os últimos avisos e erros associados a um catálogo de máquinas. Com esse recurso, agora você pode obter uma lista do histórico de avisos e erros de um catálogo de máquinas MCS. Esta lista ajuda você a entender os problemas com seu o catálogo de máquinas MCS e corrigi-los.

Para obter mais informações, consulte Recuperar avisos e erros associados a um catálogo.

Maior capacidade com desempenho aprimorado para a Citrix no Google Cloud. Agora, a Citrix pode oferecer suporte a catálogos contendo até 3.000 VDAs em um único projeto do Google Cloud. Essa atualização traz melhorias de desempenho nas operações de provisionamento e gerenciamento de energia.

Capacidade de redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS no ambiente Google Cloud e AWS. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. O recurso automatiza o processo de redefinição do disco do sistema operacional. Por exemplo, ele ajuda na redefinição da VM para o seu status inicial de catálogo de área de trabalho de desenvolvimento persistente criado usando o MCS. Atualmente, esse recurso é aplicável aos ambientes de virtualização da AWS, Azure, Citrix Hypervisor, Google Cloud e VMware. Para obter mais informações sobre como usar o comando do PowerShell para redefinir o disco do sistema operacional, consulte Redefinir disco do sistema operacional.

Suporte para alterar propriedades personalizadas relacionadas ao disco de um catálogo existente e de VMs existentes no GCP. Anteriormente, nos ambientes do GCP, você podia adicionar as propriedades personalizadas somente ao criar o catálogo de máquinas MCS. Com esse recurso, agora você pode alterar as seguintes propriedades personalizadas relacionadas ao disco de um catálogo existente e das VMs existentes do catálogo.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Essa implementação ajuda você a selecionar diferentes tipos de armazenamento para discos diferentes mesmo depois de criar um catálogo, e, assim, equilibrar os preços associados aos diferentes

tipos de armazenamento. Para obter mais informações, consulte Alterar propriedades personalizadas relacionadas ao disco de um catálogo existente.

Suporte a tempo limite de sessão dinâmica estendido para a versão 2203 LTSR CU3 ou posterior do VDA. Para grupos de entrega de SO de sessão única, esse recurso agora se aplica aos VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Para obter mais informações, consulte Tempos limite de sessão dinâmica.

Experiência aprimorada de criação de conexão de host em Full Configuration. Depois de selecionar um local de recursos, a lista suspensa **Connection type** agora exibe todos os hipervisores e serviços em nuvem compatíveis com a Citrix, e suas disponibilidades dependem de:

- Para um local de recursos sem Cloud Connectors acessíveis, somente hipervisores e serviços em nuvem que oferecem suporte a implantações sem conector estão disponíveis.
- Para um local de recursos com Cloud Connectors acessíveis, somente hipervisores e serviços em nuvem que tenham seus plug-ins devidamente instalados nesses conectores estão disponíveis.

Para obter mais informações, consulte Criar e gerenciar conexões.

Seleção adicional de componentes na atualização do VDA. Agora você pode selecionar quais componentes adicionais devem ser atualizados ou instalados durante o upgrade de um VDA. Para obter mais informações, consulte Configurar o upgrade automático para VDAs.

> **Importante:**
>
> Para usar o recurso de componentes adicionais, certifique-se de que seu VDA Upgrade Agent seja da versão 7.34 ou posterior, que está incluída na versão 2206 ou posterior do instalador do VDA.

Full Configuration agora predefine determinadas configurações para máquinas do Azure com base em perfis de máquina. Quando você provisiona VMs do Azure, a Full Configuration agora predefine 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 instâncias da AWS. Agora você pode iniciar instâncias da AWS, configurá-las conforme desejar e hiberná-las. O processo de hibernação armazena o estado na memória da instância, junto com seus endereços Elastic IP e privado, permitindo que ela continue exatamente de onde parou. Para obter mais informações sobre a criação de VMs que oferecem suporte à hibernação, consulte Hibernação de instâncias.

Suporte para otimizar a limitação da AWS. Agora você pode ligar e desligar um grande número de máquinas em um catálogo da AWS sem ter problemas de limitação. Os problemas de limitação

ocorrem quando o número de solicitações enviadas à AWS excede o número de solicitações que o servidor pode processar. Esse 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 pontos de extremidade do Azure interagissem com os recursos em seu ambiente. Como resultado, surgiam questões de segurança porque a Internet pública havia sido acessada. Com esse recurso, o MCS permite que o tráfego de rede seja roteado através de Citrix Cloud Connectors no seu ambiente. Isso torna o ambiente seguro porque, assim, 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 o tráfego gerenciado do Azure.

Depois de definir as propriedades personalizadas, você pode configurar as políticas do Azure para ter acesso ao disco privado aos discos gerenciados do Azure.

Suporte para provisionar VMs do catálogo com o agente do Azure Monitor. O Azure Monitor Agent (AMA) coleta dados de monitoramento e os entrega ao Azure Monitor. Com esse recurso, você pode provisionar VMs do catálogo de máquinas MCS (persistentes e não persistentes) com o AMA instalado como uma extensão. Essa implementação permite o monitoramento, ao identificar as máquinas virtuais de forma exclusiva nos dados de monitoramento. Para obter mais informações sobre o AMA, consulte Visão geral sobre o agente do Azure Monitor.

Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Para obter mais informações sobre o provisionamento de VMs do catálogo de máquinas com o AMA habilitado, consulte Provisionar VMs de catálogo com o agente do Azure Monitor instalado.

Ativar o agendamento de reinicialização para um catálogo MCS. Anteriormente, você podia agendar atualizações de imagens, tanto aguardando a próxima reinicialização ou acionando uma reinicialização imediata de todas as VMs. Com esse recurso, agora você pode criar um agendamento de reinicialização única para que um catálogo seja disparado na data e hora desejadas para facilitar as atualizações de imagens do MCS. Para criar um agendamento de reinicialização, use o comando `BrokerCatalogRebootSchedule`. Para obter mais informações, consulte Alterar a imagem mestre.

Gerencie segredos de clientes expirados no Azure Quick Deploy. No Azure Quick Deploy, agora você pode se manter informado com alertas quando os segredos do cliente expirarem e atualizá-los facilmente para garantir o acesso contínuo aos recursos do Azure. Para obter mais informações, consulte Atualizar segredos de clientes expirados.

Maio 2023

Recursos novos e aprimorados

Aprimoramentos de pesquisa. Esse recurso aprimora os recursos visuais e as interações dos filtros, proporcionando uma melhor experiência de pesquisa. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Nova política de exclusões de usuários na qual você pode definir caminhos de diretório que não são redirecionados para a camada de usuário. As exclusões de usuários se aplicam à camada de personalização do usuário (UPL), mas não ao host da sessão. O Logoff.txt agora contém todas as exclusões de usuários ativos. 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 do VMware, agora você pode atualizar a versão de hardware das VMs recém-adicionadas em um catálogo de máquinas MCS existente usando uma origem 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 do perfil da máquina para usar esse recurso.

Suporte para filtrar instâncias de VM da AWS. Anteriormente, quando você usava uma instância de VM da 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 à entrada inválida do perfil da máquina. Com esse recurso, agora você pode listar as instâncias de VM da AWS que podem ser usadas como VMs válidas de perfil de máquina. Para fazer isso, use o comando `Get-HypInventoryItem`. Para obter mais informações, consulte Filtrar instâncias de VM.

Suporte para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina no ambiente Azure. No ambiente do Azure, agora você pode usar uma especificação de modelo ou VM como entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina. As VMs existentes e as novas VMs adicionadas ao catálogo obtêm valores de propriedades do perfil da máquina, a menos que sejam substituídas por propriedades personalizadas explícitas. Para obter mais informações, consulte Converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina.

Suporte para criptografia dupla em disco gerenciado no ambiente Azure. No ambiente do 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 algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, instantâneos e imagens

são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla no disco gerenciado.

Suporte para perfil de máquina no VMware. Em ambientes do VMware, agora você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A fonte da entrada do perfil da máquina é um modelo VMware. O perfil da 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 sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS no Azure e no Citrix Hypervisor. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. O recurso automatiza o processo de redefinição do disco do sistema operacional. Por exemplo, ele ajuda na redefinição da VM para o seu status inicial de catálogo de área de trabalho de desenvolvimento persistente criado usando o MCS. Atualmente, esse recurso é aplicável aos ambientes de virtualização do VMware, Azure e Citrix Hypervisor. Para obter mais informações sobre como usar o comando do PowerShell para redefinir o disco do sistema operacional, consulte Redefinir disco do sistema operacional.

Experiência aprimorada de criação de conexão com o host. Agora você pode obter as seguintes informações ao criar uma conexão de host:

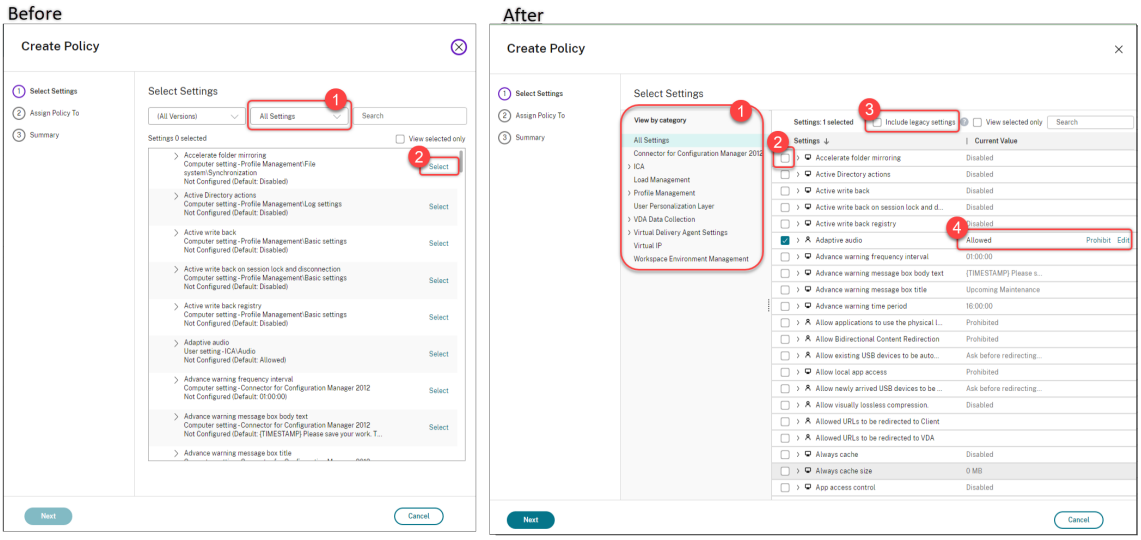
- Listar de todos os plug-ins de hipervisor compatíveis com o Citrix, incluindo plug-ins de terceiros
- Disponibilidade do plug-in de hipervisor. Se o status de disponibilidade for false, o possível motivo pode ser que o Cloud Connector não esteja instalado

Esse recurso ajuda você a configurar corretamente um local de recursos e, assim, criar uma conexão de host. Para obter mais informações, consulte a Etapa 1. Conexão.

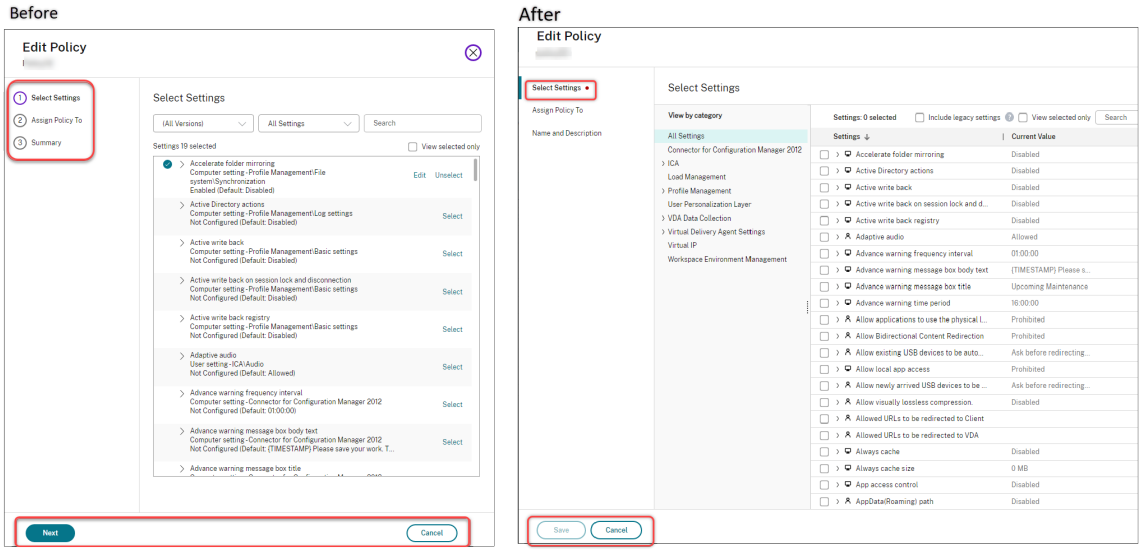
Melhorias na experiência do usuário no nó de Políticas. Para melhorar a experiência do usuário e tornar o gerenciamento de políticas mais eficiente, implementamos as seguintes melhorias no nó **Full Configuration > Policies**:

- Novo design de interface do usuário para as ações **Create Policy** e **Create Template**:
  - Exibição de pasta expansível para configurações de política. Na página **Select Settings**, todas as configurações são exibidas por categoria em um modo de exibição de árvore expansível, facilitando encontrar uma configuração.
  - Para selecionar uma configuração, basta clicar em uma caixa de seleção em vez de usar o botão **Select**.
  - As configurações antigas foram ocultadas por padrão para que somente as configurações mais relevantes sejam exibidas. Se forem necessárias configurações antigas, selecione **Include legacy settings**.

  - 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 de interface do usuário para a ação **Edit Policy**:
  - O menu de navegação foi atualizado para uma lista não ordenada. Cada item na lista agora inclui um botão **Save** em sua página. Com esse 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 as políticas. Na lista de prioridades, agora você pode alterar a prioridade de uma política arrastando-a até a posição desejada.

Nova opção para desativar o desligamento forçado do usuário no AutoScale. A nova opção **Neither notify nor force user logoff** agora está disponível na página **Manage Autoscale > User Logoff Notification**. Com a opção selecionada, o AutoScale não forçará os usuários a se desconectarem das máquinas em estado de esvaziamento nem notificará os usuários para se desconectarem e se conectarem a uma máquina diferente. Para obter mais informações, consulte Notificações de logoff do usuário.

Capacidade de reiniciar PCs na nuvem do Windows 365. Agora você pode usar o Citrix DaaS para reiniciar PCs na nuvem do Windows 365.

Mais detalhes da sessão. Quando você exibe uma sessão em **Full Configuration > Search > Sessions**, a exibição da sessão (no painel inferior) agora inclui mais detalhes da sessão para ajudá-lo a solucionar e identificar problemas do cliente:

- **Reconnect time.** A hora em que uma sessão se reconectou após ser desconectada.
- **Client platform.** A plataforma usada para iniciar a sessão.
- **Client version.** A versão da plataforma do cliente usada para iniciar a sessão.
- **Remote host IP.** O endereço IP do host remoto em que o Citrix Workspace está hospedado.

Suporte para renomear grupos de segurança do Azure AD para VMs. Para VMs adicionadas a um grupo de segurança do Azure AD por meio do Citrix DaaS, agora você pode renomear o grupo de segurança usando **Full Configuration > Edit Machine Catalog**. A renomeação ocorre depois que você salva a alteração.

Seleção de domínio padrão para contas de máquina. Quando você cria um catálogo, o domínio em que o recurso (conexão) reside é selecionado por padrão para as contas de máquina.

Capacidade de exibir os grupos de segurança atribuídos ao Azure AD das VMs a ingressar. Em Full Configuration, quando você cria VMs ingressadas no Azure Active Directory, a opção **Join an assigned security group as a member** 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 por meio de uma imagem do Azure Resource Manager.

Suporte para troca de redes das conexões. Em Full Configuration, agora você pode alterar as redes de 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 do Azure. Anteriormente, os comandos `Remove-ProvVM` e `Remove-ProvScheme` do PowerShell 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 precisava gerenciar individualmente as VMs e os catálogos de máquinas que não eram totalmente excluídos de todos os recursos. Com esse recurso, você pode usar:

- O parâmetro `Remove-ProvVM` com `ForgetVM` para remover VMs e tags criadas nos recursos de uma única VM ou de uma lista de VMs de um catálogo de máquinas.
- O parâmetro `Remove-ProvScheme` com `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e tags criadas nos recursos de um catálogo de máquinas inteiro.

Essa implementação ajuda a identificar recursos órfãos que são criados pelo MCS, mas não são mais usados pelo MCS.

Esse recurso é aplicável somente a VMs persistentes. Para obter mais informações, consulte Remover tags.

Alerta de máquinas com falha. O recurso de notificação e alertas proativos do Director foi aprimorado para incluir um novo alerta, Failed Machines (in %), que se baseia na porcentagem de máquinas com falha em um grupo de entrega. A nova condição de alerta permite que você configure 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 2023

Recursos novos e aprimorados

Publicação com plataformas de nuvem específicas usando o Citrix Provisioning no Image Portability Service. Fluxos de trabalho específicos para usar o Image Portability Service para publicar na AWS, Azure e Google Cloud já estão disponíveis. Além disso, as permissões necessárias para o Azure e a rede foram atualizadas. Para obter 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 no modo de manutenção. Agora você pode fazer isso em Full Configuration:

1. Use Search para localizar a máquina.
2. Verifique o motivo da manutenção em **Maintenance Reason** na guia **Details** no painel inferior. Ou passe o mouse sobre a coluna **Maintenance Mode**. As seguintes informações podem aparecer:

- By Administrator: colocado no modo de manutenção pelo administrador.
- Maximum Failed Registrations: colocado no modo de manutenção porque a máquina excedeu o máximo permitido de tentativas de registro.

Além disso, agora há também um filtro **Maintenance Reason** disponível. Você pode usá-lo para identificar as máquinas de destino.

O recurso é útil para que os administradores solucionem problemas com máquinas no modo de manutenção.

Use variáveis para notificar os usuários sobre o tempo restante antes de serem desconectados. Ao forçar a desconexão do usuário, agora você pode usar `%s%` ou `%m%` como variáveis para indicar o tempo específico na mensagem de notificação. Para expressar o tempo em segundos, use `%s%`. Para expressar o tempo em minutos, use `%m%`. Para obter mais informações, consulte Notificações de logoff do usuário.

Suporte para personalizar o comportamento de ativação em caso de falha na alteração do tipo de armazenamento. Ao ligar, o tipo de armazenamento de um disco gerenciado pode apresentar falha ao mudar para o tipo desejado devido a uma falha no Azure. Anteriormente, nesses cenários, a VM permanecia desligada e uma mensagem de falha era enviada para você. Com esse recurso, você pode optar por ligar a VM, mesmo quando o armazenamento não pode ser restaurado para o tipo configurado, ou optar por manter a VM desligada. Para obter mais informações, consulte Personalizar o comportamento de ativação em caso de falha na alteração do tipo de armazenamento.

Suporte para ativação da MAK. Agora você pode provisionar catálogos de máquinas persistentes e não persistentes com VMs ativadas por meio da Chave de Ativação Múltipla (MAK). Com esse recurso, agora o MCS também pode se comunicar com as VMs provisionadas. Essa implementação ajuda a ativar o sistema Windows sem perder contas de ativação. Para obter mais informações, consulte Ativação do licenciamento por volume.

Suporte para criptografia de disco do Azure no host. Com esse recurso, agora você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma especificação de modelo ou uma VM como entrada para um perfil de máquina. Para obter 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 pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta. Para obter mais informações, consulte Encryption at host - End-to-end encryption for your VM data.

Suporte ao modelo de instância do GCP como uma entrada para o perfil da máquina. Com esse recurso, agora você pode selecionar um modelo de instância do GCP como uma entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP, portanto, são muito econômicos. Para fazer isso, use os comandos do PowerShell. Para obter mais informações sobre como usar comandos do PowerShell para criar e atualizar catálogos de máquinas selecionando um modelo de instância do GCP, consulte Criar um catálogo de máquinas com perfil de máquina como 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 a partir do portal do Azure. Essa ação pode deixar o nome do grupo de segurança dinâmico do Azure AD fora de sincronia com o

grupo de segurança dinâmico associado a um catálogo de máquinas. Com esse recurso, agora você pode modificar o nome do grupo de segurança dinâmico do Azure AD associado a um catálogo de máquinas.

Essa modificação ajuda você a fazer com que as informações do grupo de segurança dinâmico do Azure AD armazenadas no objeto do pool de identidades do Azure AD sejam 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.

Adicionadas as permissões necessárias no GCP. Foram adicionadas as permissões necessárias para fazer o seguinte:

- Criar conexão de host
- Fazer o 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 de seus VDAs. As tentativas de login falham quando todas as seguintes condições são atendidas:

- O usuário está em um domínio diferente do VDA
- Não existe confiança entre os domínios
- O StoreFront está instalado no mesmo domínio do VDA

Anteriormente, sob essas 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 do usuário. Esse comportamento ainda pode ser configurado, se necessário. Para obter mais informações, consulte o parâmetro `CredentialForwardingToCloudAllowed` de Set-Brokersite no DaaS PowerShell SDK.

Março 2023

Recursos novos e aprimorados

Suporte para configurar a função e o escopo dos administradores. O Citrix Cloud agora oferece suporte com 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 esse aprimoramento, você pode selecionar uma função e depois combiná-la com o escopo de sua escolha.

Para obter mais informações, consulte Configurar o acesso personalizado para um administrador.

Suporte para criar um grupo de segurança dinâmico sob o grupo de segurança atribuído existente. Anteriormente, você podia criar grupos de segurança dinâmicos do Azure AD para um catálogo de máquinas. Com esse recurso, você também pode adicionar um grupo de segurança dinâmico do Azure AD em um grupo de segurança existente atribuído ao Azure AD. Você pode fazer o seguinte:

- Obter informações do grupo de segurança.
- Obter todos os grupos de segurança atribuídos ao Azure AD que são sincronizados a partir do servidor AD local ou dos 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 o grupo de segurança dinâmico do Azure AD como um membro do grupo atribuído do Azure AD.
- Remover a associação entre o grupo de segurança dinâmico do Azure AD e o grupo de segurança atribuído ao Azure AD quando o grupo de segurança dinâmico do Azure AD for excluído juntamente com o catálogo da máquina.

Para obter mais informações, consulte Criar um grupo de segurança dinâmico do Azure AD em um grupo de segurança existente atribuído ao Azure AD.

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 do 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). Ele 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. Quando você exclui 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 o requisito 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 aos grupos de segurança do Azure AD em Full Configuration. A opção **Azure AD security group** agora está disponível quando você cria VMs ingressadas no Azure AD. A opção permite que você adicione 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 das 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 das 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 das 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 esse recurso, agora você pode adicionar o parâmetro `ADAccountSid` para identificar as máquinas de forma exclusiva ao criar novas máquinas virtuais. Para obter mais informações, consulte Adicionar SIDs ao criar máquinas virtuais.

Capacidade de receber avisos associados aos catálogos MCS. Anteriormente, você não recebia nenhuma informação indicando que havia problemas com o seu catálogo de máquinas. Com esse recurso, agora você pode receber avisos para entender os problemas com seus catálogos do MCS e corrigir os problemas.

Os avisos, diferentemente dos erros, não fazem com que uma tarefa de provisionamento iniciada falhe.

Para receber avisos, use os comandos do PowerShell. Para obter mais informações, consulte Recuperar avisos associados a um catálogo.

Locatários compartilhados nas 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.

Removido o suporte para alterar o tipo de sistema operacional nos catálogos do Azure. Ao alterar as imagens do catálogo, somente imagens com o mesmo tipo de sistema operacional da imagem em uso são exibidas. Com esse aprimoramento, o Citrix DaaS não oferece mais suporte para alterar o tipo de sistema operacional dos catálogos do Azure após a criação do catálogo, ou seja, mudar o tipo de sistema operacional de Windows para Linux e vice-versa.

Fevereiro 2023

Recursos novos e aprimorados

Suporte para compartilhar imagens entre diferentes locatários do Azure. Anteriormente, em ambientes do Azure, você podia compartilhar imagens somente 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 disponível ao público em geral. 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 os recursos de visualização. Como administrador do Citrix Cloud com acesso total, agora você pode ativar ou desativar os recursos em Preview, em Full Configuration > Home, sem entrar em contato com a Citrix. Para obter mais informações, consulte Página inicial da interface Full Configuration.

Search Session Diagnostics with user name. Esse recurso permite o uso do Session Launch Diagnostics começando com o nome do usuário, caso você não tenha o ID da transação. Esse recurso é útil especificamente para administradores de help desk fazerem a triagem de 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 fazer a triagem em uma lista de sessões com falha que o usuário tentou iniciar nas últimas 48 horas. A página Session Launch Diagnostics mostra os detalhes da sessão que falhou. Ela lista o componente e o estágio exatos em que a falha ocorreu. Para obter mais informações, consulte o artigo Diagnóstico de início de sessão.

Implante aplicativos seguros da Web e SaaS com o Secure Private Access. Na guia **Full Configuration > Applications > Applications**, a nova opção **Add Web/SaaS Applications** agora está disponível na barra de ações. A opção permite que você implante aplicativos seguros da Web e SaaS com o Secure Private Access. O Citrix Secure Private Access fornece uma maneira fácil e flexível para usuários remotos acessarem aplicativos baseados na web, SaaS e cliente-servidor usando uma abordagem de Confiança Zero. Ele permite o logon único em aplicativos web e SaaS, além de controles de segurança granulares, como marcas 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 dos seus usuários. Consulte Citrix Secure Private Access.

Filtrar conteúdo de log por um período de tempo específico. Uma nova opção, **Custom**, agora está disponível na lista de duração em **Full Configuration > Logging > Events**. Use para especificar um período de eventos para os quais você deseja filtrar sua pesquisa. Para obter mais informações, consulte Log de configuração.

Atualizações no AutoScale. Atualizamos a opção **Control when Autoscale starts powering on tagged machines** para facilitar o entendimento. A opção controla quando o AutoScale começa a ligar as máquinas marcadas com base na porcentagem da capacidade restante das máquinas não 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. Para obter mais informações, consulte Máquinas marcadas com tag no AutoScale (intermitência da nuvem).

Políticas do App Protection. Agora você pode ativar o App Protection ao criar ou editar um grupo de entrega. Isso fornece recursos anti-keylogging e de proteção contra captura de tela para as 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 das CPUs AMD Radeon Instinct MI25 e AMD EPYC 7V12(Rome) em Monitor. O Monitor já suporta as 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 do decodificador para solucionar problemas relacionados à GPU em VDAs com SO multissessão ou de sessão única. Os gráficos de utilização da GPU AMD estão disponíveis somente para VDAs executando Windows e Citrix Virtual Apps and Desktops 7 2212 de 64 bits ou posterior. Para obter mais informações, consulte Utilização de GPU.

Suporte para agendar atualizações de configuração no Azure. Em ambientes do Azure, agora você pode agendar um intervalo de tempo para as atualizações de configuração das máquinas existentes provisionadas pelo MCS usando o comando PowerShell `Schedule-ProvVMUpdate`. Qualquer ativação ou reinicialização durante o horário programado aplica uma atualização programada do esquema de provisionamento a uma máquina. Você também pode cancelar a atualização da configuração antes do horário agendado usando `Cancel-ProvVMUpdate`.

Você pode agendar e cancelar a atualização da configuração de:

- Uma ou várias VMs
- Um catálogo inteiro

Para obter mais informações, consulte Agendar atualizações de configuração.

Suporte para usar imagens prontas da 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 somente o fluxo de trabalho de perfil de máquina para esse recurso. Para obter mais informações, consulte Google Cloud Marketplace.

Limitar o escopo de grupos de hosts na Conexão de Host SCVMM. Anteriormente, a conexão do host ao SCVMM exigia que o administrador tivesse um único grupo de hosts de nível superior configurado. Isso implica que o administrador tinha visibilidade de todos os grupos de hosts, clusters ou hosts abaixo do único grupo de hosts de nível superior. Com esse recurso, em grandes implantações em que um único SCVMM gerencia vários clusters em diferentes data centers, agora você pode limitar o escopo dos grupos de hosts dos administradores. Para isso, você pode usar a função de administrador delegado no console do Microsoft System Center Virtual Machine Manager (VMM) para selecionar os grupos de hosts 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 esse 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 o armazenamento com redundância de zona.

Janeiro 2023

Recursos novos e aprimorados

Opção para fazer downgrade do disco de armazenamento para HDD Standard quando as VMs são desligadas. Uma nova opção **Enable storage cost saving** agora está disponível na página **Disk Settings** quando você cria ou atualiza catálogos do Azure. A opção economiza nos custos de armazenamento ao fazer o downgrade para HDD Standard do disco de armazenamento e do disco de cache de write-back quando a VM é desligada. A VM muda para suas configurações originais na reinicialização. Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.

Suporte para configurar o roaming de sessão em Full Configuration. Anteriormente, o PowerShell era a sua única opção para configurar o roaming de sessão para aplicativos e áreas de trabalho. Agora você pode fazer isso em **Full Configuration**. Para obter mais informações, consulte Gerenciar grupos de entrega.

Algumas ações renomeadas para melhor alinhá-las a seus significados reais. Renomeamos as seguintes ações em **Full Configuration > Machine Catalogs** e **Full Configuration > Delivery Groups**. Os fluxos de trabalho para realizar essas ações permanecem inalterados.

- **Update Machines** renomeado para **Change Master Image**
- **Rollback Machine Update** renomeado para **Roll Back Master Image**
- **Upgrade Catalog** renomeado para **Change Functional Level**
- **Upgrade Delivery Group** renomeado para **Change Functional Level**
- **Undo Upgrade Catalog** renomeado para **Undo Functional Level Change**
- **Undo Upgrade Delivery Group** renomeado para **Undo Functional Level Change**

Suporte para organizar grupos de aplicativos usando pastas. Agora você pode criar pastas aninhadas para organizar grupos de aplicativos e 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 áreas de trabalho para um grupo de entrega, você podia especificar somente 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 você deseja bloquear. Esse aprimoramento é útil quando você adiciona um grupo de usuários a uma lista de permissão e, ao mesmo tempo, deseja bloquear um subconjunto dos usuários na lista de permissão. Para obter mais informações, consulte Criar grupos de entrega.

Acesso ao Citrix Analytics for Performance –Detalhes da sessão em Monitor. A página Session Details do Citrix Analytics for Performance agora está integrada a Monitor. Clique em **View Session Timeline** na página Sessions em Monitor para exibir a página Sessions Details do Citrix Analytics for Performance em Monitor. Isso exige que você tenha um direito válido do Citrix Analytics for Perfor-

mance. Session Details está disponível para sessões categorizadas como Excellent, Fair ou Poor no Citrix Analytics for Performance.

Você pode ver uma tendência da experiência da sessão até os últimos três dias, juntamente com os fatores que contribuem para a experiência. Essas informações complementam os dados disponíveis em Monitor em tempo real usados pelo administrador do suporte técnico para solucionar problemas relacionados à experiência da sessão.

Para obter mais informações, consulte o artigo Análise do site.

As VMs não persistentes são excluídas dos hipervisores ou dos serviços em nuvem quando você as exclui ou exclui seus catálogos de máquinas em Full Configuration. A opção de reter VMs em hipervisores ou serviços em nuvem agora está disponível somente para VMs persistentes. Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Dezembro 2022

Recursos novos e aprimorados

Suporte para criar catálogos ingressados no Azure AD , ingressados no Hybrid Azure AD e habilitados pelo Microsoft Intune com VMs mestre ingressadas no Azure AD. Agora você pode criar catálogos ingressados no Azure AD , ingressados no Hybrid Azure AD e habilitados pelo Microsoft Intune com VMs mestre ingressadas no Azure AD, ingressadas no Hybrid Azure AD e não ingressadas no domínio. Se você quiser gerenciar uma VM mestre pelo Microsoft Intune, use o VDA versão 2212 ou posterior e não pule a preparação de imagens ao criar ou atualizar catálogos de máquinas.

Para obter mais informações sobre identidades de máquinas, consulte Ingressado no Azure Active Directory, Microsoft Intune e Ingressado no Azure Active Directory híbrido.

Suporte no MCS para excluir objetos da VM sem acessar o hipervisor. Agora você pode excluir objetos da VM no MCS sem ter acesso ao hipervisor. Ao excluir uma VM ou um esquema de provisionamento, o MCS precisa remover as marcas para que os recursos não sejam mais rastreados ou identificados. Anteriormente, se o hipervisor não pudesse ser acessado, as falhas na remoção da marca eram ignoradas. Com esse recurso, se o hipervisor não estiver acessível durante o uso do comando `Remove-ProvVM`, a remoção da marca 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 2022

Recursos novos e aprimorados

Suporte para entregar aplicativos MSIX e de anexação de aplicativo MSIX. Em **Full Configuration > App Packages**, agora você pode carregar aplicativos empacotados MSIX e de anexação de aplicativo MSIX no Citrix Cloud e depois entregá-los aos seus usuários. Para obter mais informações, consulte Pacotes de aplicativos.

Aviso de versões VDA e níveis funcionais não compatíveis. A interface Full Configuration agora alerta você sobre versões VDA e níveis funcionais não suportados. Para evitar possíveis problemas:

- Se uma máquina executar uma versão de VDA não suportada, você será solicitado a fazer o upgrade para uma versão compatível.
- 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 estendidas para a criação do catálogo. Quando criar um catálogo MCS em **Full Configuration**, agora você pode anotar sua imagem mestre. Para obter mais informações, consulte Imagem mestre.

Suporte para exportar dados de atribuição de área de trabalho em Full Configuration. Ao exibir as atribuições de área de trabalho de um grupo de entrega com SO de sessão única, agora você pode exportar os dados da atribuição para um arquivo CSV para fins de auditoria. Para fazer isso, selecione o grupo de entrega em **Full Configuration > Delivery Groups**, vá para a guia **Desktops** e clique em **Export** no canto superior esquerdo da guia.

As guias All Applications e Application Folders consolidadas em uma. Em **Full Configuration > Applications**, as guias **All Applications** e **Application Folders** foram consolidadas em uma guia, **Applications**. Essa alteração unifica a experiência do usuário de gerenciamento de exibições de pastas em todos os nós de Full Configuration.

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 nos custos de armazenamento mudando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade `StorageTypeAtShutdown` personalizada. 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 para o 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 exibição Filters. A página Filters em Monitor foi atualizada para incluir listas separadas de filtros salvos e padrão para melhor visualização e acessibilidade aos filtros. Você pode selecionar uma exibição entre máquinas, sessões, conexões ou instâncias de aplicativos. Em seguida, você pode selecionar um filtro nas listas Saved Filters ou Default Filters para exibir a lista de dados filtrada. Você pode usar as listas suspensas para refinar os critérios de filtragem ou editar os critérios existentes. Você pode salvar o seu filtro na lista Saved Filter. Para obter mais informações, consulte o artigo Filtros.

Capacidade de redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. Em ambientes de virtualização VMware, agora você pode usar o comando do PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. O recurso automatiza o processo de redefinição do disco do sistema operacional. Por exemplo, ele ajuda na redefinição da VM para o seu status inicial de catálogo de área de trabalho de desenvolvimento persistente criado usando o MCS.

Para obter mais informações sobre como usar o comando do PowerShell para redefinir o disco do sistema operacional, consulte Redefinir disco do sistema operacional.

Suporte para atualização do perfil da máquina e propriedades personalizadas adicionais das máquinas provisionadas pelo MCS em ambientes do Azure. Anteriormente, em ambientes do Azure, você podia usar `Request-ProvVMUpdate` para atualizar a propriedade personalizada `ServiceOffering` de uma máquina provisionada pelo 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 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 do hardware são capturadas da VM da imagem mestre ou do instantâneo.

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 pelo MCS em ambientes GCP. Em ambientes GCP, `Set-ProvScheme` altera o modelo (esquema de provisionamento) e não afeta as máquinas existentes. Usando o comando `Request-ProvVMUpdate` do PowerShell, 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 esse recurso é o perfil da máquina. Para obter mais informações, consulte Atualizar máquinas provisionadas usando o PowerShell.

Outubro 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 em que você deseja usar um início confiável para melhorar a segurança 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 e facilitar o acesso. Para obter mais informações, consulte Organizar grupos de entrega usando pastas.

Suporte para agendar uma reinicialização única de máquinas em Full Configuration. Uma nova opção, **Once**, agora está disponível quando você cria agendamentos de reinicialização para grupos de entrega. Com essa opção, você pode programar máquinas em um grupo de entrega para reiniciarem uma vez, em uma data e hora especificadas. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Programação avançada de investigação. A programação aprimorada de investigação de aplicativos e áreas de trabalho agora pode ser feita no Monitor. Usando esse recurso, o Citrix Probe Agent pode ser configurado para executar as tarefas de investigação (sondagem) em dias específicos da semana e repetidas em intervalos específicos durante o dia. Isso permite que você programe uma única tarefa de investigação para ser repetida em horários específicos do dia e da semana. Agora você pode verificar proativamente a integridade do seu site com investigações configuradas para serem executadas regularmente em horários adequados. Esse recurso simplifica a configuração e o gerenciamento da investigação em Monitor. Para obter mais informações, consulte Investigação de aplicativo e área de trabalho.

Setembro 2022

Recursos novos e aprimorados

As versões mais antigas do Remote PowerShell SDK agora estão preteridas. Se você estiver usando uma versão preterida, o SDK para de funcionar e você vê uma mensagem de erro solicitando baixar a versão atual. Se isso acontecer, baixe o Remote PowerShell SDK mais recente no site da Citrix.

Catálogos de máquinas com início confiável no Azure. Em ambientes Azure, você pode criar catálogos de máquinas habilitados com o início confiável e usar a propriedade `SupportsTrustedLaunch` do inventário da VM para determinar os tamanhos de VM que suportam o início confiável.

O início confiável é uma excelente maneira de melhorar a segurança das VMs de 2ª geração. O início confiável protege contra técnicas de ataque avançadas e persistentes. Para obter mais informações, consulte Catálogos de máquinas com início confiável.

Suporte para identificar recursos do Microsoft System Center Virtual Machine Manager criados pelo MCS. Agora você pode identificar os recursos do Microsoft System Center Virtual Machine Manager (SCVMM) criados pelo MCS usando marcas. Para obter mais informações sobre as marcas que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para identificar recursos do VMware criados pelo MCS. Agora você pode identificar os recursos do VMware criados pelo MCS usando marcas. Para obter mais informações sobre as marcas que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para otimizar a limitação do AWS Workspace. Agora você pode ligar e desligar um grande número de máquinas no AWS Workspace sem ter problemas de limitação. Os problemas de limitação ocorrem quando o número de solicitações enviadas ao AWS Workspace excede o número de solicitações que o servidor pode processar. Portanto, a Citrix agora agrupa várias solicitações em uma única solicitação antes de enviá-las para o SDK do AWS Workspace.

Capacidade de verificar os detalhes da máquina ao visualizar a contagem de máquinas na tela inicial. Ao visualizar a contagem de máquinas por estado de disponibilidade na **página inicial**, agora você pode clicar em um estado para ver os detalhes das máquinas nesse estado. Para obter mais informações, consulte Página inicial da interface Full Configuration.

Suporte para criação de catálogo de máquinas usando uma imagem de uma assinatura diferente no mesmo locatário do Azure. Anteriormente, em ambientes do Azure, você só podia selecionar uma imagem na sua assinatura para criar um catálogo de máquinas. Com esse recurso, agora você pode selecionar uma imagem na Galeria de Computação do Azure (anteriormente Galeria de Imagens Compartilhadas) que pertence a uma assinatura compartilhada diferente para criar e atualizar catálogos MCS.

Para obter mais informações sobre como criar um catálogo, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Para obter informações sobre como compartilhar imagens com outra entidade de serviço no mesmo locatário, consulte Compartilhamento de imagem com outra entidade de serviço no mesmo locatário.

Para obter informações sobre os comandos do PowerShell para selecionar uma imagem de uma assinatura diferente, consulte Usar o 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 2022

Recursos novos e aprimorados

Suporte para identificar recursos do Citrix Hypervisor criados pelo MCS. Agora você pode identificar os recursos do Citrix Hypervisor criados pelo MCS usando marcas. Para obter mais informações sobre as marcas que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para usar grupos de hosts e zonas de disponibilidade do Azure ao mesmo tempo. Em ambientes do 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 hosts. A criação do catálogo falhará se a propriedade personalizada da zona de disponibilidade não corresponder à zona do grupo de hosts.

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.
As zonas de disponibilidade do Azure são localizações separadas fisicamente em cada região do Azure que são tolerantes a falhas locais.

Para obter mais informações sobre as várias combinações de zona de disponibilidade e zona do grupo de hosts que resultam em sucesso ou falha na criação do catálogo de máquinas, consulte Usar grupos de hosts 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 com esse novo ID de pasta. Se essa propriedade não for especificada no `CustomProperties`, as VMs serão criadas na pasta em que a imagem mestre está localizada. Para obter mais informações sobre como atualizar o 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 **Date and time**. Para obter mais informações, consulte Configuração de fuso horário.

O Image Portability Service (IPS) agora oferece suporte para Amazon Web Services (AWS). Ao configurar as permissões e os componentes necessários para a AWS, os fluxos de trabalho IPS podem ser usados com uma conta da 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 do Azure. Em ambientes do Azure, agora você pode evitar possíveis confusões com o local do arquivo de paginação. Para isso, o MCS agora determina o local do arquivo de paginação quando você cria o esquema de provisionamento durante a preparação da imagem. Esse 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 dissociar a preparação da imagem da criação do esquema de provisionamento, o MCS determina corretamente o local do arquivo de paginação. Para obter mais informações sobre a localização do arquivo de paginação, consulte Localização do arquivo de paginação.

Suporte para atualizar a configuração do arquivo de paginação em ambientes do Azure. Ao criar um catálogo em um ambiente do Azure, agora você pode especificar a configuração do arquivo de paginação, incluindo sua localização e o tamanho, usando comandos do 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 da 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 Get Started agora tem uma nova aparência. Outras atualizações à página inicial incluem:

- Ícones de Atualizar e Ajuda recém-adicionados no canto superior direito.
- Contagens de recursos clicáveis, fornecendo acesso rápido às páginas dos recursos relevantes.
- Aprimoramento do ícone de 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 do modelo ARM como um perfil de máquina para criar um catálogo de máquinas, agora você pode adicionar extensões de

VM do Azure às máquinas virtuais no catálogo, exibir a lista de extensões suportadas e remover as extensões adicionadas. As extensões de VM do Azure são pequenos aplicativos que fornecem tarefas de configuração e automação pós-implantação nas VMs do Azure. Por exemplo, se uma VM exigir 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 as extensões de VM do Azure, consulte Usar o PowerShell para habilitar extensões de VM do Azure.

Suporte para início confiável para disco de SO efêmero. Agora você pode criar esquemas de provisionamento usando o disco de SO efêmero no Windows com início confiável. O início confiável é uma excelente maneira de melhorar a segurança das VMs de 2ª geração. Ele protege contra técnicas de ataque avançadas e persistentes combinando tecnologias que podem ser habilitadas de forma independente, como inicialização segura e versão virtualizada do Trusted Platform Module (vTPM). Para obter mais informações sobre como criar um catálogo de máquinas, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Julho 2022

Recursos novos e aprimorados

Tempos limite de sessão dinâmica para máquinas com SO de sessão única. Os tempos limite de sessão dinâmica agora oferecem suporte a máquinas com SO de sessão única. É necessário um grupo de entrega com pelo menos um VDA da versão 2206 ou posterior. Certifique-se de que os VDAs tenham se registrado no Citrix Cloud pelo menos uma vez. Para obter mais informações, consulte Tempo limite de sessão dinâmica.

Enviar lembretes de logoff sem forçar o logoff do usuário no AutoScale. Um novo recurso agora está disponível em **User Logoff Notifications** (anteriormente **Force User Logoff**) no AutoScale. O recurso permite enviar lembretes de logoff aos usuários sem forçá-los a fazer logoff. Isso evita a possível 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 sistema operacional Linux ao criar catálogos de VMs do Linux no Azure. Usando a interface Full Configuration, agora você pode escolher o tipo de licença Linux OS ao criar catálogos de VMs do Linux no Azure. Você tem duas opções de BYO (traga a sua própria) do Linux: Red Hat Enterprise Linux e SUSE Linux Enterprise Server. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Experiência de pesquisa aprimorada em Full Configuration. O nó de pesquisa fornece os seguintes novos recursos e aprimoramentos:

- **Capacidade de exportar resultados da pesquisa**. Agora você pode exportar os resultados da pesquisa. Para isso, clique no ícone de exportação no canto superior direito.

- **Novo filtro disponível**. O filtro Pending Power Action agora está disponível para uso. Use o filtro para refinar sua pesquisa.
- **Suporte para a pesquisa de "Does not contain"para determinados itens**. Itens como nomes de máquinas e marcas agora suportam critérios de pesquisa "Does not contain".
- **Suporte para pesquisar objetos ao adicionar filtros**. Quando adiciona filtros para os seguintes objetos, você agora pode pesquisar conexões, catálogos de máquinas, grupos de entrega, grupos de aplicativos e marcas.

Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Suporte para perfis de armazenamento VMware. Ao criar um catálogo de máquinas usando uma imagem mestre em um vSAN Datastore, 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 RestrictedKrbHost SPN. Todas as contas de computador criadas pelo Citrix MCS agora são registradas com o SPN (Service Principal Names) `RestrictedKrbHost`. Isso evita a necessidade de executar o comando `setspn` para registrar o SPN para as contas de computador depois que o MCS as cria.

App Packages em Full Configuration para entrega de aplicativos em pacotes da Microsoft. O nó App-V foi renomeado App Packages e reprojetado para acomodar mais tipos de aplicativos empacotados da Microsoft. Anteriormente, era necessário 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 App Packages. Para obter mais informações, consulte Pacotes de aplicativos.

Suporte para usar as especificações do modelo ARM como perfis de máquina. Anteriormente, você podia usar apenas VMs como perfis de máquina. Agora você também pode usar as especificações do modelo ARM como perfis de máquina ao criar catálogos de máquinas do Azure. Esse recurso permite que você aproveite os recursos do modelo Azure ARM, como controle de versão. Para garantir que a especificação selecionada seja configurada corretamente e contenha as configurações necessárias, realizamos a validação nela. Se a validação falhar, você é solicitado a selecionar um perfil de máquina diferente. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Suporte para validar as especificações do modelo ARM. Agora você pode validar a especificação do modelo ARM para garantir que ela possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Há duas maneiras de validar a especificação do modelo ARM:

- Usando a interface de gerenciamento Full Configuration.
- Usando o comando do PowerShell.

Para obter mais informações sobre como validar a especificação do modelo ARM, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Junho 2022

Recursos novos e aprimorados

Suporte a agendamento de reinicialização para máquinas com SO de sessão única. Anteriormente, o recurso de agendamento de reinicialização estava disponível somente para máquinas com SO multissessão. Agora também está disponível para máquinas com SO de sessão única. Agora você pode criar agendamentos de reinicialização para grupos de entrega contendo máquinas com SO de sessão única. Para obter mais informações, consulte Criar e gerenciar agendamentos de reinicialização de máquinas em um grupo de entrega.

Opção para realizar verificações prévias de nome de usuário. A opção **Check name** agora está disponível quando você insere as credenciais do 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 do domínio. Se a verificação for aprovada, o nome de domínio é preenchido automaticamente.

Para obter mais informações, consulte Credenciais de domínio.

Capacidade de alterar a configuração de rede de 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 se certificar de que as sub-redes estejam sob a mesma unidade de hospedagem. Para obter mais informações, consulte Alterar a configuração de rede de um esquema de provisionamento existente.

Recupere informações de nome de região de VMs do Azure, discos gerenciados, instantâneos, VHD do Azure e modelo ARM. Agora você pode exibir informações de nome de região de uma VM do Azure, discos gerenciados, instantâneos, VHD do Azure e modelo ARM. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Para obter mais informações, consulte Recupere informações de nome de região de 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 da propriedade

de especificação do modelo ARM ou da VM, o que for usado como perfil de máquina, se os valores não estiverem explicitamente definidos nas propriedades personalizadas. As propriedades afetadas por esse recurso são:

- Zona de disponibilidade
- ID do grupo de hosts dedicados
- ID do conjunto de criptografia de disco
- Tipo de sistema operacional
- Tipo de licença
- Oferta de serviço
- Tipo de armazenamento

Se algumas das propriedades estiverem ausentes no perfil da máquina e não estiverem definidas nas propriedades personalizadas, o valor padrão das propriedades será usado sempre que aplicável. Para obter mais informações, consulte Usar valores de propriedade do perfil da máquina.

Suporte estendido para atualização do VDA. Usando a interface Full Configuration, agora você pode atualizar máquinas persistentes provisionadas pelo MCS. Você pode fazer o upgrade por catálogo ou por máquina. Para obter mais informações, consulte Atualizar VDAs usando a interface Full Configuration.

Citrix Probe Agent nos planos de controle do Citrix Cloud Japan e Citrix Cloud Government. Agora, o Citrix Probe Agent é compatível com sites hospedados nos planos de controle do Citrix Cloud Japan e Citrix Cloud Government. Para usar o agente de investigação nesses planos, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 2 para Japan e 3 para a região Government. O Citrix Probe Agent automatiza o processo de verificação da integridade de aplicativos e áreas de trabalho virtuais publicados em um site. Para obter mais informações, consulte Investigação de aplicativo e área de trabalho.

Personalização da 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 de acordo com os seus requisitos de segurança específicos. Esse recurso é útil se sua equipe de segurança não permitir que a porta padrão (porta 80) seja aberta ou se a porta padrão já estiver em uso. Para obter mais informações, consulte Personalizar a porta para comunicação com os Cloud Connectors.

Suporte para organizar 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 de que você precisa para implantar VMs. Para obter mais informações sobre os novos recursos compatíveis com o SCVMM 2022, consulte Novidades no System Center Virtual Machine Manager.

Suporte para configurar o parâmetro de operações simultâneas de provisionamento máximas na AWS. O Citrix DaaS agora oferece suporte `MaximumConcurrentProvisioningOperations` como uma propriedade personalizada configurável para o MCS na AWS. `MaximumConcurrentProvisioning` é a propriedade que determina o número de VMs que você pode criar ou excluir simultaneamente. Embora o MCS ofereça suporte a, no máximo, 100 operações de provisionamento simultâneas por padrão, agora você pode inserir comandos do PowerShell para personalizar esse valor. Você pode inserir um intervalo de 1 a 1000. Definir essa propriedade com o seu valor preferido permite controlar o número de tarefas paralelas que podem ser executadas ao criar ou excluir VMs. Para obter detalhes sobre como configurar o máximo de operações de provisionamento simultâneas, consulte Valores padrão de conexão do host.

Maio 2022

Recursos novos e aprimorados

Diagnóstico aprimorado de início de sessão. O Citrix DaaS agora oferece suporte a um diagnóstico detalhado de falha de início de sessão. Agora você pode exibir os componentes envolvidos na sequência de início da sessão. Os componentes que falharam com os últimos códigos de erro gerados são realçados. Isso ajuda a identificar o motivo exato de uma falha no início de uma sessão e a tomar a ação recomendada.

A página Transaction é estendida com o painel Transaction Details que contém uma lista de componentes que indicam a ocorrência do erro. Clicar no nome do componente exibe os detalhes em Component Details e Last Known Failure Details. O motivo da falha e o código de erro são exibidos. Clicar no link Learn more leva ao código específico em Error codes, que contém uma descrição detalhada e uma 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 ignorar a ativação do DHCP durante a preparação da imagem usando esse comando. Veja a seguir uma lista de configurações compatíveis com `Set-ProvServiceConfigurationData`:

- Mudar tempo limite de preparação de imagem: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Ignorar ativação de DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPr -Value EnableDHCP`
- Ignorar Microsoft Windows KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Ignorar Microsoft Office KMS Rearm: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps`


```
-Value OfficeRearm
```

- Desativar preparação do desligamento automático da VM:
  ```
  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 do PowerShell. Usando comandos do PowerShell, você pode definir o tipo de licença Linux ao criar catálogos de máquinas Linux. Você tem duas opções de licenças BYO (traga a sua própria) Linux: RHEL_BYOS e SLES_BYOS. A configuração é padronizada com o licenciamento do Azure Linux. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de 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 de SO, NIC, VM e assim por diante, que estão associados a um ProvScheme usando uma marca chamada `provschemeID`. Para obter mais informações sobre as marcas que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para provisionamento de Azure Stack HCI por meio do SCVMM. O MCS agora oferece suporte ao provisionamento do Azure Stack HCI por meio do Microsoft System Center Virtual Machine Manager (SCVMM). Você pode gerenciar o cluster do Azure Stack HCI com suas ferramentas existentes, incluindo o SCVMM. Para obter mais informações, consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Suporte para adicionar usuários que não são do Active Directory manualmente. Usando a interface de gerenciamento Full Configuration, agora você pode inserir uma lista de nomes de usuário separados por ponto e vírgula ao adicionar usuários que não são do 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 catálogos de máquinas.

Abril 2022

Recursos novos e aprimorados

Página inicial da interface Full Configuration. A interface Full Configuration agora tem uma página inicial que fornece uma visão geral da implantação e das cargas de trabalho do Citrix DaaS, além de

informações que ajudam você a aproveitar ao máximo a sua assinatura. A página compreende as seguintes partes:

- **Service overview**. Fornece uma visão geral da implantação e das cargas de trabalho do Citrix DaaS.
- **Recommendations**. Recomenda recursos que estão disponíveis com a sua assinatura e coleta o seu feedback.
- **What's new**. Mostra os recursos mais recentes.
- **Preview features**. Mostra os recursos que estão atualmente na versão Preview.
- **Get started**. Mostra as etapas para orientá-lo durante a configuração inicial.

Para obter mais informações, consulte Página inicial.

Exibição do progresso de criação e atualizações do catálogo. Agora, a Full Configuration permite que você se mantenha atualizado sobre a criação e as atualizações do catálogo. Você pode obter uma visão geral do processo de criação e atualização, visualizar o histórico das etapas executadas e monitorar o andamento e o tempo de execução da etapa atual. Para obter mais informações, consulte Comece a criar o catálogo.

Exibir hipervisores e serviços em nuvem disponíveis com base na zona selecionada. Em Full Configuration, ao criar conexões de hospedagem, você precisa selecionar uma zona antes de selecionar um tipo de conexão. A lista suspensa de tipos de conexão exibe os hipervisores e serviços em nuvem disponíveis com a zona. Anteriormente, para garantir que a lista de tipos de conexão mostrasse um hipervisor ou serviço de nuvem necessário, era preciso instalar o seu plug-in em todas as zonas. Com essa nova sequência de configuração, agora você pode instalar o plug-in somente na zona necessária.

Você também pode usar o comando do 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 ingressados no AD no local em Full Configuration. Um novo campo, **Select identity type**, está disponível nas interfaces em que você atribui usuários a áreas de trabalho 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 nos ambientes Google Cloud Platform (GCP) e Azure. Agora você pode evitar possíveis confusões se as propriedades personalizadas definidas em `New-ProvScheme` e `Set-ProvScheme` não entrarem em vigor. Se você

especificar propriedades personalizadas não existentes, receberá uma mensagem de erro. Para obter mais informações, consulte Consideração importante sobre a configuração de propriedades personalizadas.

Suporte para criar máquinas ingressadas no Azure Active Directory. Em **Full Configuration**, quando você cria um catálogo, o tipo de identidade **Azure Active Directory joined** fica disponível em **Machine Identities**. Com esse tipo de identidade, você pode usar o MCS para criar máquinas ingressadas no Azure Active Directory. Você também tem uma opção extra, **Enroll the machines in Microsoft Intune**, para registrar as máquinas no Microsoft Intune para gerenciamento.

Para obter informações sobre como criar catálogos ingressados no Azure Active Directory, consulte Criar catálogos de máquina. Para obter informações sobre requisitos e considerações relacionadas ao ingresso no Azure Active Directory, consulte Ingressado no Azure Active Directory.

Suporte para criar máquinas ingressadas no Azure Active Directory híbrido. Em **Full Configuration**, quando você cria um catálogo, o tipo de identidade **Hybrid Azure Active Directory joined** fica disponível em **Machine Identities**. Com esse tipo de identidade, você pode usar o MCS para criar máquinas ingressadas no Azure Active Directory híbrido. Essas máquinas são pertencentes a uma organização e conectadas com uma conta do Active Directory Domain Services que pertence à organização.

Para obter informações sobre como criar catálogos ingressados no Azure Active Directory híbrido, consulte Criar catálogos de máquinas. Para obter informações sobre requisitos e considerações relacionadas ao ingresso no Azure Active Directory híbrido, consulte Ingressado no Azure Active Directory híbrido.

Suporte ao início confiável do Azure para instantâneos. Além das imagens, o início confiável do Azure agora também está disponível para instantâneos. Se você selecionar um instantâneo com o início confiável ativado, fica obrigatório o uso de um perfil de máquina. Além disso, você precisa selecionar um perfil de máquina com início confiável ativado. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Exportar máquinas. Agora você pode exportar máquinas listadas na página **Machines** do assistente **Machine Catalog Setup** para um arquivo CSV, para ser usado como modelo ao adicionar máquinas a um catálogo em massa. Para obter mais informações, consulte Exportar máquinas de um catálogo.

Opção para acessar o console da web do Workspace Environment Management. A opção Environment Management (Web) agora está disponível no menu da guia **Manage**. A opção leva você ao novo console do Workspace Environment Management na Web. Para acessar o console legado, use **Environment Management**. Estamos migrando o conjunto completo de funcionalidades do console legado para o console da web. O console da web geralmente responde mais rápido do que o console legado. Para obter mais informações, consulte Serviço Workspace Environment Management.

Capacidade de gerenciar parâmetros do ProvScheme. Quando usar o MCS para criar um catálogo, agora você recebe um erro se definir os parâmetros `New-ProvScheme` em hipervisores não suporta-

dos durante a criação do catálogo de máquinas ou atualizar os parâmetros `Set-ProvScheme` após os catálogos de máquinas serem criados. Para obter mais informações, consulte Criar catálogos de máquinas.

Limites maiores de localização do recurso. Os limites de localização do recurso para VDAs de sessão única e VDAs multissessão agora aumentaram para 10.000 e 1.000, respectivamente. Para obter mais informações, consulte Limites.

Suporte para reiniciar máquinas sem gerenciamento de energia após o esvaziamento de todas as sessões. O Citrix DaaS agora permite criar agendamentos de reinicialização para máquinas que não têm gerenciamento de energia depois que todas as sessões são esvaziadas das máquinas. Na interface Full Configuration, selecione **Restart all machines after draining all sessions** em **Restart duration**. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Suporte para upgrade de máquinas VDA (preview). Usando a interface Full Configuration, agora você pode fazer o upgrade de máquinas VDA na sua implantação do Citrix DaaS. Você pode fazer o upgrade por catálogo ou por máquina. O recurso se aplica a máquinas que não são criadas usando o MCS (por exemplo, máquinas físicas). Para obter mais informações, consulte Atualizar VDAs usando a interface Full Configuration.

As máquinas não são desligadas durante as interrupções. O Citrix DaaS agora impede que as máquinas virtuais sejam desligadas pelo agente quando a zona em que as máquinas se encontrarem sofrer uma interrupção. As máquinas ficam automaticamente disponíveis para conexões quando a interrupção termina. Você não precisa fazer nada para disponibilizar as máquinas após a interrupção.

Diagnóstico de início de sessão. O Citrix DaaS agora oferece suporte a um diagnóstico aprimorado de falha de início 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, o serviço Citrix Director) para determinar o componente e o estágio exatos em que o problema ocorreu e aplicar as ações recomendadas para resolver o problema. Para obter mais informações, consulte Diagnóstico de início de sessão.

Opção de acesso ao serviço Session Recording. A opção Session Recording agora está disponível no menu da guia **Manage**. A introdução do serviço Session Recording fornece gerenciamento centralizado de políticas, reprodução e configurações de servidor. Ele alivia a carga sobre os administradores de TI fornecendo um ponto de entrada unificado para gerenciar e observar os objetos distribuídos em toda a organização. Para obter mais informações, consulte Serviço Session Recording (preview).

Nova denominação do Citrix Virtual Apps and Desktops Service. O **Citrix Virtual Apps and Desktops Service** foi renomeado **Citrix DaaS**. Saiba mais sobre a mudança de nome no anúncio em nosso blog.

As seguintes ofertas de serviços do Citrix Virtual Apps and Desktops Service foram renomeadas.

- **Citrix Virtual Apps service Advanced** foi renomeado **Citrix DaaS Advanced**.
- **Citrix Virtual Apps service Premium** foi renomeado **Citrix DaaS Premium**.

- **Citrix Virtual Desktops service** foi renomeado **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Advanced** foi renomeado **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Premium** agora está disponível como **Citrix DaaS Premium e Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard for Azure** foi renomeado **Citrix DaaS Standard for Azure**.
- **Citrix Virtual Apps and Desktops Standard for Google Cloud** foi renomeado **Citrix DaaS Standard for Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium for Google Cloud** foi renomeado **Citrix DaaS Premium for Google Cloud**.

Implementar essa transição em nossos produtos e em sua documentação é um processo contínuo. Agradecemos a sua paciência durante esta 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 antigos para evitar a quebra de scripts de clientes existentes.
- A documentação do produto relacionada e outros recursos (como vídeos e postagens de blog) que estão vinculados a partir da documentação deste produto ainda poderão conter nomes antigos.

> **Nota:**
>
> O nome do produto **Citrix Virtual Apps and Desktops** no local permanece o mesmo.

Suporte ao locatário em Full Configuration. Agora você pode criar partições de configuração em uma única instância do Citrix DaaS. Você faz isso criando escopos de locatário em **Administrators > Scopes** 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 somente os objetos associados ao locatário. Esse recurso é útil, por exemplo, se sua organização:

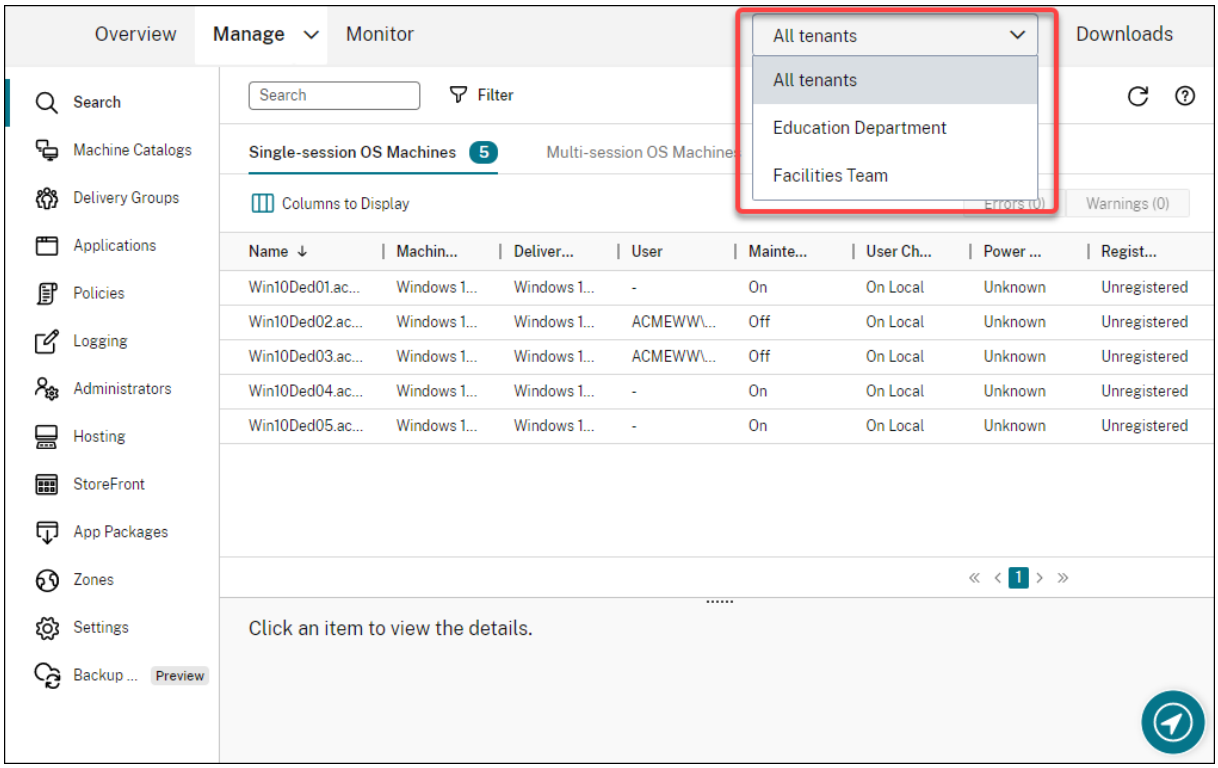
- Tem diferentes silos de negócios (divisões independentes ou equipes de gerenciamento de TI separadas) ou
- Tem vários sites locais e deseja manter a mesma configuração em uma única instância do Citrix DaaS.

Além disso, a interface Full Configuration permite filtrar clientes locatários por nome. Por padrão, a interface exibe informações sobre todos os locatários.

O recurso está disponível para Citrix Service Providers (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 os clientes locatários ao Citrix DaaS e, em seguida, configuram o acesso do administrador ao Citrix DaaS. Para obter mais informações, consulte Citrix DaaS para Citrix Service Providers.
- Os não CSPs criam clientes locatários primeiro criando escopos e, depois, configurando o acesso personalizado para os respectivos administradores. Para obter mais informações, consulte Criar e gerenciar escopos.



Atualizações no AutoScale. Atualizamos o AutoScale para o estilo de folha para oferecer lhe uma melhor experiência de usuário. Os fluxos de trabalho para definir suas configurações permanecem os mesmos. Outras atualizações ao AutoScale incluem:

- **Restrict Autoscale** foi renomeado **Autoscaling Tagged Machines** para facilitar a compreensão.
- Foi adicionada a nova opção **Control when Autoscale starts powering on tagged machines**. Essa opção permite controlar quando o AutoScale começa a ligar as máquinas marcadas baseado no uso das máquinas não marcadas.

Para obter mais informações sobre máquinas marcadas pelo AutoScale, consulte Máquinas marcadas no AutoScale.

Verificações de validade de licenças. A interface Full Configuration agora verifica automaticamente a validade das licenças em uso pelas conexões do host. A conexão de host é colocada no modo de

manutenção se a sua licença for inválida. Como resultado, você não pode executar determinadas operações, como editar a conexão e desligar o modo de manutenção. Uma licença se torna inválida, por exemplo, quando:

- A licença tiver expirado. Nesse caso, entre em contato com o seu representante de vendas da Citrix para renová-la ou comprar novas licenças.
- A licença tiver sido excluída do Servidor de Licenças.

Estilo de folha aplicado aos nós de Catálogos de máquinas e Políticas. Os estilos de folha agora são aplicados a todos os nós na Full Configuration.

Suporte para atualizar máquinas provisionadas pelo MCS em ambientes do 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 esse recurso é `ServiceOffering`. Para obter mais informações, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Março 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 Citrix Virtual Apps and Desktops Service no Google Cloud.

Suporte ao início confiável do Azure. O início confiável do Azure agora está disponível para a interface de gerenciamento Full Configuration. Se você optar por selecionar uma imagem com o início confiável ativado, fica obrigatório o uso de um perfil de máquina. Além disso, você precisa selecionar um perfil de máquina com início confiável ativado. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Estilo de folha aplicado aos assistentes em mais três nós em Full Configuration. Os nós são: **Search**, **Delivery Groups** e **Applications**.

O Image Portability Service (IPS) é lançado para disponibilidade geral. O IPS simplifica o gerenciamento de imagens entre plataformas. Esse recurso é útil para gerenciar imagens entre uma localização do recurso no local e uma na 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 2022

Recursos novos e aprimorados

Permissões do Azure. Existem dois conjuntos de permissões necessárias para os requisitos de segurança e para minimizar os riscos.

- Permissões mínimas: esse 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: esse conjunto de permissões não impede que você obtenha novos benefícios de aprimoramento.

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 do Azure. Adicionamos a opção **Use non-persistent write-back cache disk** à página **Machine Catalog Setup > Disk Settings** da interface **Manage > Full Configuration**. Selecione essa opção se 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 do host da AWS. Os valores de configuração padrão da conexão do host da AWS são atualizados para valores mais altos e provavelmente são os mesmos para todas as configurações da plataforma de nuvem da AWS. Isso ajuda a criar conexões de host em ambientes de nuvem da AWS, sem avaliar e configurar os valores de configuração padrão de acordo com a configuração individual. Para obter mais informações, consulte Valores padrão de conexão do host.

Adicionado suporte para diferentes níveis de armazenamento em ambientes do GCP. Agora você pode fornecer as seguintes propriedades personalizadas nos ambientes do GCP para definir o tipo de armazenamento dos discos conectados à VM recém-criada:

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

Para obter mais informações, consulte Citrix Virtual Apps and Desktops Service SDK.

Alterar determinadas configurações da máquina virtual depois de criar catálogos de VMs Azure. Usando a interface de gerenciamento Full Configuration, agora você pode alterar as seguintes configurações depois de criar um catálogo:

- Tamanho da máquina

- Zonas de disponibilidade
- Perfil da máquina
- Licenças do Windows

Para fazer isso, no nó **Machine Catalogs**, selecione o catálogo e, em seguida, selecione **Edit Machine Catalog** na barra de ações. Para obter mais informações, consulte Editar um catálogo.

Suporte para armazenar discos de SO efêmeros do Azure no disco de cache ou no disco temporário. O Citrix Virtual Apps and Desktops Service agora permite armazenar o disco de SO efêmero do Azure no disco de cache ou no disco temporário para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Suporte para clusters Nutanix na AWS. O serviço Citrix Virtual Apps and Desktops é compatível com clusters Nutanix na 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 na AWS.

Suporte para a nuvem VMware na Amazon Web Services (AWS). A nuvem VMware na 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 Citrix Virtual Apps and Desktops Service. Para obter mais informações, consulte Nuvem VMware na Amazon Web Services (AWS).

Suporte para configurar o disco de cache de write-back para máquinas com Google Cloud Platform (GCP). Na interface de gerenciamento Full Configuration, ao provisionar máquinas no GCP, agora você pode definir as seguintes configurações de disco de cache de write-back:

- Tamanho do disco
- Memória alocada para cache
- Tipo de armazenamento em disco
- Persistência de disco

Para obter mais informações, consulte Criar um catálogo de máquinas no artigo Ambientes de virtualização do Google Cloud Platform.

Janeiro 2022

Recursos novos e aprimorados

Suporte para clusters Nutanix na AWS. O Citrix Virtual Apps and Desktops Service agora é compatível com clusters Nutanix na AWS. Esse suporte fornece a mesma funcionalidade de um cluster local da Nutanix. Somente um único cluster é suportado, o *Prism Element*. Para obter mais informações, consulte Ambientes de virtualização do 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 é compatível com a detecção e correção automáticas de determinados problemas identificados nas máquinas em que ele está sendo executado. Agora existe um relatório de resultados que lhe mostra quais ações específicas foram tomadas. Para obter mais informações, consulte Correção automática.
- **Suporte à linha de comando.** Agora, o Cloud Health Check pode ser executado a partir da linha de comando. Para obter mais informações, consulte Executar o Cloud Health Check na linha de comando.
- **Status do Citrix Universal Injection Driver.** 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 início de sessão.** O Cloud Health Check agora verifica as configurações do registro de início de sessão.
- **Atualizações ao relatório de verificação.** Para itens verificados que têm vários pontos de verificação, o relatório de verificação final agora lista todas as verificações que foram verificadas para mostrar quais ações foram executadas durante a verificação de integridade.

Para obter mais informações, consulte Cloud Health Check.

Solução de problemas de registro do VDA e início de sessão usando Full Configuration. Usando a interface de gerenciamento Full Configuration, 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 VDA e inicializações 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 de conexões existentes. Usando a interface de gerenciamento Full Configuration, agora você pode especificar a data após a qual o segredo do aplicativo expira. Para obter orientações sobre como exibir a data de expiração do segredo, consulte Ambientes de nuvem do Microsoft Azure Resource Manager. Ao usar esse recurso, considere as seguintes diferenças:

- Para entidades de serviço criadas manualmente no Azure, você pode editar diretamente a data de expiração na página **Edit Connection > Connection Properties**.
- Ao editar pela primeira vez a data de expiração para entidades de serviço criadas através da Full Configuration em seu nome, vá para **Edit Connection > Edit settings > Use existing**. As próximas edições você pode fazer na página **Edit Connection > Connection Properties**.

Um botão para adicionar administradores. Adicionamos um botão, **Add Administrator**, à guia **Full Configuration > Administrators > Administrators**. O botão oferece uma maneira rápida de ir para

Identity and Access Management > Administrators, onde você pode adicionar (convidar) administradores. Para obter mais informações, consulte Adicionar um administrador.

Assistentes com nova aparência em Full Configuration. Atualizamos os assistentes nos seguintes nós com um novo estilo, incluindo cores, fontes e outras alterações de formatação, para lhe oferecer uma melhor experiência de usuário: **Administrators**, **Hosting**, **StoreFront**, **App Packages**, **Zones** e **Settings**. Os novos assistentes aparecem em exibições em folhas, com visores mais amplos, permitindo que mais conteúdo seja exibido. Os fluxos de trabalho para definir suas configurações permanecem os mesmos.

Suporte para reter o disco do sistema quando o MCS I/O está ativado para máquinas com Google Cloud Platform (GCP). Na interface de gerenciamento Full Configuration, 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) está ativada. Para obter mais informações, consulte Ativar atualizações de otimização de armazenamento MCS.

Suporte para upload ou download direto do EBS na Amazon Web Services (AWS). A AWS agora fornece API para permitir a criação direta do volume do EBS com o conteúdo desejado. Agora você pode usar a API para eliminar a necessidade do volume worker para a criação de catálogo e adição de VM. Para obter informações sobre as permissões da AWS necessárias para essa funcionalidade, consulte Ambientes de nuvem da Amazon Web Services.

Capacidade de identificar recursos da Amazon Web Services (AWS) criados pelo MCS. Adicionamos uma nova marca 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 Manage e Monitor. A interface de gerenciamento Full Configuration agora fornece opções adicionais para controlar se deve-se conceder acesso a funções personalizadas para **Manage** e **Monitor**. Para obter mais informações, consulte Criar e gerenciar funções.

Dezembro 2021

Recursos novos e aprimorados

Suporte para Google Cloud VMware Engine. Agora, a plataforma permite migrar as cargas de trabalho do Citrix local baseado em VMware para o Google Cloud e o seu ambiente principal do Citrix Virtual Apps and Desktops para o Citrix Virtual Apps and Desktops Service. Para obter mais informações, consulte Suporte para Google Cloud Platform (GCP) VMware Engine.

Capacidade de especificar com quais nomes de conta começar ao especificar um esquema de nomenclatura. Este lançamento introduz uma opção à página **Machine Catalog Setup > Machine Identities** da interface de gerenciamento Full Configuration. A opção permite especificar números ou

letras com os quais os nomes de conta começam, lhe dando maior controle sobre a nomenclatura das contas de máquina durante a criação do catálogo. Para obter mais informações, consulte Identidades de máquina.

Suporte para criação de conexões Nutanix AHV XI e Nutanix AHV Prism Central (PC). Na interface de gerenciamento Full Configuration, agora você pode criar conexões Nutanix AHV XI e Nutanix AHV PC. Para obter mais informações, consulte Ambientes de virtualização do Nutanix.

Suporte para selecionar o tipo de armazenamento para discos de SO ao provisionar máquinas virtuais no GCP. Na interface de gerenciamento Full Configuration, ao provisionar máquinas virtuais no GCP, agora você pode selecionar o tipo de armazenamento para o disco de SO. As opções de armazenamento disponíveis na página **Machine Catalog Setup > Storage** incluem **Standard persistent disk**, **Balanced persistent disk** e **SSD persistent disk**. Para obter mais informações, consulte Criar um catálogo de máquinas.

A interface de gerenciamento Full Configuration 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 a opção **Azure ephemeral OS disk** à página **Machine Catalog Setup > Storage and License Types**. Selecione a opção se quiser usar o disco local da máquina virtual para hospedar o disco do sistema operacional. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Proteção dos recursos gerenciados do Machine Creation Services (MCS) contra a exclusão acidental. Agora você pode proteger os recursos gerenciados do MCS no Google Cloud Platform (GCP) aplicando o sinalizador `deletionProtection` do GCP ativado para as VMs. Usando a permissão `compute.instances.setDeletionProtection` ou a função Compute Admin do IAM, 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 a exclusão acidental da máquina.

Novembro 2021

Recursos novos e aprimorados

Anotar uma imagem ao atualizar máquinas. Na interface de gerenciamento Full Configuration, agora você pode anotar uma imagem adicionando uma nota sobre ela ao atualizar um catálogo criado pelo MCS. Cada vez que você atualiza o catálogo, é criada uma entrada relacionada à nota se você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como null (-). Para exibir o histórico de notas da imagem, selecione o catálogo, clique em **Template Properties** no painel inferior e, em seguida, clique em **View note history**. Para obter mais informações, consulte Atualizar um catálogo.

Suporte ao licenciamento multitipos. A interface de gerenciamento Full Configuration agora oferece suporte ao licenciamento multitipos, permitindo que você especifique qual direito de licença deseja que seu site (sua implantação de um produto Citrix Virtual Apps and Desktops Service) 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 um 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 multitipos.

Para obter mais informações, consulte Licenciamento multitipos.

Suporte para exibir informações do plano de compra do Azure Marketplace. Na interface de gerenciamento Full Configuration, ao criar um catálogo de máquinas, agora você pode exibir as informações do plano de compra em imagens mestre originadas de imagens do Azure Marketplace.

Outubro 2021

Recursos novos e aprimorados

Capacidade de atualizar catálogos persistentes do MCS. Introduzimos a opção **Update Machines** para catálogos persistentes do MCS na interface de gerenciamento Full Configuration. A opção permite gerenciar a imagem ou o modelo usado pelo catálogo. Ao atualizar um catálogo persistente, considere o seguinte: Somente as máquinas adicionadas ao catálogo posteriormente são criadas usando a nova imagem ou modelo. Não lançamos a atualização para as máquinas existentes no catálogo. Para obter mais informações, consulte Atualizar um catálogo.

Opção de provisionar máquinas virtuais em um host dedicado do Azure. Adicionamos a opção **Use a host group** à página **Machine Catalog Setup > Master Image** da interface de gerenciamento Full Configuration. A opção permite especificar qual grupo de host você deseja usar ao provisionar máquinas virtuais em ambientes do Azure. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Melhore o desempenho preservando uma VM provisionada durante o ciclo de energia. Adicionamos a configuração **Retain VMs across power cycles** à página **Machine Catalog Setup > Disk Settings** da interface de gerenciamento Full Configuration. A configuração permite preservar uma máquina virtual provisionada durante o ciclo de energia em ambientes do Azure. Para obter mais informações, consulte Otimização de armazenamento MCS. Como alternativa, você pode configurar o recurso usando o PowerShell. Para obter mais informações, consulte Preservação de uma máquina virtual provisionada durante o ciclo de energia.

Vincular um catálogo de máquinas a um conjunto de configurações do Workspace Environment Management. Ao criar um catálogo de máquinas, agora você pode associá-lo a um conjunto de configurações 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 associar o catálogo depois de criá-lo. Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.

Setembro 2021

Recursos novos e aprimorados

Adicione uma descrição informativa sobre atualizações de imagens. Agora você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagens a catálogos de máquinas. Essa funcionalidade é útil para administradores que desejam adicionar rótulos descritivos ao atualizar uma imagem usada por um catálogo, por exemplo, o *Office 365 instalado*. Usando os comandos do PowerShell, você pode criar e exibir essas mensagens. Para obter detalhes, consulte Adicionar descrições a uma imagem.

Integração do Azure VMware Solution (AVS). O Citrix Virtual Apps and Desktops Service oferece suporte ao AVS, a solução VMware do Azure. O AVS fornece infraestrutura de nuvem contendo clusters do vSphere criados pelo Azure. Aproveite o serviço Citrix Virtual Apps and Desktops para usar o AVS para provisionar sua carga de trabalho do 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 Citrix Virtual Apps and Desktops Service. Esse processo:

- aplica-se a qualquer grupo de recursos que contenha um ou mais catálogos de máquina.
- oferece suporte a grupos de recursos que não são criados pelo Machine Creation Services.
- cria a máquina virtual e os recursos associados.
- exclui recursos no grupo de recursos quando a máquina virtual ou o catálogo é removido.

Para obter mais informações, consulte Grupos de recursos do Azure.

Recuperar informações para VMs do Azure, instantâneos, disco de SO e definição de imagem da galeria. Você pode exibir informações para uma VM do Azure, disco de 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 exibir e selecionar uma imagem do Linux ou do Windows. Para obter mais informações, consulte Recuperar informações para VMs do Azure, instantâneos, disco de SO e definição de imagem da galeria.

Nova atualização da configuração automatizada. A configuração automatizada foi atualizada para uma nova versão com recursos que incluem:

- Suporte a Machines Creation Services (MCS) –a configuração automatizada agora oferece suporte a catálogos MCS. Para obter mais informações, consulte Noções básicas sobre a migração de catálogos provisionados do Machine Creation Services.

Outras atualizações à configuração automatizada incluem:

- Suporte aprimorado às zonas, com o preenchimento prévio do arquivo ZoneMapping.yml com o nome das zonas locais durante a exportação e os locais de recursos da nuvem ao fazer backup.
- O StoreFront tornou-se um componente gerenciável de alto nível. Antes disso, o StoreFront era gerenciado como parte dos grupos de entrega. Essa separação facilita a mesclagem de sites.
- Alteração de `AddMachinesOnly` para `MergeMachines` para corresponder ao padrão das opções de mesclagem atual e nova.
- 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 de usuário.
- Corrigido o suporte do plano de controle em japonês.
- Outras correções e melhorias.

Baixe o Automated Configuration nos Downloads da Citrix. Para obter mais informações sobre a configuração automatizada, consulte Migrar a configuração para o Citrix Cloud.

Mais opções de agendamento disponíveis com agendamentos de reinicialização. A interface de gerenciamento Full Configuration agora fornece opções adicionais para controlar quando ocorrerem reinicializações programadas. Além dos agendamentos de reinicialização recorrentes diários, agora você pode definir padrões de recorrência semanais e mensais. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Preserve colunas personalizadas que degradam o desempenho. Anteriormente, no nó **Search** da interface de gerenciamento Full Configuration, as colunas personalizadas que degradavam o desempenho desapareciam depois que você atualizava a janela do navegador ou quando se desconectava do console e entrava novamente. Agora você pode controlar se deseja preservar as colunas personalizadas. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Use a ferramenta Automated Configuration para backup e restauração. Adicionamos o nó **Backup and Restore** à interface de gerenciamento Full Configuration. Esse nó agrega todos os recursos relacionados à ferramenta Automated Configuration, incluindo informações sobre:

- Agendar backups automatizados de sua configuração do Citrix Virtual Apps and Desktops usando um único comando
- Restaurar a partir de um backup anterior, se necessário
- Realizar backups e restaurações de forma granular
- Outros casos de uso suportados

Para obter mais informações, consulte a documentação de Automated Configuration.

Suporte para catálogos não ingressados no domínio. Adicionamos o tipo de identidade **Non-domain-joined** à página **Machine Catalog Setup > Machine Identities** da interface de gerenciamento Full Configuration. Com esse tipo de identidade, você pode usar o MCS para criar máquinas que não estão ingressadas em nenhum domínio. Para obter mais informações, consulte Criar catálogos de máquinas.

Suporte para usar um perfil de máquina. Adicionamos a opção **Use a machine profile** à página **Machine Catalog Setup > Master Image** da interface de gerenciamento Full Configuration. A opção permite especificar de qual perfil de máquina você deseja que as máquinas virtuais herdem configurações ao criar VMs em ambientes do Azure. Assim, as VMs no catálogo podem herdar configurações do perfil de máquina selecionado. Alguns exemplos de configurações:

- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado aos discos OS e MCSIO)
- Tamanho da máquina (salvo indicação em contrário)
- Tags colocadas na VM

Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Suporte para Windows Server 2022. Requer, no mínimo, VDA 2106.

Agosto 2021

Recursos novos e aprimorados

Estenda o número de itens classificáveis de 500 para 5.000. No nó **Search** da interface de gerenciamento Full Configuration, 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 a pesquisa na interface de gerenciamento Full Configuration.

Suporte para tipos adicionais de armazenamento do Azure. Agora você pode selecionar diferentes tipos de armazenamento para máquinas virtuais em ambientes do Azure usando o MCS. Para obter detalhes, consulte Tipos de armazenamento.

Suporte para selecionar o tipo de armazenamento para discos de cache de write-back. Na interface de gerenciamento Full Configuration, 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 Standard e HDD Standard. Para obter mais informações, consulte Criar catálogos de máquinas.

Desligar máquinas suspensas. Na interface **Manage > Full Configuration**, adicionamos a opção **When no reconnection in (minutes)** à página **Load-based Settings** da interface do usuário Manage Autoscale para grupos de entrega de SO de sessão única. A opção fica disponível depois que você seleciona **Suspend**, permitindo especificar quando desligar as máquinas suspensas. As máquinas suspensas permanecem disponíveis para os usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Desligar as máquinas as torna disponíveis novamente para lidar com 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 **Manage > Full Configuration**, agora você pode usar um arquivo CSV para adicionar, em massa, máquinas que já estão em seu data center a um catálogo em que essas máquinas apresentam gerenciamento de energia. Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.

Julho 2021

Recursos novos e aprimorados

Log de configuração. A interface do usuário **Logging** foi alterada em **Manage > Full Configuration**. As três guias a seguir formam a interface:

- **Events** (anteriormente, Configuration logging). Essa guia permite controlar as alterações de configuração e as atividades administrativas.
- **Tarefas**. Essa guia permite exibir tarefas relacionadas às operações do catálogo de máquinas.
- **APIs**. Essa guia permite que você visualize as solicitações da API REST feitas durante um determinado período de tempo.

Para obter mais informações, consulte Log de configuração.

Agora, o AutoScale oferece opções de tempo limite de sessão dinâmica. Você pode configurar tempos limite de sessão desconectada e ociosa para os horários de uso 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 dinâmica.

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 fornece 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 esse recurso, consulte Usar chaves de criptografia gerenciadas pelo cliente (CMEK). O recurso está disponível na página **Machine Catalog Setup > Disk Settings** da interface **Manage > Full Configuration**.

> **Nota:**
>
> Esse recurso está disponível como Preview.

Atualizações na guia Manage. Atualizamos as opções no menu da guia **Manage**:

- **Full Configuration**: anteriormente, essa opção levava você ao console legado. Agora, ela o leva para o novo console na Web (Web Studio). O console baseado na Web tem paridade total com o console legado e inclui vários aprimoramentos. Recomendamos que você comece a usá-lo agora.
- **Legacy Configuration**: essa opção leva você ao console legado, que está programado para ser removido em setembro de 2021. Depois disso, **Full Configuration** será a única interface a oferecer acesso a toda a gama de ações de configuração e gerenciamento.

O Web Studio agora suporta a escolha de uma conexão de gerenciamento de energia para um catálogo de acesso ao PC remoto. Anteriormente, você podia usar o Studio para criar uma conexão de host Wake on LAN com a localização do recurso (selecionando **Remote PC Wake on LAN** como o tipo de conexão). No entanto, o PowerShell era a sua única opção para associar a conexão a um catálogo de acesso ao PC remoto. Agora você pode usar o Studio para fazer isso. Para obter mais informações, consulte Configurar a Wake on LAN na interface Full Configuration.

Junho 2021

Recursos novos e aprimorados

Acesse 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 Master Image. Para obter detalhes, consulte Acessar imagens da Galeria de Imagens Compartilhadas do Azure.

Suporte a máquinas virtuais protegidas no Google Cloud Platform (GCP). Você pode provisionar máquinas virtuais protegidas no GCP. Uma máquina virtual protegida é reforçada por um conjunto de controles de segurança que fornecem integridade verificável das instâncias do Compute Engine usando recursos avançados de segurança de plataforma, como reinicialização segura, Trusted Platform Module virtual, firmware UEFI e monitoramento de integridade. Para obter mais informações, consulte VMs protegidas.

Imposição de HTTPS ou HTTP. Use as configurações do registro para impor o tráfego HTTPS ou HTTP por meio do serviço XML.

Sempre use SSD Standard para um disco de identidade para reduzir custos em ambientes do Azure. Os catálogos de máquinas usam o tipo de armazenamento SSD Standard para discos de identidade. Os SSDs Standard 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 preços do disco gerenciado do Azure, consulte Preços de discos gerenciados.

Novo recurso disponível no Web Studio. Os seguintes recursos agora estão disponíveis no console 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 na 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. Quando você clona um catálogo, não é possível alterar as configurações associadas ao sistema operacional e gerenciamento da máquina. O catálogo clonado herda essas configurações do original. Para obter mais informações, consulte Clonar um catálogo.
- **Agora há um novo nó chamado Settings disponível no painel de navegação do Studio**. O nó **Settings** permite definir os parâmetros de configuração que se aplicam a todo o site (a implantação do seu produto Citrix Virtual Apps and Desktops Service). As seguintes configurações estão disponíveis:
  - **Balanceamento de carga de catálogos multissessão**. 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 Balanceamento de carga das máquinas.
- **Experiência de pesquisa aprimorada no Studio**. Esta versão aprimora sua experiência de pesquisa no Studio. Quando você usa filtros para realizar uma pesquisa avançada, a janela Add filters aparece em primeiro plano, deixando a exibição em segundo plano inalterada. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.
- **Capacidade de suspender e retomar as VMs do Google Cloud no MCS**. Agora você pode suspender e retomar as VMs do Google Cloud no MCS como faria com qualquer máquina virtual.

Para obter detalhes, consulte Gerenciar grupos de entrega. Para ativar a funcionalidade, defina as permissões `compute.instances.suspend` e `compute.instances.resume` na conta de serviço do Google Cloud. A função Compute Admin vem com essas permissões.

No Citrix Virtual Apps and Desktops, você também pode usar o comando `New-BrokerHostingPowerAct` do PowerShell para suspender e retomar as VMs. Para obter detalhes, consulte New-Brokerhostingpoweraction.

O Google Cloud impõe algumas limitações no tipo e na configuração de instâncias que podem ser suspensas. Para obter mais informações, consulte Suspender e retomar uma instância no site do Google Cloud.

Maio 2021

Recursos novos e aprimorados

Reconexão de sessão após desconectar da máquina no modo de manutenção. Anteriormente, quando os usuários da área de trabalho de sessão única (VDI) em pool (aleatórios) eram desconectados de uma máquina no modo de manutenção, a reconexão de sessão não era permitida a nenhuma máquina no pool. As máquinas de sessão única estática e multissessão sempre permitiram a reconexão de sessão em tais circunstâncias.

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 no modo de manutenção. Isso se aplica a todos os VDAs no grupo (sessão única e multissessão).

Para obter detalhes, consulte Controlar reconexão da sessão quando desconectada da máquina no modo de manutenção.

Suporte para sondagem de aplicativos e sondagem de área de trabalho em todas as edições do Citrix Virtual Apps and Desktops Service. Além do suporte existente à edição **Premium**, a sondagem de aplicativos e a sondagem de área de trabalho estão agora disponíveis nas edições **Citrix Virtual Apps Advanced Service** e **Citrix Virtual Apps and Desktops Advanced Service**.

Novo recurso disponível no Web Studio. O recurso a seguir agora está disponível no console na Web:

- **O Studio agora suporta a 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 do 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) deixa que o Azure coloque as máquinas nas regiões. Se mais de uma zona for especificada, o MCS

distribuirá aleatoriamente as máquinas entre elas. Para obter mais informações, consulte Provisionar máquinas em zonas de disponibilidade especificadas.

Disco efêmero do Azure. O Citrix Virtual Apps and Desktops Service é compatível com o disco efêmero do Azure. Um disco efêmero permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão.

> **Nota:**
>
> Os catálogos persistentes não oferecem suporte a discos de SO efêmeros. Além disso, ao usar esse recurso, considere que o disco com desempenho extra incorre em um custo extra. É benéfico reutilizar o disco de cache para armazenar o disco de SO em vez de pagar por um disco gerenciado extra.

Os 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 pelo MCS no Azure. O Citrix Virtual Apps and Desktops Service melhora o desempenho dos VDAs gerenciados com o Machine Creation Services (MCS) no Azure. Esse aprimoramento altera os valores padrão para *Absolute Simultaneous actions*, para a conexão de hospedagem até 500, e *Maximum new actions per minute*, para a conexão de hospedagem até 2.000. Nenhuma tarefa de configuração manual é necessária para aproveitar esse 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**. Agora o Cloud Health Check pode descobrir e recuperar automaticamente VDAs de suas implantações do Citrix Virtual Apps and Desktops Service. Para obter mais informações, consulte Recuperar máquinas VDA.
- **Agendar verificações de integridade**. Agora, o Cloud Health Check permite que você configure programações para realizar verificações de integridade periódicas. Para obter mais informações, consulte Agendador do Cloud Health Check.
- **Informações sobre a versão do Cloud Health Check**. Agora você pode verificar qual versão do Cloud Health Check está sendo usada. Para ver 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 é compatível com a detecção e correção automáticas de determinados problemas identificados nas máquinas em que ele está sendo executado. Para obter mais informações, consulte Correção automática.

> **Nota:**
>
> A correção automática está disponível como versão preview.

Abril 2021

Recursos novos e aprimorados

Recupere instâncias dinâmicas usando a API da AWS. O Citrix Virtual Apps and Desktops Service 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 daqueles definidos no Citrix Virtual Apps and Desktops Service. Essas informações eram fornecidas anteriormente no arquivo `InstanceTypes.xml`. Para facilitar esse acesso dinâmico aos tipos de instância disponíveis da AWS, os usuários devem atualizar as permissões em suas entidades de serviço para incluir permissões `ec2:DescribeInstanceTypes`. Para oferecer suporte à compatibilidade com versões anteriores para clientes que optam por não atualizar suas permissões de entidade de serviço, são usados os tipos de instância da AWS listados em `InstanceTypes.xml`. 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 Definição de permissões do IAM e Sobre as permissões da AWS.

Novo recurso disponível no Web Studio. O recurso a seguir agora está disponível no console 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 no fuso horário do sistema. O Studio agora oferece suporte à exibição de data e hora locais para seu fuso horário quando você passa o ponteiro do mouse sobre um item de evento. A hora é expressa em UTC.

Suporte a MCS I/O para VMs Azure em armazenamento temporário. O MCS I/O agora oferece suporte à criação de catálogo de máquinas para VMs que não têm discos temporários ou armazenamento conectado. Com esse suporte:

- O instantâneo (disco gerenciado) é recuperado da VM de origem *sem* armazenamento temporário. As VMs no catálogo de máquinas não têm armazenamento temporário.
- O instantâneo (disco gerenciado) é recuperado da VM de origem *com* armazenamento temporário. As VMs no catálogo de máquinas têm armazenamento temporário.

Para obter mais informações, consulte Otimização de armazenamento do Machine Creation Services (MCS).

Novo recurso disponível no Web Studio. O recurso a seguir agora está disponível no console na Web:

- **Forçar logoff**. Agora, o AutoScale permite que você faça logoff à força das sessões existentes nas máquinas quando o período de tolerância estabelecido é atingido, tornando a máquina elegível para desligamento. Isso permite que o AutoScale desligue as máquinas muito mais rapidamente, reduzindo os custos. Você pode enviar notificações aos usuários antes que seja feito o logoff. Para obter mais informações, consulte AutoScale.

Nova atualização da 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 o conflito de nomes usando prefixos e sufixos. Para obter mais informações, consulte Mesclar vários sites em um único site.
- **Ativação do site** —você pode selecionar se sua implantação no local ou na nuvem controla recursos como agendamentos de reinicialização e esquemas de energia. Para obter mais informações, consulte Ativação de sites.

Outras atualizações à configuração automatizada incluem:

- A capacidade de migrar funções e escopos de administrador.
- Um parâmetro `Quiet` para cmdlets selecionados para suprimir o log no 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 do parâmetro switch, eliminando a necessidade de adicionar `$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 o Automated Configuration nos Downloads da Citrix. Para obter mais informações sobre a configuração automatizada, consulte Migrar para a nuvem.

Preserve instâncias do GCP em todos os 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 todos os ciclos de energia. Quando uma instância não persistente é desligada, o disco de SO é desconectado e excluído. Quando a instância é ligada, o disco de SO é recriado a partir do disco básico e anexado à instância existente.

Suporte para imagens do Azure Gen2. Agora você pode provisionar um catálogo de VMs Gen2 usando um instantâneo Gen2 ou um disco gerenciado Gen 2 para melhorar o desempenho do tempo de inicialização. Para obter mais informações, consulte Criar catálogos de máquinas. Os seguintes sistemas operacionais são compatíveis com imagens do Azure Gen2:

- Windows Server 2019, 2016, 2012 e 2012 R2
- Windows 10

> **Nota:**
>
> Não há suporte para a criação de um catálogo de máquinas Gen2 usando um instantâneo Gen1 ou disco gerenciado. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando um instantâneo Gen2, ou disco gerenciado, também não é suportada. Para obter mais informações, consulte Suporte para VMs de geração 2 no Azure.

Desativar contas de armazenamento de tabelas. O Machine Creation Services (MCS) não cria mais contas de armazenamento de tabelas para catálogos que usam discos gerenciados ao provisionar VDAs no Azure. Para obter mais informações, consulte Armazenamento de tabelas do Azure.

Eliminar bloqueios nas contas de armazenamento. Ao criar um catálogo no Azure usando um disco gerenciado, a conta de armazenamento não é mais criada. As contas de armazenamento criadas para catálogos existentes permanecem inalteradas. Essa alteração é aplicável somente para 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 agora estão disponíveis no console 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 **Machine Catalog Setup > Disk Settings**. 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, era necessário usar o PowerShell para restringir o AutoScale a determinadas máquinas em um grupo de entrega. Agora você também pode usar o Studio. Para obter mais informações, consulte Restringir o AutoScale a determinadas máquinas em um grupo de entrega.

Março 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 sejam as únicas máquinas em execução no host. Isso proporciona mais controle e visibilidade aos clientes, garantindo que atendam aos requisitos regulamentares ou de segurança interna. Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`. É necessário também o posicionamento automático do Azure. Para obter mais informações, consulte Hosts dedicados do Azure.

> **Dica:**
>
> Ao usar hosts dedicados do Azure, selecionar a **Zona de disponibilidade do Azure** não tem efeito. A máquina virtual é posicionada pelo processo de posicionamento automático do Azure.

Suporte para criptografia do lado do servidor do Azure. O Citrix Virtual Apps and Desktops Service 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 de seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Criptografia do servidor do Azure.

Provisionar máquinas em zonas de disponibilidade especificadas no Azure. Você pode provisionar máquinas em uma zona de disponibilidade específica em ambientes do Azure. Com essa funcionalidade:

- Você pode especificar uma ou várias zonas de disponibilidade no Azure. As máquinas são nominalmente distribuídas igualmente em todas as zonas fornecidas, se mais de uma zona for fornecida.
- A máquina virtual e o disco correspondente são colocados na zona ou zonas especificadas.
- Você pode navegar pelas zonas de disponibilidade de uma determinada oferta de serviço ou região. As zonas de disponibilidade válidas são exibidas usando comandos do PowerShell. Veja 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 agora estão disponíveis no console na Web:

- **O Studio agora oferece suporte à associação de aplicativos com ícones personalizados**. Anteriormente, era necessário 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 marcas a catálogos de máquinas**. Anteriormente, você podia usar o Studio para criar ou excluir marcas para uso com um catálogo. No entanto, você tinha que usar o PowerShell para aplicar marcas ao catálogo. Agora você também pode usar o Studio para aplicar uma marca a um catálogo ou removê-la, como faz com grupos de entrega. Para obter mais informações, consulte Aplicar marcas 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 com SO multissessão. Para obter mais informações, consulte Balanceamento de carga das máquinas.
- **O Studio agora suporta a inclusão de máquinas no modo de manutenção em agendamentos de reinicialização**. Anteriormente, o PowerShell era sua única opção para configurar reinicializações programadas para máquinas no 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 suporta a configuração de Wake on LAN para acesso ao PC remoto**. Anteriormente, era necessário usar o PowerShell para configurar o Wake on LAN para acesso ao PC remoto. 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 instâncias da AWS e à marcação de recursos operacionais**. Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode especificar se as propriedades de função e marcação do IAM devem ser aplicadas a essas máquinas. Você também pode especificar se as marcas de máquina devem ser aplicadas aos recursos operacionais. Você tem as duas opções a seguir:

  - Aplicar propriedades de modelo de máquina a máquinas virtuais, em **Apply machine template properties to virtual machines**
  - Aplicar marcas de máquina a recursos operacionais, em **Apply machine tags to operational resources**

  Para obter mais informações, consulte Aplicar propriedades de instâncias da AWS e marcar 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 publicadas para máquinas provisionadas do MCS no Azure. Os administradores têm a opção de armazenar uma

imagem na galeria para acelerar a criação e a hidratação dos discos de SO. Esse processo melhora os tempos de reinicialização e de inicialização 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 legadas.

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 do disco. Esses buckets abrangiam várias regiões, que o Google define como uma grande área geográfica contendo duas ou mais localidades geográficas. Esses buckets temporários residiam na localização geográfica dos Estados Unidos, independentemente de onde o catálogo era provisionado. O MCS agora cria buckets de armazenamento na mesma região em que você provisiona seus catálogos. Os buckets de armazenamento não são mais temporários: eles permanecem no projeto do Google Cloud Platform depois que você conclui o processo de provisionamento. As futuras operações de provisionamento usam o bucket de armazenamento existente, se houver um bucket na região. Um novo bucket de armazenamento será criado se não existir um na região especificada.

Fevereiro 2021

Recursos novos e aprimorados

Suporte para imagens do Azure Gen2. 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 esse suporte, somente um subconjunto de VMs é suportado. Por exemplo, algumas VMs podem ser dos tipos Gen1 e Gen2, enquanto outras VMs podem ser somente Gen1. Para obter mais informações, consulte Suporte para VMs de geração 2 no Azure.

Agendamentos de reinicialização da máquina. O Citrix Studio agora adiciona uma opção chamada **Restart all machines after draining sessions** ao menu **Restart duration**. A opção permite que você escolha se deseja reiniciar todas as máquinas depois de esvaziar todas as sessões. Quando o horário de reinicialização é atingido, as máquinas são colocadas no estado de esvaziamento e reinicializadas

quando for feito o logoff de todas as sessões. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Novos recursos disponíveis no Web Studio. Os seguintes recursos agora estão disponíveis no console na Web:

- **O Studio agora suporta o uso de arquivos CSV para adicionar máquinas em massa a um catálogo**. Esse recurso permite que você use um arquivo CSV para:
  - Adicionar máquinas em massa a um catálogo de SO multissessão ou de sessão única em que as máquinas não têm gerenciamento de energia por meio do Studio.
  - Adicionar máquinas em massa a um catálogo de acesso ao PC remoto. Anteriormente, você tinha que escolher unidades organizacionais (UOs) para adicionar máquinas em massa a um catálogo de acesso ao PC remoto. No entanto, isso não é fácil de fazer 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 junto com atribuições de usuário.

  Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.

- **Suporte estendido para o Citrix Managed Azure.** O Citrix Managed Azure agora está disponível nas seguintes edições do Citrix Virtual Apps and Desktops Service: Standard for Azure, Advanced, Premium e Workspace Premium Plus.

- **Suporte para posicionar imagens mestre na Galeria de Imagens Compartilhadas do Azure**. O Studio agora oferece a opção de posicionar imagens mestre na Galeria de Imagens Compartilhadas do Azure (SIG). SIG é um repositório para gerenciar e compartilhar imagens. Ele permite que você disponibilize suas imagens em toda a organização. Recomendamos que você armazene uma imagem mestre na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite a redefinição mais rápida dos discos de SO do VDA. Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

- **Reter o disco do sistema para catálogos de máquinas MCS no Azure**. O Studio agora permite controlar a retenção de discos de sistema para VDAs durante os ciclos de energia. Normalmente, o disco de 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 mais longos da VM. Se as gravações do sistema forem redirecionadas para o cache, e for feito o write-back para o disco de cache, o disco do sistema permanece inalterado. Para evitar a recriação desnecessária do disco, use a opção **Retain system disk during power cycles**, disponível na página **Machine Catalog Setup > Disk Settings**. Ativar a opção reduz os tempos de reinicialização da VM, mas aumenta os custos de armazenamento. A opção pode ser útil nos cenários

em que um ambiente contém cargas de trabalho com tempos de reinicialização sensíveis. Para obter mais informações, consulte Otimização de armazenamento MCS.

- **O Studio agora suporta a criação de catálogos de máquinas MCS com disco de cache de write-back persistente**. Anteriormente, o PowerShell era sua única opção para criar um catálogo com disco de cache de write-back persistente. Agora você pode usar o Studio para controlar se o disco de cache de write-back persiste para as VMs provisionadas no Azure quando você está criando um catálogo. Se desativado, o disco de cache de write-back é excluído durante cada ciclo de energia para economizar custos de armazenamento, fazendo com que todos os dados redirecionados para o disco sejam perdidos. Para reter os dados, ative a opção **Use persistent write-back cache disk**, disponível na página **Machine Catalog Setup > Disk Settings**. Para obter mais informações, consulte Otimização de armazenamento MCS.

Suporte para App Protection para Citrix Virtual Apps and Desktops Service com StoreFront. Para obter mais informações, consulte App Protection.

Janeiro 2021

Novos recursos disponíveis no Web Studio. Os seguintes recursos agora estão disponíveis no console na Web:

- **O Studio agora oferece suporte à associação de aplicativos com ícones personalizados**. Anteriormente, era necessário 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 marcas a catálogos de máquinas**. Anteriormente, você podia usar o Studio para criar ou excluir marcas para uso com um catálogo. No entanto, você tinha que usar o PowerShell para aplicar marcas ao catálogo. Agora você também pode usar o Studio para aplicar uma marca a um catálogo ou removê-la, como faz com grupos de entrega. Para obter mais informações, consulte Aplicar marcas 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 com SO multissessão. Para obter mais informações, consulte Balanceamento de carga das máquinas.
- **O Studio agora suporta a inclusão de máquinas no modo de manutenção em agendamentos de reinicialização**. Anteriormente, o PowerShell era sua única opção para configurar reinicializações programadas para máquinas no 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 suporta a configuração de Wake on LAN para acesso ao PC remoto**. Anteriormente, era necessário usar o PowerShell para configurar o Wake on LAN para acesso ao PC remoto. 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 instâncias da AWS e à marcação de recursos operacionais**. Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode especificar se as propriedades de função e marcação do IAM devem ser aplicadas a essas máquinas. Você também pode especificar se as marcas de máquina devem ser aplicadas aos recursos operacionais. Você tem as duas opções a seguir:
  - Aplicar propriedades de modelo de máquina a máquinas virtuais, em **Apply machine template properties to virtual machines**
  - Aplicar marcas de máquina a recursos operacionais, em **Apply machine tags to operational resources**

  Para obter mais informações, consulte Aplicar propriedades de instâncias da AWS e marcar recursos operacionais.
- **Host dedicado da AWS**. O Citrix Studio agora adiciona uma opção chamada **Use dedicated host** à página **Machine Catalog Setup > Security**. Essa configuração é adequada para implantações com restrições de licenciamento ou requisitos de segurança que precisam do uso de um host dedicado. Com um host dedicado, você tem um host físico inteiro e é cobrado por hora. Possuir esse host permite que você gire quantas instâncias do EC2 o host permitir, sem mais cobranças. Para obter mais informações, consulte Locação da AWS.
- **O Studio agora suporta a execução de um agendamento de reinicialização imediatamente**. O Studio agora permite que você execute um agendamento de reinicialização imediatamente para reiniciar todas as máquinas aplicáveis na programação. Para obter mais informações, consulte Executar imediatamente um agendamento de reinicialização.
- **AutoScale**. O AutoScale fornece os seguintes novos recursos e aprimoramentos:
  - **O Studio agora suporta a exibição de máquinas no estado de esvaziamento**. Anteriormente, o PowerShell era sua única opção para identificar máquinas em estado de esvaziamento. Agora você pode usar o Studio para identificar máquinas que estão em estado de esvaziamento. Para obter mais informações, consulte Exibir máquinas em estado de esvaziamento.
  - **O Studio agora suporta a definição de horários de pico em um nível granular de 30 minutos para grupos de entrega de VDI**. Anteriormente, era necessário usar o PowerShell para definir os horários de pico para os dias incluídos em uma programação em um

nível granular de 30 minutos para grupos de entrega de 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 de 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 publicadas para máquinas provisionadas do MCS no Azure. Os administradores têm a opção de armazenar uma imagem na galeria para acelerar a criação e a hidratação dos discos de SO a partir da imagem mestre. Esse processo melhora os tempos de reinicialização e de inicialização 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 Citrix Virtual Apps and Desktops Service 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 proporção de réplicas configuradas e no máximo de réplicas configuradas.

> **Nota:**
>
> A funcionalidade da Galeria de Imagens Compartilhadas só funciona com discos gerenciados. Não está disponível para catálogos de máquinas legadas.

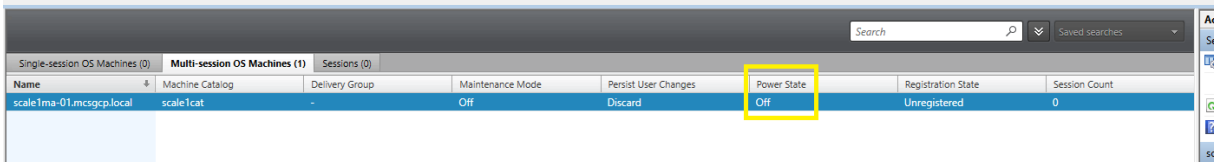
Para obter detalhes sobre esse recurso, consulte Configurar a galeria de imagens compartilhadas.

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 do disco. Esses buckets abrangiam várias regiões, que o Google define como uma grande área geográfica contendo duas ou mais localidades geográficas. Esses buckets temporários residiam na localização geográfica dos Estados Unidos, independentemente de onde o catálogo era provisionado. O MCS agora cria buckets de armazenamento na mesma região em que você provisiona seus catálogos. Os buckets de armazenamento não são mais temporários: eles permanecem no projeto do Google Cloud Platform depois que você conclui o processo de provisionamento. As futuras operações de provisionamento usam o bucket de armazenamento existente. Isso se houver um na região; ou um novo bucket de armazenamento é criado se não

existir um na região especificada.

Opção do PowerShell que define o padrão para reutilizar VDAs em pool durante uma interrupção. Uma nova opção de comando do PowerShell (`-DefaultReuseMachinesWithoutShutdownInOut`) estende a capacidade de reutilizar VDAs de área de trabalho em pool que não foram desligados durante uma interrupção, por padrão. Consulte Suporte a aplicativos e áreas de trabalho.

Provisionamento sob demanda do Google Cloud Platform. O Citrix Virtual Apps and Desktops Service atualiza como o Google Cloud Platform (GCP) provisiona catálogos de máquinas. Ao criar um catálogo de máquinas, a instância da máquina correspondente não é criada no GCP e o estado de energia é definido como **desativado**. As máquinas não são provisionadas no momento da criação do catálogo, mas, sim, na primeira vez em que as máquinas são ligadas. Por exemplo, depois de criar um catálogo, o estado de energia da VM é definido como **desativado**:

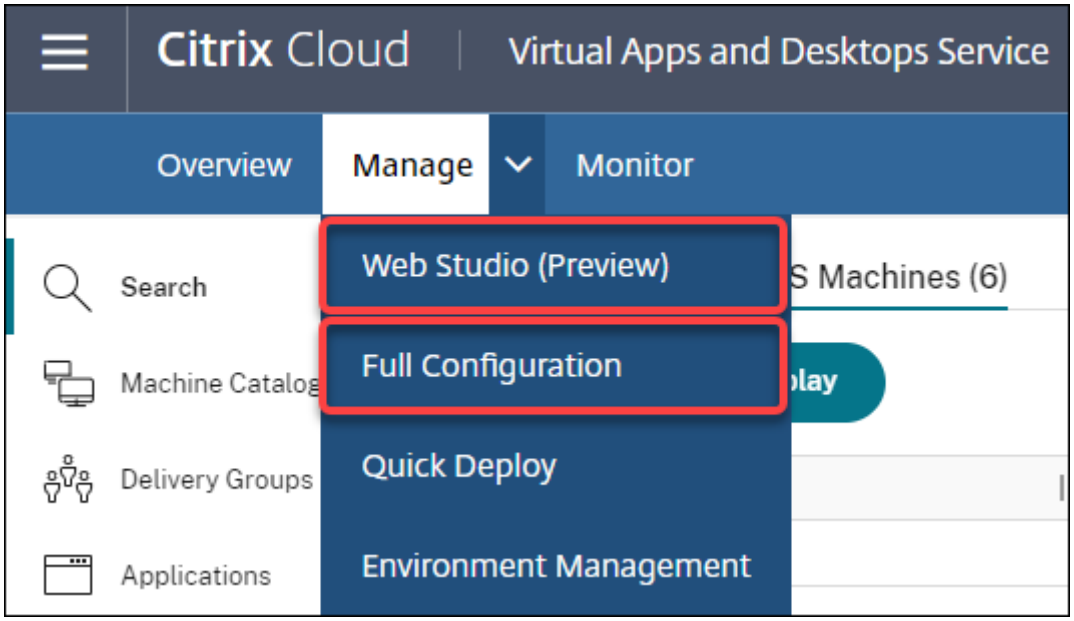


Dezembro 2020

Recursos novos e aprimorados

O Web Studio está disponível na versão Preview. Um novo console baseado na Web já está disponível. Estamos migrando o conjunto completo de funcionalidades do Studio do console legado para o novo console baseado na Web. O console na Web geralmente responde mais rápido do que o console legado. Por padrão, você faz logon automaticamente no console baseado na Web. Você pode alternar facilmente entre o console na Web e o console legado na guia **Manage** para executar suas tarefas de configuração ou gerenciamento de site. Clique na seta para baixo ao lado de **Manage** e selecione uma opção:

- **Web Studio (Preview)**. Leva você para o novo console baseado na Web.
- **Full Configuration**. Leva você para o console legado.



Os seguintes recursos estão disponíveis somente no console na Web:

- **Suporte ao tipo de disco Standard SSD para Azure**. O Studio agora adiciona suporte para o tipo de disco Standard SSD. Os SSDs Standard 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 por meio de uma imagem mestre do Azure Resource Manager.
- **O Studio agora oferece suporte à configuração do atraso de desligamento para grupos de entrega de VDI estáticos**. Anteriormente, era possível configurar o atraso de desligamento para grupos de entrega de VDI estáticos somente 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 de VDI estáticos. Para obter mais informações, consulte AutoScale.

Outubro 2020

Recursos novos e aprimorados

Ignorar vários alertas do Hypervisor. O Citrix Monitor agora suporta ignorar automaticamente alertas do Hypervisor com mais de um dia. Para obter mais informações, consulte Monitoramento de alertas do Hypervisor.

Remover o endereço IP externo. Não é mais necessário usar um endereço IP externo em uma máquina virtual temporária usada para preparar uma imagem provisionada no Google Cloud Platform (GCP). Esse endereço IP externo permite que a máquina virtual temporária acesse a API pública do Google para concluir o processo de provisionamento.

Ative 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 Ativar o acesso privado do Google.

Novo modelo aborda como as identidades de máquinas são gerenciadas. As identidades de máquina usadas em catálogos de máquinas são gerenciadas e mantidas usando o Active Directory. Todas as máquinas criadas pelo MCS agora ingressarão no Active Directory. O novo modelo do Citrix Virtual Apps and Desktops Service aborda como as identidades das máquinas são gerenciadas. Esse modelo permite a criação de catálogos de máquinas usando *grupo de trabalho* ou máquinas não ingressadas no domínio.

> **Dica:**
>
> Essa funcionalidade oferece suporte a um novo serviço de identidade, *FMA trust*, adicionado ao Citrix Cloud para máquinas não ingressadas no domínio.

O MCS se comunica com o novo serviço FMA trust para o gerenciamento de identidades. 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 senha de conta de máquina e SID de domínio usado pelo Active Directory. Os VDAs que usam máquinas não ingressadas no domínio usam essa combinação de GUID e chave privada para registro de agente. Para obter mais informações, consulte Configurar suporte para catálogos não ingressados no domínio.

Usar upload direto para discos gerenciados do Azure. Esta versão permite que você use o carregamento direto ao criar discos gerenciados em um ambiente do Azure. Essa funcionalidade reduz os custos associados a contas de armazenamento extra. 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 conectar 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 usar como um disco gerenciado. Os discos gerenciados suportados incluem Standard HDD, Standard SSD e Premium SSD.

Para obter mais informações sobre esse recurso, consulte o blog do Microsoft Azure.

Para obter mais informações sobre os 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. Esse aprimoramento se aplica às entidades de serviço de escopo completo e de escopo restrito.
O limite de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure estabelecido anteriormente foi removido. Não há mais limite para o número de máquinas virtuais, discos gerenciados, instantâneos e imagens por Grupo de Recursos do Azure.

Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

Setembro 2020

Recursos novos e aprimorados

Quick Deploy. O novo recurso Quick Deploy substitui o Azure Quick Deploy anterior. O novo recurso oferece uma maneira rápida de começar a usar o Citrix Virtual Apps and Desktops Service usando o Microsoft Azure. Você pode usar o Quick Deploy para entregar áreas de trabalho e aplicativos e configurar o acesso ao PC remoto.

Session Administrator (função interna). O Citrix Studio agora adiciona uma nova função interna chamada **Session Administrator**. A função permite que um administrador visualize grupos de entrega e gerencie suas sessões e máquinas associadas na página **Filters** da guia **Monitor**. Com esse recurso você pode definir permissões de acesso de administradores existentes ou administradores que você convidar de uma forma que se alinhe com a função que tem na sua organização. Para obter mais informações sobre a função interna, consulte Escopos e funções internas. Para obter informações sobre como atribuir a função interna a um administrador, consulte Administração delegada e monitoramento.

Para obter um nível mais granular de controle sobre o acesso à página **Filters** relacionada a sessões e máquinas, crie uma função personalizada e selecione uma das seguintes opções para o objeto Director: **View Filters page - Machines only**, **View Filters page - Sessions only**. 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 Premium Disks para um catálogo de máquinas. Para obter mais informações, consulte Criar grupos de entrega.

Agosto 2020

Recursos novos e aprimorados

Acesso limitado ao Remote PowerShell SDK durante uma interrupção. Anteriormente, não era possível 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 não está disponível durante uma interrupção.

Suporte para duas novas edições do Citrix Virtual Apps and Desktops Service. O Citrix Monitor agora suporta duas novas edições do Citrix Virtual Apps and Desktops Service: **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 Citrix Virtual Apps and Desktops Service oferece suporte à 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 a VPC compartilhada, consulte Nuvem privada virtual compartilhada.

Suporte à seleção de zona para o Google Cloud Platform. O Citrix Virtual Apps and Desktops Service oferece suporte à seleção de zona no Google Cloud Platform. Esse recurso permite que os administradores especifiquem uma ou várias zonas em uma região para a criação do catálogo.

Para VMs do tipo locatário único, a seleção de zona fornece aos administradores a capacidade de posicionar nós de locatário único nas zonas de sua escolha. Para VMs de locatário não único, a seleção de zona fornece a capacidade de posicionar VMs de forma determinística entre as zonas de sua escolha, proporcionando flexibilidade no projeto da implantação. Para obter informações sobre configuração, consulte Habilitar a seleção de zona.

Além disso:

- A locação única fornece acesso exclusivo a um único nó de locatário, que é um servidor físico com 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 BYOL (traga sua própria licença). Eles também permitem que você cumpra os requisitos da política de controle de acesso à rede, segurança e privacidade, como a HIPAA.

> **Nota:**
>
> A locação única é o único caminho possível para usar as implantações de VDI do Windows 10 no Google Cloud. O Server VDI também é compatível com esse método. Uma descrição detalhada da locação única pode ser encontrada no site de documentação do Google.

Melhor desempenho de inicialização para discos de sistema Azure. Esta versão oferece suporte que ajuda a melhorar o desempenho de inicialização para implementações do Citrix Cloud usando o Azure quando o MCSIO está habilitado. Com esse suporte, você pode reter o disco de sistema. Isso oferece as seguintes vantagens:

- As VMs e os aplicativos agora inicializam e iniciam com desempenho semelhante ao da transmissão da imagem de ouro.
- Redução no consumo de cota da API, exclusão e criação do disco de sistema e atraso na transição de estado causado quando você exclui uma VM.

Por exemplo, use a propriedade personalizada do PowerShell `PersistOSDisk` 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>'
<!--NeedCopy-->
```

Para obter mais informações sobre configuração, consulte Melhorar o desempenho de inicialização.

Julho 2020

Recursos novos e aprimorados

Suporte ao acesso granular e baseado em função da página de filtros. O Citrix Studio agora fornece um controle de acesso mais granular à página **Monitor > Filters** quando você cria uma função personalizada. Especificamente, você pode atribuir permissões para visualizar qualquer combinação de **máquinas**, **sessões**, **conexões** e **instâncias de aplicativos** a uma função personalizada. Veja a seguir mais quatro opções para o objeto **Director** na janela **Create Role** :

- View Filters page - Application Instances only
- View Filters page - Connections only
- View Filters page - Machines only
- View Filters page - Sessions only

Para obter informações sobre como criar funções, consulte Criar e gerenciar funções.

Suporte a atraso de desligamento para máquinas VDI atribuídas (somente PowerShell). Em versões anteriores, o atraso de desligamento era aplicado somente a máquinas não atribuídas. A partir desta versão, o atraso de desligamento se aplica a máquinas atribuídas e não atribuídas. Para obter mais informações, consulte Como a energia de AutoScale gerencia as máquinas.

Suporte para licenças do Windows Client. O Citrix Virtual Apps and Desktops Service agora oferece suporte ao uso de licenças do Windows Cliente para provisionar máquinas virtuais no Azure. Para executar VMs do Windows 10 no Azure, verifique se o seu contrato de licenciamento por volume com a Microsoft o qualifica para esse uso. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem mestre do Azure Resource Manager.

Maio 2020

Recursos novos e aprimorados

Agendamentos de reinicialização da máquina. Agora você pode indicar se um agendamento de reinicialização afeta as máquinas que estão no modo de manutenção. Este recurso está disponível apenas no PowerShell. Para obter detalhes, consulte Reinicializações agendadas para máquinas no modo de manutenção.

Disponibilidade de recursos. Agora você pode garantir a disponibilidade dos recursos durante uma interrupção sem precisar publicar recursos em todas as zonas (localização do recurso). Para obter detalhes, consulte Disponibilidade de recursos.

Abril 2020

Recursos novos e aprimorados

Granularidade de agendamento aprimorada para grupos de entrega de VDI (somente PowerShell). O AutoScale agora suporta a definição dos horários de pico para os dias incluídos em uma programação em um nível granular de 30 minutos. Você pode definir o número mínimo de máquinas em execução em um grupo de entrega de VDI separadamente para cada meia hora do dia. Além disso, o AutoScale agora pode aumentar ou diminuir o número de máquinas ligadas nos grupos de entrega de VDI a cada meia hora, em vez de a cada hora. Para obter mais informações, consulte Comandos do Broker PowerShell SDK.

Descoberta de MTU. O protocolo Citrix Enlightened Data Transport (EDT) agora tem 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. Esse recurso permite que a sessão ICA se ajuste a redes com requisitos não padrão de MTU (Unidade Máxima de Transmissão) ou MSS (Tamanho Máximo de Segmento). A capacidade de ajuste evita a fragmentação de pacotes que pode resultar em desempenho degradado ou falha para estabelecer uma sessão ICA. Esta atualização requer, no mínimo, o aplicativo Citrix Workspace 1911 para Windows. Se estiver usando o Citrix Gateway, a versão mínima do firmware do Citrix ADC necessária é 13.0.52.24 ou 12.1.56.22. Para obter mais informações, consulte Descoberta de MTU em EDT.

Março 2020

Recursos novos e aprimorados

Métricas do dispositivo de destino PVS. O Citrix Monitor agora fornece um painel de métricas do dispositivo de destino PVS na página Machine Details. Use o painel para exibir o status dos disposi-

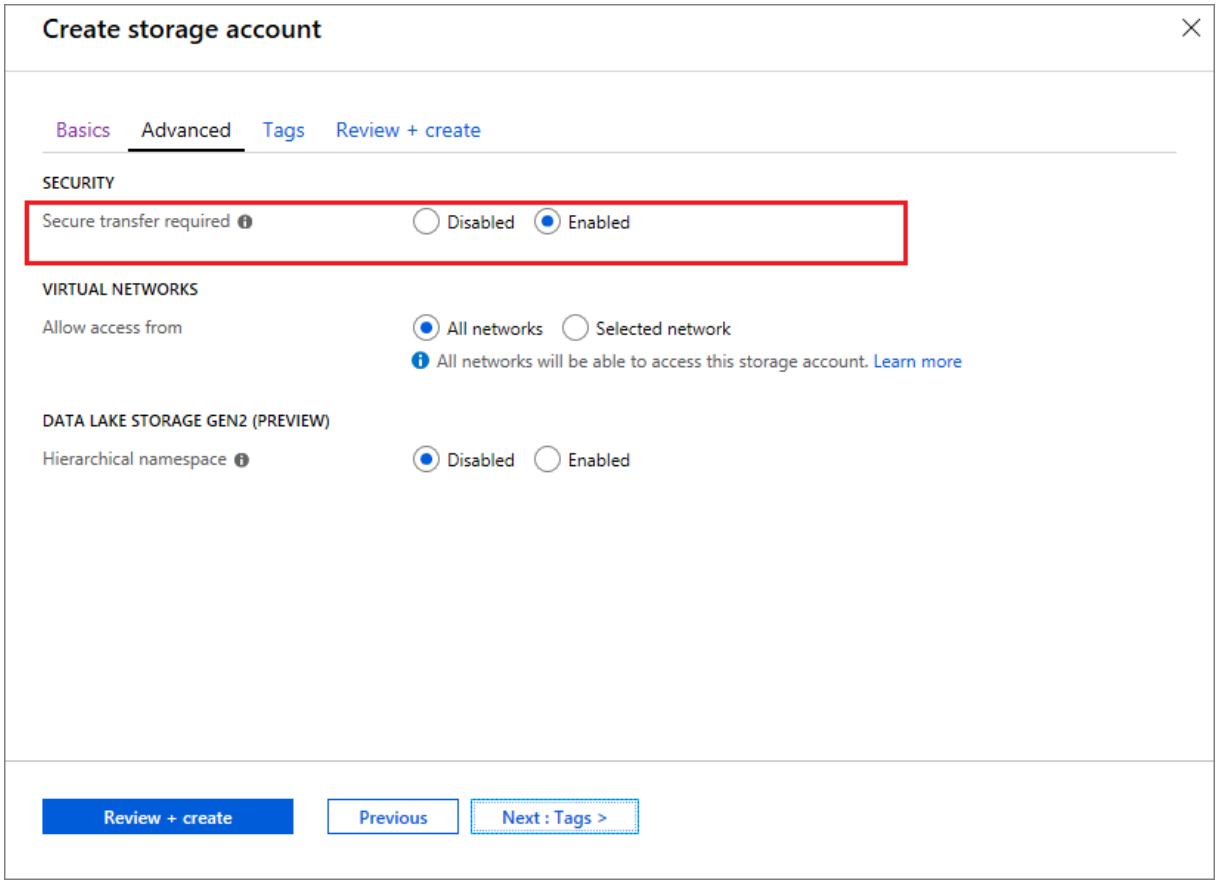
tivos de destino do Provisioning de máquinas com SO de sessão única e multissessão. Várias métricas de Network, Boot e Cache estão disponíveis nesse painel. Essas métricas ajudam você a monitorar e solucionar problemas de dispositivos de destino PVS para garantir que estejam em condições de funcionamento adequadas. Para obter mais informações, consulte Métricas do dispositivo de destino PVS.

Captura de propriedade de instâncias da AWS. O MCS agora lê as propriedades da instância a partir da qual a AMI foi obtida e aplica a função do IAM e as marcas da máquina às máquinas provisionadas de um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo localiza a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são armazenadas em um Launch Template da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturada. Para obter mais informações, consulte Captura de propriedade de instâncias da AWS.

Marcação de recursos operacionais da AWS. Esta versão apresenta uma opção para marcar recursos criados pelos componentes Citrix durante o provisionamento. Cada marca 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) fornece um aprimoramento para contas de armazenamento criadas por catálogos provisionados pelo MCS em ambientes do Azure Resource Manager. Esse aprimoramento habilita automaticamente a propriedade de transferência segura obrigatória. Essa opção aumenta a segurança da conta de armazenamento permitindo somente solicitações à conta a partir de conexões seguras. Para obter mais informações, consulte Exigir transferência segura para garantir conexões seguras no site da Microsoft.

Ative a propriedade **Transferência segura obrigatória** 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 Standard para máquinas virtuais do Azure. Esse tipo de disco fornece desempenho consistente e oferece melhor disponibilidade em comparação aos discos HDD. Para obter mais informações, consulte Discos SSD Standard para cargas de trabalho de máquinas virtuais do Azure.

Use a propriedade personalizada do PowerShell `StorageAccountType` no comando `New-ProvScheme` ou no comando `Set-ProvScheme` para configurar o recurso:

```
1 <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
    true`" /><Property xsi:type=`"StringProperty`" Name=`"
    StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type
    =`"StringProperty`" Value=`"Windows_Server`" />
2 <!--NeedCopy-->
```

> **Nota:**
>
> Esse recurso só está disponível ao usar discos gerenciados, ou seja, a propriedade personalizada `UseManagedDisks` definida como **true**. Para discos não gerenciados, somente HDD Standard e SSD Premium são suportados.

Janeiro 2020

Recursos novos e aprimorados

Barra de idiomas no Citrix Studio. A partir desta versão, o Citrix Studio fornece 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 será exibida.
- 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 será exibida depois que você fizer logon no Citrix Studio. Há duas opções de idioma na lista da barra de idiomas. Selecione uma opção que corresponda ao idioma mais alto do seu navegador.

> **Dica:**
>
> ```
> - Settings that you configure for the language bar might not take effect. In this case, log out and log back on.
> - You might fail to input certain symbols and localized characters by using the language bar. To resolve the issue, you need to configure the language of Citrix Cloud, the display language of your browser, and the local keyboard layout. For more information, see Knowledge Center article [CTX310743](https://support.citrix.com/article/CTX310743).
> ```

Temporizador de atraso máximo de agendamento de reinicialização (somente PowerShell). Se uma reinicialização agendada de máquinas em um Grupo de Entrega não começar devido a uma interrupção do banco de dados do site, você poderá especificar quanto tempo esperar além da hora de início agendada. Se a conexão do banco de dados for restaurada durante esse intervalo, as reinicializações serão iniciadas. Se a conexão não for restaurada durante esse intervalo, as reinicializações não serão iniciadas. Para obter detalhes, consulte Reinicializações programadas atrasadas devido à interrupção do banco de dados.

Balanceamento de carga vertical (somente PowerShell). Anteriormente, o serviço usava o balanceamento de carga horizontal para todas as execuções do RDS, o que atribui a carga de entrada à máquina RDS menos carregada. Isso continua sendo o padrão. Agora, você pode usar o PowerShell para habilitar o balanceamento de carga vertical como uma configuração para todo o site.

Quando o balanceamento de carga vertical está ativado, o agente 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 as novas máquinas. À medida que os usuários se desconectam e liberam as máquinas existentes, uma nova carga é atribuída às máquinas.

Por padrão, o balanceamento de carga horizontal está habilitado. Para exibir, habilitar ou desabilitar o balanceamento de carga vertical, os cmdlets `Get-BrokerSite` e `Set-BrokerSite`agora

oferecem suporte à configuração `UseVerticalScalingForRdsLaunches`. Para obter mais informações, consulte Carregar máquinas gerenciadas em Grupos de entrega.

Dezembro 2019

Recursos novos e aprimorados

Serviço para Citrix Service Providers (CSP). Os CSPs agora podem integrar clientes locatários ao serviço do 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 Citrix Service Provider.

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 isso, use o parâmetro `-MaintenanceModeReason`. O recurso é útil para que os administradores solucionem 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 máquinas e excluí-las dinamicamente. Você pode aproveitar o recurso usando um script do PowerShell. O script ajuda a aumentar ou diminuir dinamicamente o número de máquinas no grupo de entrega com base nas condições de carga atuais. Para obter mais informações, consulte Provisionar máquinas dinamicamente com AutoScale.

Novembro 2019

Recursos novos e aprimorados

GroomStartHour. O Monitor agora oferece suporte a **GroomStartHour** –uma nova configuração que ajuda os administradores a determinar a hora do dia em que a limpeza deve começar. Para obter mais informações, consulte a documentação do Citrix Virtual Apps and Desktops SDK.

Paginação OData. O Monitor agora suporta a **paginação OData**. Todos os pontos de extremidade do 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 Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Outubro 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 na sua configuração do Citrix Cloud no modo de administração simples ou dupla. O *Virtual Apps and Desktops Service App-V package discovery module*, disponível no Citrix Downloads, permite importar pacotes App-V e registrar servidores Microsoft App-V. Os aplicativos contidos ficam disponíveis para seus usuários. Esse módulo do PowerShell permite que você registre Microsoft App-V Management and Publishing Servers usando URLs DNS sem precisar que os servidores por trás dos mecanismos de balanceamento de carga sejam registrados usando o URL real da máquina. Para obter mais informações, consulte Módulo de descoberta do serviço Citrix Virtual Apps and Desktops para pacotes e servidores App-V.

Google Cloud Platform. O Citrix Virtual Apps and Desktops Service agora adiciona suporte ao uso do 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 2019

Recursos novos e aprimorados

Suporte VDA para a Área de Trabalho Virtual do Azure. Para ver os sistemas operacionais compatíveis e as versões de VDA, consulte VDAs em um ambiente de Área de Trabalho Virtual do Azure.

Política de energia aprimorada. Em versões anteriores, uma máquina VDI fazendo a transição para um período em que era necessária uma ação (ação de desconexão="**Suspend**"ou "**Shutdown**") tinha que permanecer ligada. Esse cenário ocorria se a máquina se desconectasse durante um período de tempo (horários de pico ou fora de pico) em que não era necessária nenhuma ação (ação de desconexão="**Nothing**").

A partir desta versão, o AutoScale suspende ou desliga a máquina quando o tempo de desconexão especificado é decorrido, dependendo da ação de desconexão configurada para o período de destino. Para obter mais informações, consulte Gerenciar a energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas.

Catálogos de máquinas: marcas. Agora você pode usar o PowerShell para aplicar tags a catálogos de máquinas. Para obter mais informações, consulte Aplicar marcas a catálogos de máquinas.

Duração do início da sessão. O Monitor agora exibe a duração da inicialização da sessão dividida nos períodos de tempo de inicialização da sessão do aplicativo Workspace e de inicialização da sessão do VDA. Esses dados ajudam você a entender e solucionar problemas de alta duração na inicialização da sessão. Além disso, a duração de tempo de cada fase envolvida na inicialização da sessão ajuda na

solução de problemas associados a fases individuais. Por exemplo, se o tempo de mapeamento da unidade for alto, você poderá verificar se todas as unidades de disco válidas estão mapeadas corretamente no GPO ou no script. Esse recurso está disponível nos VDAs 1903 ou posteriores. Para obter mais informações, consulte Diagnosticar problemas de inicialização de sessão.

Agosto 2019

Recursos novos e aprimorados

Reconexão automática de sessão. A página Sessions na guia Trends agora inclui informações sobre o número de reconexões automáticas. A reconexão automática é realizada quando as políticas Session Reliability ou Auto Client Reconnect 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 facilidade.

A análise detalhada fornece informações adicionais, como dados de confiabilidade da sessão ou reconexão automática de cliente, carimbos de hora, IP do ponto de extremidade e nome do ponto de extremidade da máquina em que o aplicativo Workspace está instalado. Esse recurso está disponível para o aplicativo Citrix Workspace para Windows, aplicativo Citrix Workspace para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Esse recurso requer VDAs 1906 ou posterior. 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 2019

Recursos novos e aprimorados

Log de configuração. Agora você pode usar o SDK do PowerShell remoto para excluir periodicamente o conteúdo do banco de dados Configuration Logging. Para obter detalhes, consulte Agendar a exclusão periódica de dados.

AutoScale. O AutoScale agora fornece a flexibilidade para gerenciar a energia de somente um subconjunto de máquinas em um grupo de entrega. Esse recurso pode ser útil em casos de uso de intermitência da nuvem, em que você deseja usar recursos locais para lidar com cargas de trabalho antes que os recursos baseados em nuvem abordem outras demandas (ou seja, cargas de trabalho intermitentes). Para obter mais informações, consulte Restringir o AutoScale a determinadas máquinas em um grupo de entrega.

Acesso a aplicativo local e redirecionamento de URL. O Citrix Studio agora permite adicionar a opção Add Local App Access Application à interface de usuário do Studio para o seu site usando o SDK do PowerShell. Para obter mais informações, consulte Fornecer acesso apenas a aplicativos publicados.

Alterações no nome do sistema operacional. Os nomes do sistema operacional nas páginas **Create Machine Catalog > Machine Catalog Setup > Operating System** e **Monitor** foram alterados:

- SO multissessão (anteriormente Server OS): o catálogo de máquinas do SO de várias sessões fornece áreas de trabalho compartilhadas hospedadas para uma implantação em larga escala de máquinas Windows padronizadas com múltiplas sessões ou sistema operacional Linux.
- SO de sessão única (anteriormente Desktop OS): o catálogo de máquinas de SO de sessão única fornece áreas de trabalho VDI, ideal para vários usuários.

Duração do Citrix Profile Management no carregamento do perfil. O Monitor agora inclui a duração do processamento de perfil na barra de carregamento de perfil do gráfico de duração de logon. Essa é a duração que o Citrix Profile Management leva para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de carregamento de perfil com maior precisão. Esse aprimoramento está disponível em VDAs 1903 e posteriores. Para obter mais informações, consulte Carregamento de perfil.

Investigação da área de trabalho. A sondagem de área de trabalho é um recurso do Citrix Virtual Apps and Desktops Service. Ele automatiza as verificações de integridade de áreas de trabalho virtuais publicadas em um site, o que melhora a experiência do usuário. Para iniciar a sondagem de área de trabalho, instale e configure o Citrix Probe Agent em um ou mais pontos de extremidade. A investigação de área de trabalho está disponível para sites licenciados Premium. Esse recurso requer o Citrix Probe Agent 1903 ou posterior. Para obter mais informações, consulte Investigação de aplicativo e área de trabalho.

> **Nota:**
>
> O Citrix Probe Agent agora oferece suporte a TLS 1.2.

Junho 2019

Recursos novos e aprimorados

Restringir por marcas. Marcas são cadeias de caracteres que identificam itens como máquinas, aplicativos, áreas de trabalho, grupos de aplicativos e políticas. Depois de criar uma marca e adicioná-la a um item, você pode personalizar certas operações para aplicá-las apenas a itens que têm uma marca especificada. Para obter mais informações, consulte Grupos de aplicativos e Marcas.

Notificações por e-mail. O Citrix Virtual Apps and Desktops Service envia diretamente notificações por e-mail relacionadas a alertas e investigações. Isso elimina a necessidade de configurar o servi-

dor de e-mail SMTP. A caixa **Notification Preferences** está ativada por padrão e o Citrix Cloud envia notificações de alerta para os endereços de e-mail fornecidos na seção **Notification Preferences**. Certifique-se de que o endereço de e-mail `donotreplynotifications@citrix.com` esteja na lista branca em sua configuração de e-mail.

Maio 2019

Recursos novos e aprimorados

AutoScale. AutoScale é um recurso do Citrix Virtual Apps and Desktops Service que fornece uma solução consistente e de alto desempenho para gerenciar a energia de suas máquinas de forma proativa. O objetivo é equilibrar os custos e a experiência do usuário. O AutoScale incorpora a tecnologia preterida do Smart Scale 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 Trends na guia **Monitor**. Para obter mais informações, consulte Monitorar máquinas gerenciadas por AutoScale.

Fevereiro 2019

Recursos novos e aprimorados

Monitoramento de alertas do Hypervisor. Os alertas do Citrix Hypervisor e do VMware vSphere agora são exibidos na guia **Monitor** > **Alerts** para ajudar a monitorar os seguintes estados/parâmetros da integridade do hipervisor:

- Uso de CPU
- Uso de memória
- Uso de rede
- Conexão com o Hypervisor não disponível
- Uso de disco (somente vSphere)
- Conexão do host ou estado de energia (somente vSphere)

Para obter mais informações, consulte a seção Monitoramento de alertas do Hypervisor em Alertas e notificações.

Comunicações por versões de TLS anteriores. Para melhorar a segurança do serviço, a Citrix bloqueará qualquer comunicação por Transport Layer Security (TLS) 1.0 e 1.1 a partir de 15 de março de 2019, permitindo apenas comunicações por TLS 1.2. Para obter mais informações, consulte Versões de TLS. Para obter orientação abrangente, consulte CTX247067.

Grupos de aplicativos. Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos que são compartilhados entre diferentes grupos de

entrega ou usados por um subconjunto de usuários dentro de grupos de entrega. Para obter mais informações, consulte Criar grupos de aplicativos.

Desempenho de logon –Detalhamento do perfil. O painel **Logon Duration** na página **User Details** em **Monitor** agora inclui informações sobre o detalhamento de **Profile load phase** do processo de logon. O detalhamento do perfil fornece informações úteis sobre os perfis de usuário da sessão atual que podem ajudar os administradores a solucionar problemas de carga de perfil alta. 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 aprofundado fornece informações sobre as pastas individuais, com tamanhos e número de arquivos. Esse recurso está disponível nos VDAs 1811 e posteriores. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Integridade da licença do Microsoft RDS. Monitore o status da licença do Microsoft RDS (Serviços de Área de Trabalho Remota) no painel **Detalhes da máquina** na página Detalhes da máquina e Detalhes do usuário nas máquinas com Server OS. 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 de integridade da licença do Microsoft RDS em Solução de problemas de máquinas.

Investigação de aplicativo. Esse recurso automatiza a avaliação da integridade dos aplicativos virtuais publicados em um site.

Para iniciar a investigação do aplicativo:

- Em uma ou mais máquinas de ponto de extremidade, instale o Citrix Application Probe Agent.
- Configure o Citrix Application Probe Agent com as credenciais do Citrix Workspace e do Citrix Virtual Apps and Desktops Service.
- Configure os aplicativos a serem investigados, as máquinas de ponto de extremidade nas quais executar a sondagem e a hora agendada da sondagem em **Monitor** > **Configuration** do Citrix Virtual Apps and Desktops Service.

O agente testa a inicialização do aplicativos selecionados por meio do Citrix Workspace e relata os resultados da sondagem na guia **Monitor** do Citrix Virtual Apps and Desktops Service:

- na página Applications —os dados das últimas 24 horas e na página **Trends** > **Application Probe Results**
- nos dados históricos de investigação juntamente com o estágio em que a falha de sondagem ocorreu: Workspace Reachability, WorkspaceAuthentication, WorkspaceEnumeration, ICA download ou Application launch

O relatório de falhas é enviado para os endereços de e-mail configurados. Você pode agendar as investigações do aplicativo para serem executadas fora do horário de pico em várias localizações geográficas. Dessa forma, você pode usar os resultados para solucionar problemas proativamente relacionados a aplicativos provisionados, máquinas de hospedagem ou conexões antes que os usuários enfrentem esses problemas. Para obter mais informações, consulte Investigação de aplicativo e área de trabalho.

Janeiro 2019

Recursos novos e aprimorados

Administração delegada com escopo personalizado. O monitoramento agora oferece suporte a escopo personalizado para funções internas de administrador delegado. Para obter mais informações sobre as funções internas disponíveis para monitoramento e como atribuí-las, consulte Funções de administrador delegado.

Dezembro 2018

Recursos novos e aprimorados

A data após a qual a Citrix bloqueará a comunicação por Transport Layer Security (TLS) 1.0 e 1.1 foi alterada de 31 de dezembro de 2018 para 31 de janeiro de 2019. Para obter detalhes, consulte Substituição das versões de TLS.

Novembro 2018

Recursos novos e aprimorados

Dados históricos da máquina disponíveis usando a API OData: os dados históricos que contêm análise de máquina agora estão disponíveis por meio da API OData. Esses dados são coletados por 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 pelo período de tempo durante o qual o Monitoring Service está sendo executado. 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 –análise detalhada da sessão interativa: o painel **Logon Duration** na exibição **User and Session Details** inclui informações sobre a fase **Interactive Session** do processo de logon. O tempo gasto para cada uma das três subfases (**Pre-userinit**, **Userinit** e **Shell**) é exibido na barra **Interactive Session** como uma dica de ferramenta. Isso fornece maior granularidade de solução de problemas e correção dessa fase do logon. O atraso cumulativo entre as subfases e um link à documentação também é fornecido. Esse recurso está disponível no Delivery Controller versão 7 1808 e posterior. A barra de detalhamento da **Interactive Session** mostra o tempo de duração somente da sessão atual. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Desempenho de logon –detalhamento de GPO: o painel **Logon Duration** na exibição detalhada **User and Session** contém a duração do GPO (objeto de política de grupo). Esse é o tempo total necessário 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 os CSEs (extensão do lado do cliente) como uma dica de ferramenta na barra do GPO. Para cada aplicativo de política, o detalhamento exibe o status e o tempo gasto. Essas informações adicionais facilitam a solução de problemas e a correção de problemas que envolvem alta duração do GPO. As durações de tempo no detalhamento representam apenas o tempo de processamento do CSE e não somam o tempo total do GPO. Esse 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 a relatórios personalizados salvas durante o monitoramento não ficam disponíveis após uma atualização do Cloud. [DNA-23420]

Outubro 2018

Recursos novos e aprimorados

Aplicativos: limite por máquina. Agora você pode limitar o número de instâncias de aplicativos por máquina. Esse limite se aplica a todas as máquinas no site. Esse limite é um acréscimo ao limite do aplicativo existente para todos os usuários no grupo de entrega e ao limite por usuário. O recurso está disponível somente por meio do PowerShell, não no Studio. Para obter detalhes, consulte Configurar limites de aplicativos.

Windows Server 2019. Agora você pode instalar VDAs para SO multissessão (anteriormente VDAs para Server OS) em máquinas Windows Server 2019, conforme observado nos Requisitos do sistema.

Setembro 2018

Recursos novos e aprimorados

Administração delegada. Com a administração delegada, você pode configurar as permissões de acesso de que todos os seus administradores precisam, de acordo com suas funções na organização. Para obter detalhes, consulte Administração delegada. O monitoramento oferece suporte à alocação de funções internas. As funções internas estão disponíveis com o escopo completo. Para obter mais informações sobre funções internas para monitoramento e como atribuí-las, consulte Funções de administrador delegado.

Log de configuração. O log de configuração permite que os administradores acompanhem as alterações de configuração e as atividades administrativas. Para obter detalhes, consulte Log de configuração.

Vários cmdlets do PowerShell no SDK do PowerShell remoto que estavam desabilitados anteriormente agora estão habilitados para usar com o Configuration Logging:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Cache do host local. O cache do 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 recursos não pode se comunicar com o Citrix Cloud. Para obter detalhes, consulte Cache do host local.

Citrix Provisioning. Para provisionar VDAs, agora você pode usar o Citrix Provisioning ou o Machine Creation Services. Para obter informações sobre o 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, somente as máquinas virtuais em pools são excluídas. As máquinas virtuais persistentes (dedicadas) não são excluídas quando desligadas.

Agosto 2018

- **Novos nomes de produtos**

Se você já é cliente ou parceiro da Citrix há algum tempo, notará novos nomes em nossos produtos e na documentação deste produto. Se este produto Citrix é novo para você, poderá ver nomes diferentes para um produto ou componente.

Os novos nomes de produtos e componentes derivam do portfólio em expansão da Citrix e da estratégia de nuvem. Os artigos na documentação deste produto usam os seguintes nomes.

- **Citrix Virtual Apps and Desktops:** o Citrix Virtual Apps and Desktops oferece uma solução para aplicativos e áreas de trabalho virtuais, fornecida como um serviço de nuvem e como um produto local, oferecendo aos funcionários a liberdade de trabalhar de qualquer lugar em qualquer dispositivo, reduzindo os custos de TI. Entregue aplicativos Windows, Linux, Web e SaaS ou áreas de trabalho virtuais completas de qualquer nuvem: pública, local ou híbrida. Virtual Apps and Desktops era, anteriormente, XenApp e XenDesktop.
- **Aplicativo Citrix Workspace:** o aplicativo Citrix Workspace incorpora a tecnologia Citrix Receiver existente e as outras tecnologias cliente do Citrix Workspace. Ele foi aprimorado para oferecer mais recursos para fornecer aos usuários finais uma experiência contextual unificada, onde eles podem interagir com todos os aplicativos, arquivos e dispositivos de trabalho necessários para trabalhar com eficiência. Para obter mais informações, consulte esta postagem no blog.
- **Citrix SD-WAN:** o NetScaler SD-WAN, uma tecnologia crucial para nossos clientes e parceiros que estão transformam suas redes de filiais e WANs com a tecnologia de nuvem, agora é chamado de Citrix SD-WAN.
- **Citrix Secure Web Gateway:** à medida que o portfólio do Citrix Networking se expande, nos orgulhamos em oferecer nosso serviço robusto 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 fazer o seu trabalho melhor, agora é o Citrix Gateway.
- **Citrix Content Collaboration e Citrix Files for Windows:** os recursos avançados de acesso, colaboração, fluxo de trabalho, gerenciamento de direitos e integração do ShareFile agora estão disponíveis nos componentes do Citrix Content Collaboration, unificados a nosso Citrix Workspace seguro, contextual e integrado. O Citrix Files para Windows permite que você acesse seus arquivos do Content Collaboration diretamente através de uma unidade mapeada, proporcionando a mesma experiência nativa do Windows Explorer.
- **Citrix Hypervisor**: a tecnologia do XenServer para infraestrutura de virtualização, baseada no hipervisor XenProject, agora passou a ser Citrix Hypervisor.

Eis aqui uma rápida recapitulação:

É	Era
Citrix Virtual Apps and 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

Implementar essa transição em nossos produtos e em sua documentação é um processo contínuo.

- O conteúdo no produto ainda pode apresentar nomes antigos. Por exemplo, você pode ver instâncias de nomes anteriores no texto, nas mensagens e no nome de diretórios/arquivos do console.
- É possível que alguns itens, como comandos e MSIs, continuem a manter seus nomes antigos para evitar a quebra de scripts de clientes existentes.
- A documentação do produto relacionada e outros recursos (como vídeos e postagens de blog) que estão vinculados a partir da documentação deste produto ainda poderão conter nomes antigos.
- Para o Citrix Hypervisor, o novo nome é usado no site da Citrix e em materiais de produtos informativos a partir de setembro de 2018. Você também verá o novo nome nos consoles de administração de alguns produtos Citrix, como o Citrix Virtual Apps and Desktops. A versão do produto XenServer e os materiais de documentação técnica continuam a usar o XenServer 7.x até o início de 2019.

Agradecemos a sua paciência durante esta transição.

Para obter mais detalhes sobre nossos novos nomes, consulte https://www.citrix.com/about/citrix-product-guide/.

- **Alterações no número da versão do produto e do componente**

A Citrix instala e gerencia a maioria dos componentes do Citrix Virtual Apps and Desktops, para que você não precise se preocupar com seus números de versão. No entanto, você pode ver os

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: **AAMM.*c.m.b***

- AAMM = Ano e mês em que o produto ou componente foi lançado. Por exemplo, uma versão de setembro de 2018 aparece como 1809.
- c = o número da versão do Citrix Cloud para o mês.
- m = versão de manutenção (se aplicável).
- b = número de compilação (build). Esse campo é mostrado somente 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 ao Citrix Cloud versão 1 naquele mês e não é uma versão de manutenção. Alguns monitores 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*, com a versão incrementada em um para cada lançamento. Por exemplo, a versão do VDA seguinte ao XenApp e XenDesktop 7.17 foi a 7.18. Versões anteriores (7.18 e anteriores) não serão atualizadas com o novo formato de numeração.

- **Substituição das versões de TLS.** Para melhorar a segurança do Citrix Virtual Apps and Desktops Service, a Citrix bloqueará qualquer comunicação através do Transport Layer Security (TLS) 1.0 e 1.1 a partir de 31 de dezembro de 2018. Para obter detalhes, consulte Substituição das versões de TLS.
- **Ambiente de virtualização do Google Cloud Platform.** O Citrix Virtual Apps and Desktops Service oferece suporte à capacidade de ligar manualmente as máquinas virtuais de Virtual Apps and Desktops no Google Cloud Platform (GCP). Para obter mais informações, consulte Ambientes de virtualização do Google Cloud Platform.

Julho 2018

- **Exportação de dados de filtros.** Agora você pode exportar dados de monitoramento em tempo real na guia **Monitor** > **Filters** 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 oferecem uma visão abrangente dos dados em tempo real e ajudam a facilitar a análise de grandes conjuntos de dados.

Junho 2018

- **Conexões do Azure Resource Manager.** No assistente de criação de conexão do Studio, a seleção de ambiente do Azure na página **Connection** inclui todas as nuvens do Azure válidas para a sua assinatura do Azure. A disponibilidade geral do Azure US Government Cloud e do Azure Germany Cloud substitui as versões preview desses dois ambientes em versões anteriores.

Maio 2018

- **Azure Quick Deploy.** Agora, quando o local do seu recurso usa máquinas do Azure Resource Manager para entregar aplicativos e áreas de trabalho, você pode escolher um método de implantação:
  - Full Configuration: esse método existente usa o console de gerenciamento do Studio, que o orienta na criação de um catálogo de máquinas e na criação de um grupo de entrega.
  - Azure Quick Deploy: essa nova opção fornece uma interface mais simples que oferece implantação mais rápida de aplicativos e áreas de trabalho.
- **Link do Citrix Health Assistant.** A página Machine Details de uma máquina não registrada no console do Monitoring agora contém um botão **Health Assistant**. Atualmente, o botão está vinculado a Troubleshoot machines e ao artigo do Knowledge Center Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch, 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 integridade para identificar possíveis causas de problemas comuns de registro do VDA, início de sessão e configuração de redirecionamento de fuso horário.
- **Análise detalhada da sessão interativa.** No console de monitoramento, o painel **User Details view > Logon Duration** agora inclui informações sobre o estágio **Interactive Session** do processo de logon. Para fornecer maior granularidade de solução de problemas e correção dessa fase do logon, a **Sessão Interativa** agora tem três subfases: **Pre-userinit**, **Userinit** e **Shell**. Nesta versão, passar o mouse sobre a **Interactive Session** exibe uma dica de ferramenta mostrando as subfases e um link à documentação. Para obter uma descrição das subfases e como melhorar o desempenho de cada fase, consulte Diagnosticar problemas de logon do usuário.

Março 2018

- **Previsão de instâncias de aplicativo (recurso em preview).** Esse 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 instância do aplicativo indica o número de instâncias do aplicativo hospedadas que provavelmente serão iniciadas por site ou grupo de entrega com o 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 Director. Envie seus comentários sobre a utilidade e a usabilidade desse recurso no fórum de discussão do Citrix Cloud.

- **APIs de grupos de entrega —Preview**

  O preview de 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 no Web Studio**

  O console de gerenciamento de serviços 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 do grupo de entrega.

- **Acesse os dados do Monitor Service usando a API do OData Versão 4 (recurso em preview)**

  Você pode criar seus painéis personalizados de monitoramento e relatórios com base nos dados do Monitor Service usando o ponto de extremidade 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 e token de portador do Citrix Cloud para acessar os dados com o ponto de extremidade V4. Para obter mais informações e exemplos, consulte Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Compartilhe seu feedback sobre a utilidade desse recurso no fórum de discussão do Citrix Cloud.

Correções

- Você pode renomear, mover e excluir pastas de aplicativos. [#STUD-2376]

Janeiro 2018

- **Verificação de licença RDS.** A criação de catálogos de máquinas contendo máquinas com Windows Server OS agora inclui uma verificação automática de licença RDS. Todos os problemas en-

contrados com a licença RDS são exibidos, para que você possa tomar as medidas apropriadas para evitar uma lacuna no serviço. Para obter detalhes, consulte Criar catálogos de máquinas.

- **Acesso ao console da máquina a partir do Monitor.** O painel de detalhes da máquina do Monitor agora fornece acesso aos consoles de máquinas hospedadas no XenServer Hypervisor 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 2017

Recursos novos e aprimorados

- **Citrix Workspace.** O Citrix Workspace agora está disponível para **novos** clientes do XenApp e XenDesktop Service. Para obter mais informações, consulte Configuração do Workspace.
- **Análise de aplicativos.** Agora você pode analisar e monitorar o desempenho dos aplicativos de forma eficiente com a nova página Application Analytics disponível na guia **Monitor** > **Applications**. A página fornece uma exibição consolidada da integridade e do uso de todos os aplicativos publicados no seu site. Ela mostra métricas, tais 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 2017

Recursos novos e aprimorados

- **Cache do host local.** O cache de host local permite que as operações de intermediação de conexão continuem quando um Cloud Connector em um local de recursos não pode se comunicar com o Citrix Cloud. Para obter detalhes, consulte Cache do host local.
- **Discos gerenciados do Azure.** Os discos gerenciados do Azure agora são usados por padrão para máquinas virtuais provisionadas pelo 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 serviços de uma conta de cliente do Citrix Cloud, agora você tem uma nova opção: Help Desk Administrator. Um administrador de help desk pode acessar as funções do Monitor no serviço. Para obter detalhes, consulte Gerenciar.

Correções

- Agora você pode usar o assistente do console de gerenciamento de serviços para criar um catálogo de máquinas de acesso ao PC remoto. Em versões anteriores, você tinha que usar um cmdlet do PowerShell para criar um catálogo (conforme documentado em CTX220737). Depois, você tinha que 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 pelo MCS podem usar contas de máquina existentes do Active Directory. [#DNA -24566]
- Ao monitorar uma implantação, rolar a tabela classificada em **Trends > Sessions** exibe resultados precisos. [DNA-51257]

Mais informações

- Problemas conhecidos.
- Para obter informações sobre softwares de terceiros incluídos no serviço, consulte Notificações de terceiros.

Problemas conhecidos

November 9, 2023

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) tem os seguintes problemas conhecidos:

- O disco de identidade de preparação da AWS fica disponível mesmo após o processo de criação da máquina excluir a VM de preparação. Esse problema foi resolvido. No entanto, você pode excluir qualquer disco de identidade de preparação disponível se não houver uma tarefa de criação de catálogo ou de atualização de imagem em andamento. [PMCS-34500]
- Em um ambiente VMware hospedado na AWS, a criação do catálogo de máquinas MCS falha se a imagem mestre estiver habilitada para vTPM. Para obter suporte a VMware, consulte Get Support. [PMCS-37603]
- As telas de Monitor podem não carregar se a URL do Pendo, `https://citrix-cloud-content.customer.pendo.io/`, estiver bloqueada.
  [DIR-18482]
- Você receberá um erro ao executar um comando com `XDHyp:\` no SDK do PowerShell remoto. Para resolver esse problema:

1. Execute um comando com `Hyp`. Por exemplo: `Get-HypServiceStatus`
2. Execute um comando com `XDHyp:\`. Por exemplo: `Get-ChildItem XDHyp:\Connections\`

[BRK-13723]

- A criação do catálogo de máquinas MCS falha se você usar o disco de SO efêmero para criar um catálogo usando uma imagem de uma assinatura diferente no ambiente Azure. [CCVADHELP-2600]
- Após mudanças na arquitetura do Citrix DaaS na versão 2209, os ícones padrão para áreas de trabalho Windows e para aplicativos implantados antes dessa versão foram alterados para ícones genéricos de área de trabalho de PC. Essa alteração só se aplica a áreas de trabalho e aplicativos que estão apontando para o ícone padrão. Se você quiser alterar os ícones de volta para o ícone padrão do aplicativo Windows, execute o seguinte script usando o SDK remoto do PowerShell:
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- Em **Manage > Full Configuration**, as tentativas de alterar o tipo de sistema operacional dos catálogos do Azure falham com uma mensagem de erro. Não há mais suporte para alterar o tipo de sistema operacional dos catálogos do Azure, mesmo se você usar o PowerShell. [STUD-19819]
- Se você não atualizar para o Remote SDK mais recente antes de introduzir VDAs do Citrix Virtual Apps and Desktops versão 2206 ao ambiente DaaS, receberá o seguinte erro ao executar os cmdlets: **Invalid enum value *L7_34* cannot be deserialized into *Citrix.Broker.Admin.SDK.FunctionalLevel***. [PMCS-27248]
- Ao criar um catálogo de máquinas, a máquina virtual de bootstrapper do volume worker (XenDesktop Temp) não é encerrada corretamente. Como resultado, ocorre um erro e o vazamento da VM. Isso ocorre quando o Machine Creation Services (MCS) falha ao reconhecer um nome de dispositivo associado ao bootstrapper HVM Linux. Para resolver esse problema, exclua manualmente o bootstrapper do volume worker (XenDesktop Temp) e sua interface de rede associada. [PMCS-20277]
- Em ambientes Microsoft Azure, habilitar o disco de SO efêmero do Azure e o MCS I/O ao mesmo tempo interfere na criação de um catálogo de máquinas. No entanto, para os catálogos de máquinas existentes, você pode atualizar um catálogo de máquinas, adicionar ou excluir máquinas virtuais e excluir um catálogo de máquinas. [PMCS-21698]
- A implementação atual de comunicação do hipervisor, *Remote HCL*, pode gerar exceções pela plataforma do hipervisor de destino. Como resultado, a conexão entre o controlador de nuvem e o conector de nuvem falha e então é restabelecida. Se outras operações estiverem em andamento no Remote HCL usando a mesma conexão, essas conexões também poderão falhar. Isso

faz com que a energia da máquina e os estados de registro fiquem fora de sincronia. Com isso, podem surgir outros problemas, porque o problema afeta todos os tipos de operação Remote HCL, não apenas os estados de energia. As conexões de hospedagem dos hipervisores Azure e GCP não são afetadas. Essas conexões não usam o Remote HCL. [CCVADHELP-483]

- As máquinas VMware falham na reinicialização e não podem ser reiniciadas à força. Esse problema se aplica a todas as versões do VMware, incluindo VMC na AWS. O problema ocorre em catálogos de máquinas que têm máquinas virtuais persistentes (dedicadas) ou máquinas virtuais com gerenciamento de energia. Para resolver esse problema, use o cmdlet `New-Brokerhostingpoweraction` para reiniciar ou forçar a reinicialização de suas máquinas. [PMCS-15797]
- O ícone de seta suspensa dos botões Average IOPS, Session Control e Power Control às vezes não aparecerem nas páginas **User Details** e **Machine Details**. No entanto, a funcionalidade funciona conforme o esperado. Para ver todos os itens no menu, clique em qualquer lugar no botão. [DIR-11875]
- Se você usa o Azure AD Domain Services: os UPNs de logon do Workspace (ou StoreFront) 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.
- Ao implantar no Azure e criar um catálogo MCS versão 7.9 ou posterior com cache de write-back habilitado, e o VDA instalado na imagem mestre for 1811 ou anterior, ocorre um erro. Além disso, você não pode criar nada relacionado ao Personal vDisk do Microsoft Azure. Como solução alternativa, selecione uma versão de catálogo diferente para implantar no Azure ou desative o cache de write-back. Para desativar o cache de write-back ao criar um catálogo, desmarque as caixas de seleção **Memory allocated to cache** e **Disk cache size** na página **Machines**.
- O link **Console** em **Monitor > Machine Details** não inicia o Machine Console nos navegadores Microsoft Edge 44 e Firefox 68 ESR. [DIR-8160]
- Alterar o nome de uma AWS Virtual Private Cloud (VPC) no console da AWS quebra a unidade de hospedagem existente no Citrix Cloud. Quando a unidade de hospedagem quebra, você não pode criar catálogos ou adicionar máquinas a catálogos existentes. [PMCS-7701]
- Quando você tenta usar a opção "Restart"no Workspace App na Web ou na área de trabalho, a caixa de diálogo "Restarting"nunca fecha e nunca relata sucesso. O hipervisor mostra que a máquina foi desligada, mas que não foi iniciada. Como solução alternativa, depois de algum tempo, o usuário pode fechar a caixa de diálogo "Restarting"e iniciar a área de trabalho, e a área de trabalho deve iniciar. [BRK-5564]
- Quando você implanta máquinas em um catálogo MCS, a tarefa de provisionamento pode falhar e a seguinte mensagem de erro é exibida: "Terminating Error: Desktop Studio closed". Os detalhes do erro podem mostrar que nenhuma conta do AD foi criada. O catálogo pode ser con-

cluído com êxito mais tarde, sem intervenção. O problema é visto em implantações grandes e complexas. [PMCS-8869]

- O Cloud Library não pode ser usado para atribuir recursos em implantações que incluem um StoreFront local. [CCVADHELP-625]

Para problemas relacionados aos VDAs atuais, consulte Problemas conhecidos.

Substituição

December 20, 2023

Este artigo fornece um aviso prévio sobre os recursos do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que serão desativados, para que você possa tomar as medidas cabíveis. A Citrix monitora o uso e os comentários dos clientes para determinar quando os recursos são eliminados. Os anúncios podem ser alterados em versões subsequentes e nem sempre incluirão todos os recursos ou funcionalidades preteridos. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo da Política de suporte ao ciclo de vida do produto.

> **Nota:**
>
> As substituições e remoções do Citrix Virtual Apps and Desktops são descritas em seus próprios artigos de Substituição.

Substituições e remoções

A lista a seguir mostra os recursos do Citrix DaaS que foram preteridos ou removidos.

Os itens *preteridos* não são removidos imediatamente. A Citrix continua a oferecer suporte a eles, mas eles serão removidos em uma versão futura.

Os itens *removidos* são removidos, ou não têm mais suporte, do Citrix DaaS. As datas em **negrito** indicam as atualizações mais recentes.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para o AWS Volume Worker	Novembro 2023		Use o upload e download direto do disco Consulte Upload e download direto do disco

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para `Leave user management to Citrix Cloud` usado na criação de grupos de entrega	Setembro 2023	Setembro 2023	
Suporte para `AwsCaptureInstanceProperties` uso em ambientes da AWS	Agosto 2023		Use um perfil de máquina. Consulte Criar um catálogo usando um perfil de máquina.
Suporte para VMware vSphere 6.7		Junho 2023	Use versões superiores do VMware vSphere.
Comando `Schedule-ProvVMUpdate` do PowerShell	Abril 2023		Use o comando `Set-ProvVMUpdateTimeWindow`.
Comando `Request-ProvVMUpdate` do PowerShell	Abril 2023		Use o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.
Comando `Cancel-ProvVMUpdate` do PowerShell	Abril 2023		Use o comando `Clear-ProvVMUpdateTimeWindow`.
Parâmetro `DedicatedTenancy` usado no comando `New-ProvScheme`	Março 2023		Use o parâmetro `TenancyType`.
Disco não gerenciado para provisionar VM em ambientes do Azure	Junho 2022		

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress`	Maio 2022		
Parâmetro `StorageAccountType` usado em ambientes do Azure	Abril 2022		Use `StorageType`.
Console legado (console baseado em MMC)	Julho 2021	Novembro 2021	Use **Manage > Full Configuration** para acessar toda a gama de ações de configuração e gerenciamento.
Azure Quick Deploy	Setembro 2020		Use Quick Deploy.
Capacidade de importar dispositivos do destino Citrix Provisioning para criar catálogos no Citrix Studio.	Agosto 2020	Fevereiro 2021	Use o Citrix Provisioning Export Devices Wizard para enviar máquinas virtuais Citrix Provisioning para Delivery Controllers/MCS para criar catálogos. Consulte Export Devices Wizard.

Requisitos do sistema

November 9, 2023

Introdução

Os requisitos de sistema de componentes não cobertos aqui (como aplicativo Citrix Workspace e Citrix Provisioning) são descritos em suas respectivas documentações.

Recomendações específicas para dimensionar VMs que fornecem áreas de trabalho e aplicativos não podem ser fornecidas devido à natureza complexa e dinâmica das ofertas de hardware. Cada implantação tem necessidades específicas. 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 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 o uso de VDAs LTSR com o Citrix DaaS, consulte CTX205549.

Lembre-se: em uma implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops), você não precisa instalar ou gerenciar os componentes principais (Delivery Controllers, o banco de dados do site ou consoles de gerenciamento e monitoramento). Para obter orientações de instalação do Virtual Delivery Agent (VDA), consulte:

- Instalar VDAs
- Instalar VDAs usando a linha de comando.

Conectores de nuvem

Para obter detalhes, consulte Detalhes técnicos do Cloud Connector.

VDAs em um ambiente Azure

Sistemas operacionais compatíveis:

- Windows 11 multissessão
- Windows 11 de sessão única

- Windows 10 multissessão
- Windows 10 de sessão única
- Windows Server 2022 (requer o mínimo de VDA 2106)
- Windows Server 2019
- Windows Server 2016

Todos os VDAs que não atingiram o fim da vida útil têm suporte para uso com o Citrix DaaS. Quanto aos 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 compatível apenas com VDA 1912 (e atualizações cumulativas posteriores).

O Windows Server requer licenciamento do Microsoft RDS.

Para obter informações sobre a Área de Trabalho Virtual do Azure, consulte a documentação da Microsoft.

VDA para SO de sessão única

As informações a seguir se aplicam à versão mais recente do VDA.

Sistemas operacionais compatíveis:

- Windows 11
- Windows 10
  - Para obter suporte à edição, consulte CTX224843. Esse artigo também contém links para problemas conhecidos da Citrix com as versões compatíveis 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 redistribuível.
  - Se a máquina contiver uma versão anterior do Runtime (como 2015-2017), o instalador Citrix a atualizará.
  - Se a máquina contiver uma versão anterior a 2015, a Citrix instalará a versão mais recente em paralelo.

O Remote PC Access usa esse VDA, que você instala em PCs de escritórios físicos. Esse VDA suporta a Inicialização Segura para o acesso ao PC remoto do Citrix Virtual Desktops.

Vários recursos de aceleração de multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado no computador em que você instala o VDA. Se o computador não tiver o Media Foundation instalado, os recursos de aceleração de multimídia não serão instalados e não funcionarão. Não remova o Media Foundation do computador depois de instalar o software da Citrix. Caso contrário, os usuários não podem fazer logon no computador. Na maioria das edições Windows de SO de área de trabalho suportadas, o suporte ao Media Foundation já está instalado e não pode ser removido. No entanto, as edições N não incluem certas tecnologias relacionadas à mídia. Você pode obter esse software da Microsoft ou de terceiros.

Mais informações:

- Para obter informações sobre o Linux VDA, 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 uma máquina Windows Server com suporte. Consulte Server VDI para obter orientação.
- Para obter informações sobre como instalar um VDA em uma máquina 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 compatíveis:

- Windows Server 2022 (requer o mínimo de VDA 2106)
- 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 redistribuível.
  - Se a máquina contiver uma versão anterior do Runtime (como 2015-2017), o instalador 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 ativa automaticamente os serviços de função dos Serviços de Área de Trabalho Remota, se ainda não estiverem instalados e ativados. Isso provoca um reinício.

Vários recursos de aceleração de multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado no computador em que você instala o VDA. Se o computador não tiver o Media Foundation instalado, os recursos de aceleração de multimídia não serão instalados e não funcionarão. Não remova o Media Foundation do computador depois de instalar o software da Citrix. Caso contrário, os usuários não podem fazer logon no computador. 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 à mídia. Você pode obter esse software da Microsoft ou de terceiros.

Se o Media Foundation não estiver presente no VDA, estes recursos multimídia não funcionam:

- Redirecionamento Flash
- Windows Media Redirection
- Redirecionamento de vídeo HTML5
- Redirecionamento de Webcam HDX RealTime

Mais informações:

- Para obter informações sobre o Linux VDA, consulte os artigos do Linux Virtual Delivery Agent.
- Para obter informações sobre como instalar um VDA em um sistema operacional Windows que não tem mais suporte, consulte Sistemas operacionais anteriores.
- Consulte também VDAs em um ambiente de Área de Trabalho Virtual do Azure.

Recursos de virtualização e hosts

Os seguintes recursos de virtualização/host (listados alfabeticamente) são suportados. Quando aplicável, as versões *superior.inferior* são suportadas, incluindo atualizações a essas versões. CTX131239 contém as informações mas atuais sobre a versão atual de hipervisor, além de links para problemas conhecidos.

- **Amazon Web Services (AWS)**
  - Você pode provisionar aplicativos e áreas de trabalho em sistemas operacionais Windows Server compatíveis.
  - O Amazon Relational Database Service (RDS) não é compatível.

  Para obter mais informações, consulte Ambientes de nuvem AWS.

- **Citrix Hypervisor (anteriormente XenServer)**

  CTX131239 contém informações sobre a versão atual, além de links para problemas conhecidos.

Para obter mais informações, consulte Ambientes de virtualização do Citrix Hypervisor.

- **Google Cloud Platform**

  Para obter mais informações, consulte Ambientes do Google Cloud e Introdução ao Citrix DaaS no Google Cloud.

- **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 se registrar nas versões suportadas do System Center Virtual Machine Manager.

  CTX131239 contém informações sobre a versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

- **Nutanix Acropolis**

  CTX131239 contém informações sobre a versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Ambientes de virtualização do Nutanix.

- **VMware Cloud na AWS**

  CTX131239 contém informações sobre a versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Nuvem VMware na Amazon Web Services (AWS).

- **Solução VMware no Azure (AVS)**

  CTX131239 contém informações sobre a 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 sobre a versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Mecanismo VMware do Google Cloud.

- **VMware vSphere(vCenter + ESXi)**

  Não há suporte para o operação Linked Mode do vSphere vCenter.

  CTX131239 contém informações sobre a versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Ambientes de virtualização do VMware.

> **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 só é permitida para desenvolver uma prova de conceito ou ao publicar o console de administração do Studio somente para administradores. Nesse caso, você deve garantir que os 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 Ingressado no Active Directory.

Tecnologias HDX

Para obter suporte e requisitos específicos de recursos HDX, consulte HDX.

Universal Print Server

O servidor de impressão universal compreende componentes cliente e servidor. O componente UpsClient está incluído na instalação do VDA. Você instala o componente UpsServer em cada servidor de impressão onde residam impressoras compartilhadas que você deseje provisionar com o Citrix Universal Print Driver nas sessões do usuário.

O componente UpsServer é compatível com:

- Windows Server 2019
- Windows Server 2016

Requisitos:

- Microsoft .NET Framework 4.8 (mínimo)
- Microsoft Visual C++ 2015-2022 redistribuível.
  - Se a máquina contiver uma versão anterior do Runtime (como 2015-2017), o instalador Citrix a atualizará.

  - Se a máquina contiver uma versão anterior a 2015, a Citrix instalará a versão mais recente em paralelo.

Para VDAs de multissessão, a autenticação do usuário durante as operações de impressão exige que o servidor de impressão universal esteja conectado ao mesmo domínio que o VDA.

Os pacotes de componentes 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 conexão à Internet. Essas informações incluem requisitos comuns à maioria dos serviços do Citrix Cloud, além de requisitos específicos do Citrix DaaS.

Outros

- O Console de Gerenciamento de Política de Grupo (GPMC) da Microsoft é necessário se você armazenar informações de políticas da Citrix no Active Directory em vez de no banco de dados de configuração do site. A máquina na qual você instalar o `CitrixGroupPolicyManagement_x64.msi` deverá ter o tempo de execução do Visual Studio 2015 instalado. Para obter mais informações, consulte a documentação da Microsoft.
- Este produto oferece suporte ao PowerShell versões 3 a 5.
- Para componentes e recursos de produtos que podem ser instalados em Windows Servers, Server Core e instalações Nano Server não têm suporte, salvo indicação em contrário.
- Para obter detalhes sobre limites de recursos em uma implantação, consulte Limites.
- Para ver as versões compatíveis com o StoreFront, consulte os requisitos do sistema StoreFront.
- Para obter informações sobre globalização, consulte CTX119253.
- Para obter informações sobre as portas que o Citrix DaaS usa, consulte Communications Ports Used by Citrix Technologies.
- Para obter informações sobre os requisitos ao usar a interface de gerenciamento Quick Deploy, consulte Requisitos.

Limites

December 20, 2023

Os valores neste artigo indicam os limites de uma única instância do Citrix DaaS (anteriormente um serviço Citrix Virtual Apps and Desktops). Esses limites são amplamente testados pela Citrix e recomendados para proporcionar a melhor experiência ao usuário final e ao administrador. Esses são limites flexíveis e não são impostos tecnicamente (exceto o número total de VDAs por localização do recurso). Quando o número de usuários simultâneos exceder 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. Volte com frequência para atualizações. Se você tiver requisitos atuais que os limites publicados não abordam, entre em contato com seu representante da Citrix para obter assistência assim que possível.

Limites de configuração

Se as políticas excederem o limite, a Citrix recomenda o uso do serviço Workspace Environment Management ou dos Objetos de Política de Grupo (GPOs) do Active Directory.

Recurso	Limite
Domínios do Active Directory	100
Pastas de aplicativos	1.000
Grupos de aplicativos	250
Aplicativos	5.000
Catálogos	2.000
Grupos de entrega	2.000
Conexões de host	200
Locais de recursos	100
Políticas do console Manage (Full Configuration)	200
Marcas	10.000
VDAs	100.000

Limites de local de recursos

A tabela a seguir lista os limites para cada local de recursos.

Se seus requisitos excederem esses limites, a Citrix recomenda o uso de locais de recursos adicionais.

Recurso	Limite
Total de VDAs (limite rígido)	10.000
Total de sessões	25.000
Domínios do Active Directory	1
Conexões de host	40

Os conectores do Citrix Cloud são atribuídos a locais de recursos e vinculam cargas de trabalho ao Citrix DaaS. Para obter informações sobre os limites do Cloud Connector, consulte Considerações de tamanho e escala de 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 de maior escala, a Citrix recomenda um modelo hub-and-spoke, em que os VDAs são distribuídos por várias assinaturas e conexões de host.

Para obter mais informações, consulte as seguintes arquiteturas de referência:

- Citrix DaaS na AWS
- Virtualização Citrix no Google Cloud
- Citrix DaaS no Azure

Recurso	Limite
VDAs por conta da Amazon Web Services por região	1.500
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 funções de administrador e as diferenças entre elas, consulte:

- Manage (Full Configuration) administrators
- Monitor (Director) administrators

Recurso	Limite
Administradores completos de Monitor (Director) simultâneos	40
Administradores de suporte técnico de Monitor (Director) simultâneos	200
Administradores de sessão de Monitor (Director) simultâneos	50
Administradores de nuvem de Manage (Full Configuration) simultâneos	100
Administradores de help desk de Manage (Full Configuration) simultâneos	60
Usuários finais simultâneos	125.000
Recursos publicados para um único usuário	250
Inícios de sessão por minuto	3.000

- O Monitor (Director) suporta agregar até quatro locatários do Citrix DaaS (spokes) sob um único locatário (hub).
- Um administrador de help desk na instância do hub pode monitorar e solucionar problemas de usuários, máquinas, pontos de extremidade e transações de todas as instâncias agregadas (hub e spokes) de acordo com a configuração da administração delegada na instância específica.
- O número de administradores simultâneos por instância do Citrix DaaS segue a tabela de limites de uso.

Log de alterações de limites

A tabela a seguir acompanha a modificação do limite da configuração:

Data	Recurso	Descrição
22 Nov 2023	Domínios do Active Directory	Limite aumentado de 85 para 100.
	Catálogos	Limite aumentado de 1000 para 2000.
	Grupos de entrega	Limite aumentado de 1000 para 2000.
	Locais de recursos	Limite aumentado de 85 para 100.
	Locais de recurso -> Total de sessões	Limite aumentado de 20.000 para 25.000.
07 Dez 2023	Limites de provisionamento -> VDA por assinatura do Microsoft Azure por região	Limite aumentado de 2.500 para 5.000.

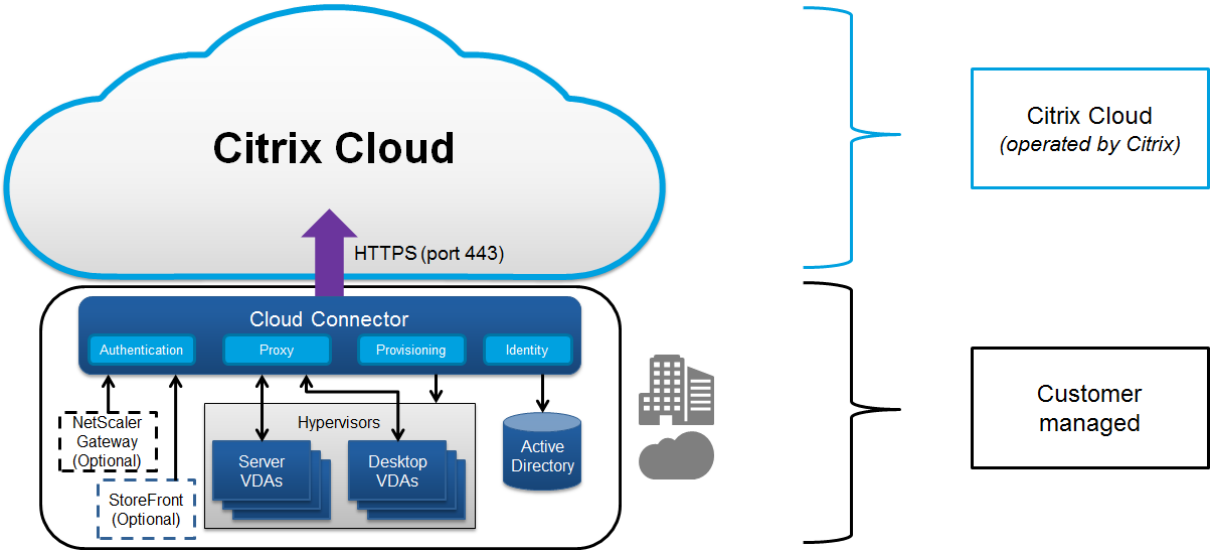
Visão técnica geral da segurança

June 6, 2023

Visão geral de segurança

Este documento se aplica ao Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) hospedado no Citrix Cloud. As informações incluem 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, os consoles de gerenciamento, o banco de dados SQL, o servidor de licenças e, opcionalmente, o StoreFront e o Citrix Gateway (anteriormente NetScaler Gateway). Os Virtual Delivery Agents (VDA) que hospedam os aplicativos e áreas de trabalho permanecem sob o controle do cliente no datacenter da escolha do cliente, 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 Workspace, eles também poderão optar por usar o Citrix Gateway Service em vez de executar o Citrix Gateway em seus datacenters. O diagrama a seguir ilustra o Citrix DaaS e seus limites de segurança.



Conformidade de uso baseado em nuvem da Citrix

Desde janeiro de 2021, o uso da capacidade Citrix Managed Azure com várias edições do Citrix DaaS e Workspace Premium Plus ainda não foi avaliado em relação a Citrix SOC 2 (Tipo 1 ou 2), ISO 27001, HIPAA ou outros requisitos de conformidade na nuvem. Visite o Citrix Trust Center para obter mais informações sobre as certificações do Citrix Cloud e volte com frequência para ver mais atualizações.

Fluxo de dados

O Citrix DaaS não hospeda os VDAs, portanto, os dados e imagens de aplicativos do cliente necessários para o provisionamento estão sempre hospedados na configuração do cliente. O plano de controle tem acesso a metadados, como nomes de usuários, 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 o monitoramento dos aplicativos e áreas de trabalho do cliente. Informações confidenciais, incluindo imagens, perfis de usuários e outros dados de aplicativos, permanecem nas instalações do cliente ou em assinaturas de fornecedores de nuvem pública.

Edições do serviço

Os recursos do Citrix DaaS variam de acordo com a edição. Por exemplo, o Citrix Virtual Apps Essentials suporta apenas o serviço Citrix Gateway e o Citrix Workspace. Consulte a documentação do produto para saber mais sobre os recursos compatíveis.

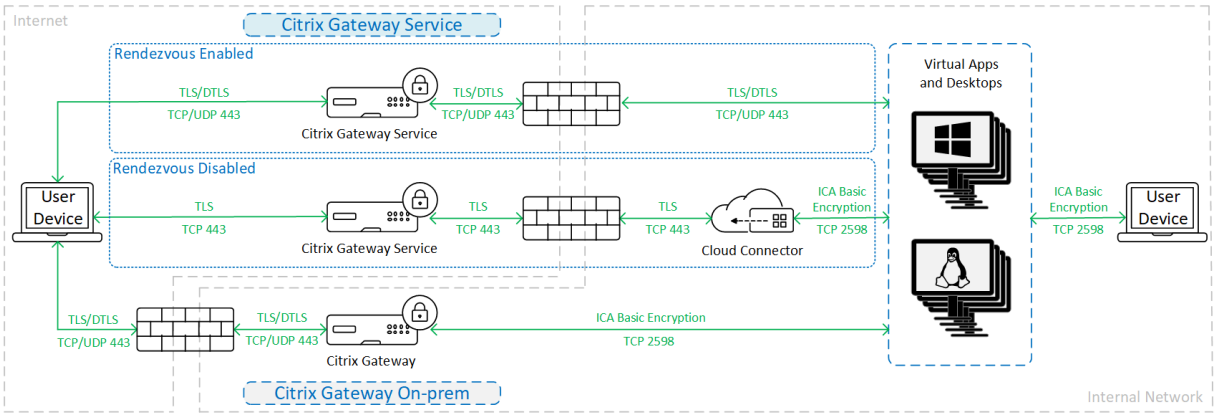
Segurança ICA

O Citrix DaaS oferece várias opções para proteger o tráfego ICA em trânsito. A seguir estão as opções disponíveis:

- **Basic encryption:** a configuração padrão.
- **SecureICA:** permite criptografar dados da sessão usando criptografia RC5 (128 bits).
- **VDA TLS/DTLS:** permite o uso de criptografia no nível da rede usando TLS/DTLS.
- **Rendezvous protocol:** disponível somente quando usar o Citrix Gateway Service. Quando usar o protocolo Rendezvous, as sessões ICA serão criptografadas de ponta a ponta usando TLS/DTLS.

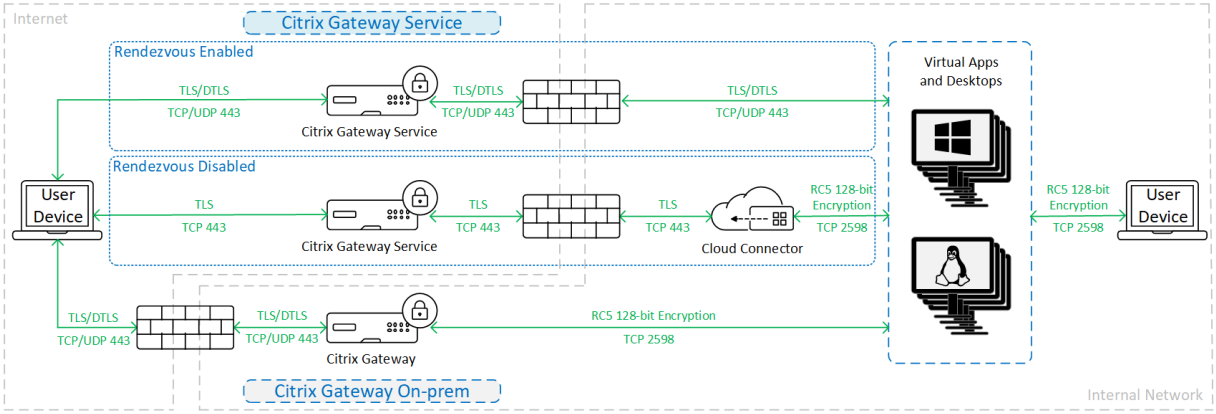
Criptografia básica

Quando usar a criptografia básica, o tráfego será criptografado conforme mostra o gráfico a seguir.



SecureICA

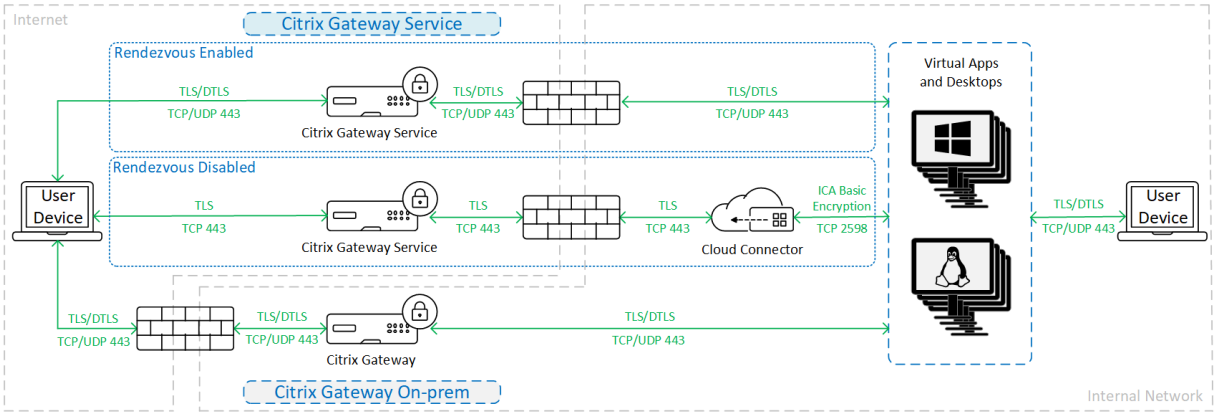
Quando usar SecureICA, o tráfego será criptografado conforme mostra o gráfico a seguir.



> **Nota:**
>
> O SecureICA não é compatível com o aplicativo Workspace para HTML5.

VDA TLS/DTLS

Quando usar a criptografia VDA TLS/DTLS, o tráfego será criptografado conforme mostra o gráfico a seguir.



> **Nota:**
>
> Quando usar o Gateway Service sem o Rendezvous, o tráfego entre o VDA e o Cloud Connector não será criptografado por TLS, porque o Cloud Connector não suporta a conexão ao VDA com criptografia no nível da rede.

Mais recursos

Para obter mais informações sobre as opções de segurança ICA e como configurá-las, consulte:

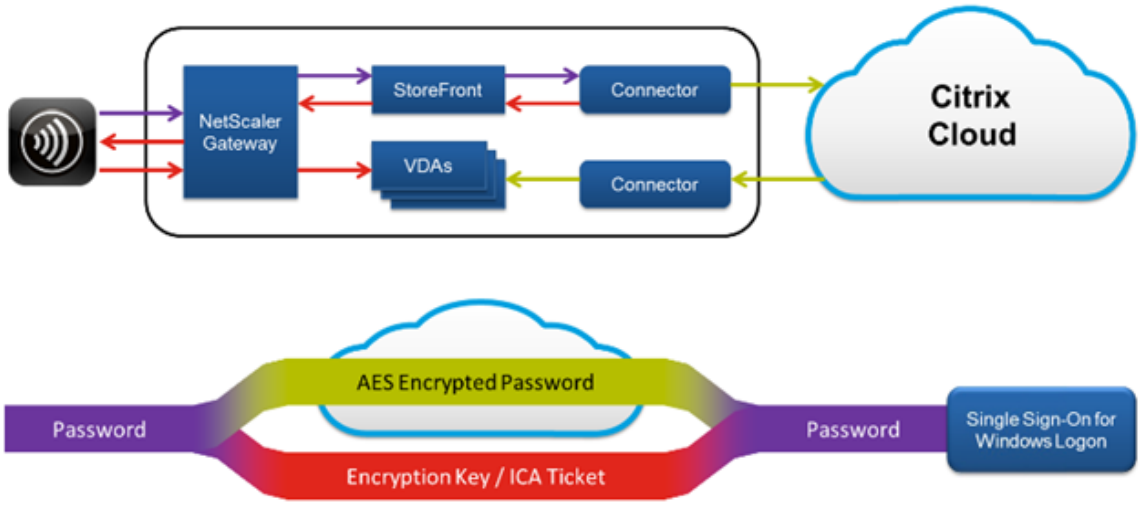
- SecureICA: Configurações da política de segurança
- VDA TLS/DTLS: Transport Layer Security
- Rendezvous protocol: Protocolo Rendezvous

Tratamento de credenciais

O Citrix DaaS lida com quatro tipos de credenciais:

- Credenciais do usuário: ao usar um StoreFront gerenciado pelo cliente, o Cloud Connector criptografa as credenciais do usuário usando a criptografia AES-256 e uma chave única aleatória gerada para cada inicialização. A chave nunca é passada para a nuvem e é retornada apenas para o aplicativo Citrix Workspace. Em seguida, o aplicativo Citrix Workspace passa essa chave para o VDA para descriptografar a senha do usuário durante a inicialização da sessão de logon único. O fluxo é mostrado na figura a seguir.

  Por padrão, as credenciais do usuário não são encaminhadas para além dos limites de domínio não confiáveis. Se um VDA e um StoreFront estiverem instalados em um domínio e um usuário em um domínio diferente tentar se conectar ao VDA, a tentativa de logon falhará, a menos que uma relação de confiança seja estabelecida entre os domínios. Você pode desativar esse comportamento e permitir que as credenciais sejam encaminhadas entre domínios não confiáveis usando o DaaS PowerShell SDK. Para obter mais informações, consulte Set-Brokersite.



- Credenciais do administrador: os administradores se autenticam no Citrix Cloud. A autenticação gera um JSON Web Token (JWT) assinado de uso único que dá ao administrador acesso ao Citrix DaaS.
- Senhas do hipervisor: os hipervisores locais que exigem uma senha para autenticação têm uma senha gerada pelo administrador que é criptografada e armazenada diretamente no banco de dados SQL na nuvem. A Citrix gerencia o par de chaves para garantir que as credenciais do hipervisor 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 só tem 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 somente na memória e são mantidas apenas para um único evento de provisionamento.

Considerações sobre implantação

A Citrix recomenda que os usuários consultem a documentação de melhores práticas publicada para implantar aplicativos Citrix Gateway e VDAs em seus ambientes.

Requisitos de acesso à rede Citrix Cloud Connector

Os Citrix Cloud Connectors exigem apenas tráfego de saída da porta 443 para a Internet e podem ser hospedados atrás de um proxy HTTP.

- A comunicação usada no Citrix Cloud para HTTPS é TLS. (Consulte Substituição das versões de TLS.)
- Na rede interna, o Cloud Connector precisa acessar o seguinte para o Citrix DaaS:
  - VDAs: porta 80, tanto de entrada quanto de saída, além das 1494 e 2598 de entrada se estiver usando o serviço Citrix Gateway
  - Servidores StoreFront: entrada da porta 80.
  - Citrix Gateways, se configurados como STA: entrada da porta 80.
  - Controladores de domínio do Active Directory
  - Hipervisores: somente saída. Consulte Portas de comunicação usadas pela Citrix Technologies para obter as portas específicas.

O tráfego entre os VDAs e os Cloud Connectors é criptografado usando a segurança no nível de mensagem do Kerberos.

StoreFront gerenciado pelo cliente

Um StoreFront gerenciado pelo cliente oferece mais opções de configuração de segurança e flexibilidade para a arquitetura de implantação, incluindo a capacidade de manter as credenciais do usuário no local. O StoreFront pode ser hospedado atrás do Citrix Gateway para fornecer acesso remoto seguro, impor autenticação multifator e adicionar outros recursos de segurança.

Serviço Citrix Gateway

O uso do serviço Citrix Gateway evita a necessidade de implantar o Citrix Gateway nos datacenters dos clientes.

Para obter detalhes, consulte o Serviço Citrix Gateway.

Todas as conexões TLS entre o Cloud Connector e o Citrix Cloud são iniciadas do Cloud Connector para o Citrix Cloud. Não é necessário mapeamento de porta de firewall de entrada.

Confiança em XML

Essa configuração está disponível em **Full Configuration > Settings > Enable XML trust** e está desativada por padrão. Como alternativa, você pode usar o Citrix DaaS Remote PowerShell SDK para gerenciar a confiança em XML.

A confiança em XML se aplica a implantações que usam:

- Um StoreFront local.
- Uma tecnologia de autenticação de (usuário) assinante que não requer senhas. Exemplos de tais tecnologias são as soluções de passagem de domínio, cartões inteligentes, SAML e Veridium.

Habilitar a confiança em XML permite que os usuários autentiquem com êxito e iniciem aplicativos. O Cloud Connector confia nas credenciais enviadas do StoreFront. Ative a confiança em XML somente quando você tiver protegido as comunicações entre os Citrix Cloud Connectors e o StoreFront (usando firewalls, IPsec ou outras recomendações de segurança).

Essa configuração é desativada por padrão.

Use o SDK do PowerShell remoto do Citrix DaaS para gerenciar a confiança em XML.

- Para verificar o valor atual da confiança em XML, execute `Get-BrokerSite` e inspecione o valor de `TrustRequestsSentToTheXMLServicePort`.
- Para ativar a confiança em XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlServic` `$true`
- Para desativar a confiança em XML, execute `Set-BrokerSite -TrustRequestsSentToTheXmlSer` `$false`

Impor tráfego HTTPS ou HTTP

Para impor tráfego HTTPS ou HTTP por meio do XML Service, configure um dos seguintes conjuntos de valores de registro em cada um dos seus Cloud Connectors.

Depois de definir as configurações, reinicie o Remote Broker Provider Service em cada Cloud Connector.

Em `HKLM\Software\Citrix\DesktopServer\`:

- Para impor tráfego HTTPS (ignorar HTTP): defina `XmlServicesEnableSsl` como `1` e `XmlServicesEnableNonSsl` como `0`.

- Para impor tráfego HTTP (ignorar HTTPS): defina `XmlServicesEnableNonSsl` como `1` e `XmlServicesEnableSsl` como `0`.

Substituição das versões de TLS

Para melhorar a segurança do Citrix DaaS, a Citrix começou a bloquear qualquer comunicação por TLS (Transport Layer Security) 1.0 e 1.1 a partir de 15 de março de 2019.

Todas as conexões com os serviços do Citrix Cloud a partir dos Citrix Cloud Connectors exigem TLS 1.2.

Para garantir uma conexão bem-sucedida com o Citrix Workspace a partir de dispositivos do usuário, a versão instalada do Citrix Receiver deve ser igual ou mais recente do que as versões a seguir.

Citrix Receiver	Versão
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0
Chrome/HTML5	Mais recente (o navegador deve oferecer suporte ao TLS 1.2)

Para atualizar para a versão mais recente do Citrix Receiver, acesse https://www.citrix.com/products/receiver/.

Como alternativa, atualize para o aplicativo Citrix Workspace, que usa o TLS 1.2. Para baixar o aplicativo Citrix Workspace, acesse https://www.citrix.com/downloads/workspace-app/.

Se você precisar continuar usando o TLS 1.0 ou 1.1 (por exemplo, com um cliente fino baseado em uma versão anterior do Receiver para Linux), instale um StoreFront no local do recurso. Em seguida, faça com que todos os Citrix Receivers apontem para ele.

Mais informações

Os seguintes recursos contêm informações de segurança:

- Visão técnica geral da segurança do Citrix Managed Azure.
- Site de segurança da Citrix.

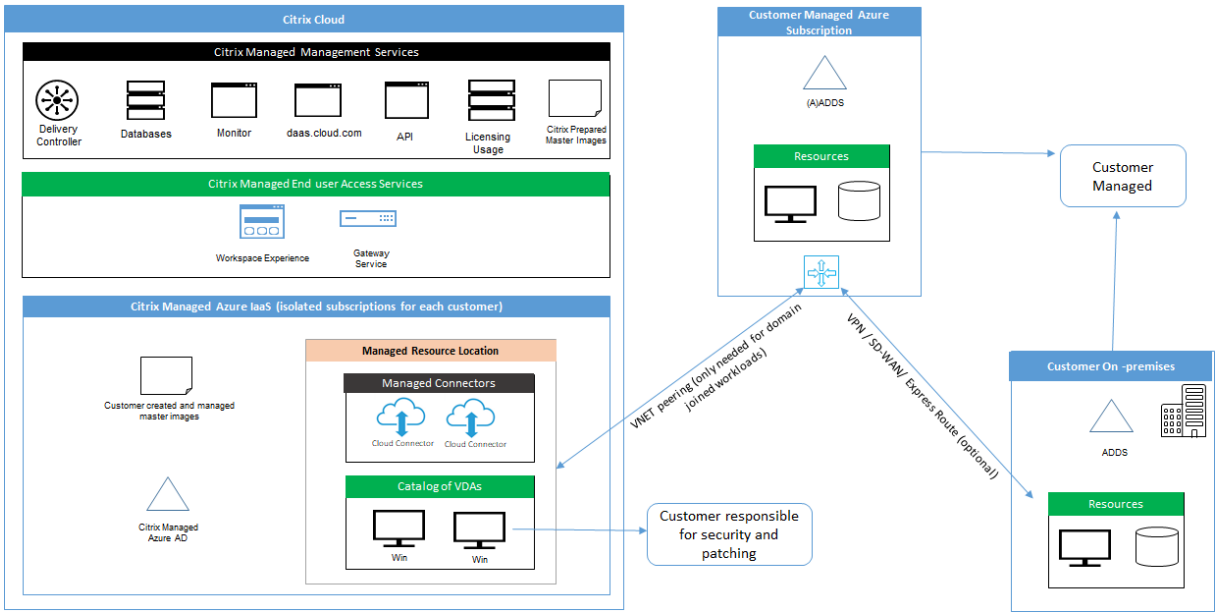
- Informações de segurança e conformidade: o centro de segurança e conformidade contém boletins de segurança que podem ajudá-lo a se manter informado. O centro também possui documentação sobre padrões e certificações que são importantes para manter um ambiente de TI seguro e compatível.
- Guia de implantação 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. Esse guia também contém links para informações abrangentes sobre o Citrix Cloud Connector.
- Requisitos de sistema e conectividade.
- Considerações de segurança e práticas recomendadas.
- Cartões inteligentes.
- Transport Layer Security (TLS).

> **Nota:**
>
> Este documento tem como objetivo fornecer ao leitor uma introdução e uma visão geral da funcionalidade de segurança do Citrix Cloud, e também definir a divisão de responsabilidades entre a Citrix e os clientes no que diz respeito à proteção da implantação do Citrix Cloud. Ele 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 da segurança técnica do Citrix Managed Azure

June 24, 2022

O diagrama a seguir mostra os componentes em uma implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que usa o Citrix Managed Azure. Este exemplo usa uma conexão de emparelhamento VNet.



Com o Citrix Managed Azure, os VDAs (Virtual Delivery Agents) do cliente que entregam áreas de trabalho e aplicativos, além de Citrix Cloud Connectors, são implantados em uma assinatura e locatário do Azure que a Citrix gerencia.

Conformidade de uso baseado em nuvem da Citrix

Desde janeiro de 2021, o uso da capacidade Citrix Managed Azure com várias edições do Citrix DaaS e Workspace Premium Plus ainda não foi avaliado em relação a Citrix SOC 2 (Tipo 1 ou 2), ISO 27001, HIPAA ou outros requisitos de conformidade na nuvem. Visite o Citrix Trust Center para obter mais informações sobre as certificações do Citrix Cloud e volte com frequência para ver mais atualizações.

Responsabilidade da Citrix

Citrix Cloud Connectors para catálogos não ingressados no domínio

Ao usar uma assinatura do Citrix Managed Azure, o Citrix DaaS implanta pelo menos dois Cloud Connectors em cada local de recurso. Alguns catálogos podem compartilhar um local de recurso se estiverem na mesma região que os outros catálogos para o mesmo cliente.

A Citrix é responsável pelas seguintes operações de segurança nos Cloud Connectors no catálogo não ingressado no domínio:

- Aplicação de atualizações do sistema operacional e patches de segurança
- Instalação e manutenção do software antivírus
- Aplicação de atualizações de software do Cloud Connector

Os clientes não têm acesso aos Cloud Connectors. Portanto, a Citrix é totalmente responsável pelo desempenho dos Cloud Connectors no catálogo não ingressado no domínio.

Assinatura do Azure e Azure Active Directory

A Citrix é responsável pela segurança da assinatura do Azure e do Azure Active Directory (AAD) criados para o cliente. A Citrix garante o isolamento do locatário, para que cada cliente tenha sua própria assinatura do Azure e AAD, e o crosstalk entre diferentes locatários seja evitado. A Citrix também restringe o acesso ao AAD apenas à equipe de operações da Citrix e do Citrix DaaS. O acesso da Citrix à assinatura do Azure de cada cliente é auditado.

Os clientes que empregam catálogos não ingressados no domínio podem usar o AAD gerenciado pela Citrix como um meio de autenticação no Citrix Workspace. Para esses clientes, a Citrix cria contas de usuário com privilégios limitados no AAD gerenciado pela Citrix. No entanto, nem os usuários nem os administradores dos clientes podem realizar ações no AAD gerenciado pela Citrix. Se esses clientes optarem por usar seus próprios AAD, eles serão totalmente responsáveis por sua segurança.

Redes virtuais e infraestrutura

Na assinatura do Citrix Managed Azure do cliente, a Citrix cria redes virtuais para isolar os locais de recursos. Dentro dessas redes, a Citrix cria máquinas virtuais para VDAs, Cloud Connectors e máquinas com construtor de imagens, além de contas de armazenamento, cofres de chaves e outros recursos do Azure. A Citrix, em parceria com a Microsoft, é responsável pela segurança das redes virtuais, incluindo o firewall das redes virtuais.

A Citrix garante que a política de firewall padrão do Azure (grupos de segurança de rede) esteja configurada para limitar o acesso às interfaces de rede no emparelhamento VNet e conexões SD-WAN. Geralmente, isso controla o tráfego de entrada para VDAs e Cloud Connectors. Para obter detalhes, consulte:

- Política de firewall para conexões de emparelhamento Azure VNet
- Política de firewall para conexões SD-WAN

Os clientes não podem alterar essa política de firewall padrão, mas podem implantar regras de firewall adicionais em máquinas VDA criadas pela Citrix; por exemplo, para restringir parcialmente o tráfego de saída. Os clientes que instalam uma rede privada virtual cliente, ou outro software capaz de ignorar as regras de firewall, em máquinas VDA criadas pela Citrix são responsáveis por quaisquer riscos de segurança que possam resultar.

Ao usar o construtor de imagens no Citrix DaaS para criar e personalizar a imagem de uma nova máquina, as portas 3389-3390 são abertas temporariamente na VNet gerenciada pela Citrix, para que

o cliente possa estabelecer o protocolo RDP com a máquina que contém a imagem da nova máquina, para personalizá-la.

Responsabilidade da Citrix ao usar conexões de emparelhamento Azure VNet

Para que os VDAs no Citrix DaaS estabeleçam contato com controladores de domínio locais, compartilhamentos de arquivos ou outros recursos da intranet, o Citrix DaaS fornece um fluxo de trabalho de emparelhamento VNet como uma opção de conectividade. A rede virtual gerenciada pela Citrix do cliente é emparelhada com uma rede virtual Azure gerenciada pelo cliente. A rede virtual gerenciada pelo cliente pode permitir a conectividade com os recursos locais do cliente usando a solução de conectividade entre nuvem e local da escolha do cliente, como o Azure ExpressRoute ou túneis IPsec.

A responsabilidade da Citrix pelo emparelhamento VNet é limitada ao suporte ao fluxo de trabalho e à configuração de recursos relacionados do Azure para estabelecer uma relação de emparelhamento entre a Citrix e as VNets gerenciadas pelo cliente.

Política de firewall para conexões de emparelhamento Azure VNet A Citrix abre ou fecha as seguintes portas para tráfego de entrada e saída que usa uma conexão de emparelhamento VNet.

VNet gerenciada pela Citrix com máquinas não ingressadas no domínio

- Regras de entrada
  - Permitir a entrada nas portas 80, 443, 1494 e 2598 de VDAs para Cloud Connectors e de Cloud Connectors para VDAs.
  - Permitir a entrada pelas portas 49152-65535 para os VDAs a partir de um intervalo de IP usado pelo recurso de sombreamento Monitor. Consulte Portas de comunicação usadas pela Citrix Technologies.
  - Negar todas as outras entradas. Isso inclui o tráfego intra-VNet do VDA para o VDA e do VDA para o Cloud Connector.
- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pela Citrix com máquinas ingressadas no domínio

- Regras de entrada:
  - Permitir a entrada nas portas 80, 443, 1494 e 2598 de VDAs para Cloud Connectors e de Cloud Connectors para VDAs.

  - Permitir a entrada pelas portas 49152-65535 para os VDAs a partir de um intervalo de IP usado pelo recurso de sombreamento Monitor. Consulte Portas de comunicação usadas pela Citrix Technologies.
  - Negar todas as outras entradas. Isso inclui o tráfego intra-VNet do VDA para o VDA e do VDA para o Cloud Connector.

- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pelo cliente com máquinas ingressadas no domínio

- O cliente é responsável por configurar sua VNet corretamente. Isso inclui abrir as seguintes portas para associação do domínio.
- Regras de entrada:
  - Permitir a entrada na 443, 1494, 2598 de seus IPs clientes para inicializações internas.
  - Permitir a entrada na 53, 88, 123, 135-139, 389, 445, 636 do Citrix VNet (intervalo de IP especificado pelo cliente).
  - Permitir a entrada pelas portas abertas com uma configuração de proxy.
  - Outras regras criadas pelo cliente.
- Regras de saída:
  - Permitir a saída na 443, 1494, 2598 para o Citrix VNet (intervalo de IP especificado pelo cliente) para inicializações internas.
  - Outras regras criadas pelo cliente.

Responsabilidade da Citrix ao usar a conectividade SD-WAN

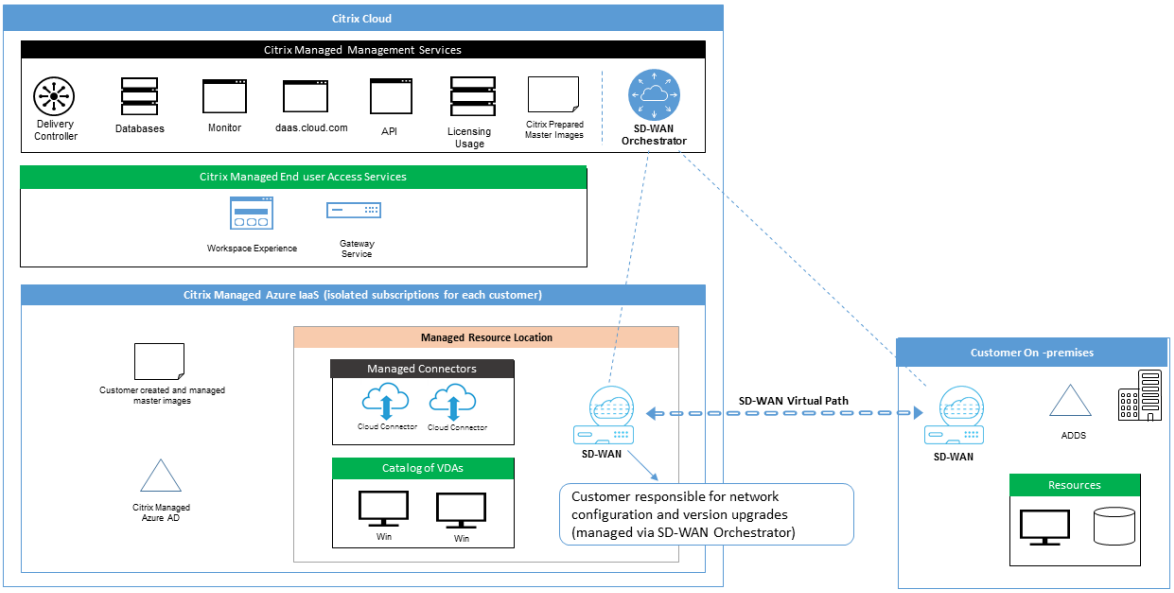
A Citrix oferece suporte a uma maneira totalmente automatizada de implantar instâncias virtuais do Citrix SD-WAN para permitir a conectividade entre o Citrix DaaS e os recursos locais. A conectividade Citrix SD-WAN tem várias vantagens em comparação com o emparelhamento VNet, incluindo:

Alta confiabilidade e segurança das conexões VDA-para-datacenter e VDA-para-branch (ICA).

- A melhor experiência de usuário final para funcionários de escritório, com recursos avançados de QoS e otimizações de VoIP.
- Capacidade interna de inspecionar, priorizar e gerar relatórios sobre o tráfego de rede do Citrix HDX e outros usos de aplicativo.

A Citrix requer que os clientes que desejam aproveitar a conectividade SD-WAN para o Citrix DaaS usem o SD-WAN Orchestrator para gerenciar suas redes Citrix SD-WAN.

O diagrama a seguir mostra os componentes adicionados em uma implantação do Citrix DaaS usando uma assinatura do Citrix Managed Azure e conectividade SD-WAN.



A implantação do Citrix SD-WAN para o Citrix DaaS é semelhante à configuração de implantação Standard do Azure para o Citrix SD-WAN. Para obter mais informações, consulte Implantar uma instância do Citrix SD-WAN Standard Edition no Azure. Em uma configuração de alta disponibilidade, um par ativo/em espera de instâncias de SD-WAN com balanceadores de carga do Azure é implantado como um gateway entre a sub-rede que contém VDAs e Cloud Connectors e a Internet. Em uma configuração sem HA (alta disponibilidade), apenas uma única instância de SD-WAN é implantada como gateway. As interfaces de rede dos dispositivos SD-WAN virtuais recebem endereços de um pequeno intervalo de endereços separado dividido em duas sub-redes.

Ao configurar a conectividade SD-WAN, a Citrix faz algumas alterações na configuração de rede das áreas de trabalho gerenciadas descritas acima. Em particular, todo o tráfego de saída da VNet, incluindo o tráfego para destinos da Internet, é roteado através de uma instância SD-WAN na nuvem. A instância de SD-WAN também está configurada para ser o servidor DNS da VNet gerenciada pela Citrix.

O acesso de gerenciamento às instâncias virtuais de SD-WAN requer login e senha de administrador. Cada instância de SD-WAN recebe uma senha segura exclusiva e aleatória que pode ser usada pelos administradores de SD-WAN para o login remoto e a solução de problemas por meio da interface do usuário do SD-WAN Orchestrator, interface do usuário de gerenciamento do dispositivo virtual e CLI.

Assim como outros recursos específicos do locatário, as instâncias virtuais de SD-WAN implantadas em uma VNet de cliente específica são totalmente isoladas de todas as outras VNets.

Quando o cliente ativa a conectividade Citrix SD-WAN, a Citrix automatiza a implantação inicial de instâncias virtuais SD-WAN usadas com o Citrix DaaS, mantém os recursos subjacentes do Azure (máquinas virtuais, balanceadores de carga, etc.), fornece definições de segurança e eficiência padrão para a configuração inicial de instâncias virtuais de SD-WAN, e permite a manutenção contínua e a solução de problemas por meio do SD-WAN Orchestrator. A Citrix também toma medidas razoáveis para realizar a validação automática da configuração de rede SD-WAN, verificar riscos de segurança conhecidos e exibir alertas correspondentes por meio do SD-WAN Orchestrator.

Política de firewall para conexões SD-WAN A Citrix usa políticas de firewall do Azure (grupos de segurança de rede) e atribuição de endereço IP público para limitar o acesso às interfaces de rede de dispositivos SD-WAN virtuais:

- Somente interfaces WAN e de gerenciamento recebem endereços IP públicos e permitem conectividade de saída com a Internet.
- As interfaces LAN, atuando como gateways para a VNet gerenciada pela Citrix, só podem trocar tráfego de rede com máquinas virtuais na mesma VNet.
- As interfaces WAN limitam o tráfego de entrada para a porta UDP 4980 (usada pelo Citrix SD-WAN para conectividade de caminho virtual) e negam o tráfego de saída para a VNet.
- As portas de gerenciamento permitem o tráfego de entrada para as portas 443 (HTTPS) e 22 (SSH).
- As interfaces HA só podem trocar tráfego de controle entre si.

Acesso à infraestrutura

A Citrix pode acessar a infraestrutura do cliente gerenciada pela Citrix (Cloud Connectors) para executar determinadas tarefas administrativas, como coletar logs (incluindo o Windows Event Viewer) e reiniciar serviços sem notificar o cliente. A Citrix é responsável por executar essas tarefas com segurança e com impacto mínimo para o cliente. A Citrix também é responsável por garantir que todos os arquivos de log sejam recuperados, transportados e manipulados com segurança. Os VDAs do cliente não podem ser acessados dessa forma.

Backups de catálogos não ingressados no domínio

A Citrix não é responsável por realizar backups de catálogos não ingressados no domínio.

Backups de imagens de máquinas

A Citrix é responsável por fazer backup de qualquer imagem de máquina carregada para o Citrix DaaS, incluindo imagens criadas com o construtor de imagens. A Citrix usa armazenamento com redundân-

cia local para essas imagens.

Bastions para catálogos não ingressados no domínio

O pessoal de operações da Citrix tem a capacidade de criar um bastion, se necessário, para acessar a assinatura do Azure gerenciado pela Citrix do cliente para diagnosticar e reparar problemas do cliente, possivelmente antes que o cliente esteja ciente do problema. A Citrix não precisa do consentimento do cliente para criar um bastion. Quando a Citrix cria o bastion, a Citrix cria uma senha forte gerada aleatoriamente para o bastion e restringe o acesso RDP aos endereços IP NAT da Citrix. Quando o bastion não é mais necessário, a Citrix o descarta e a senha não é mais válida. O bastion e as regras de acesso RDP que o acompanham são descartados quando a operação é concluída. Com o bastion, a Citrix pode acessar apenas os Cloud Connectors não ingressados no domínio do cliente. A Citrix não tem a senha para fazer login em VDAs não ingressados no domínio ou em VDAs e Cloud Connectors ingressados no domínio.

Política de firewall ao usar ferramentas de solução de problemas

Quando um cliente solicita a criação de uma máquina bastion para a solução de um problema, as seguintes modificações do grupo de segurança são feitas na VNet gerenciada pela Citrix:

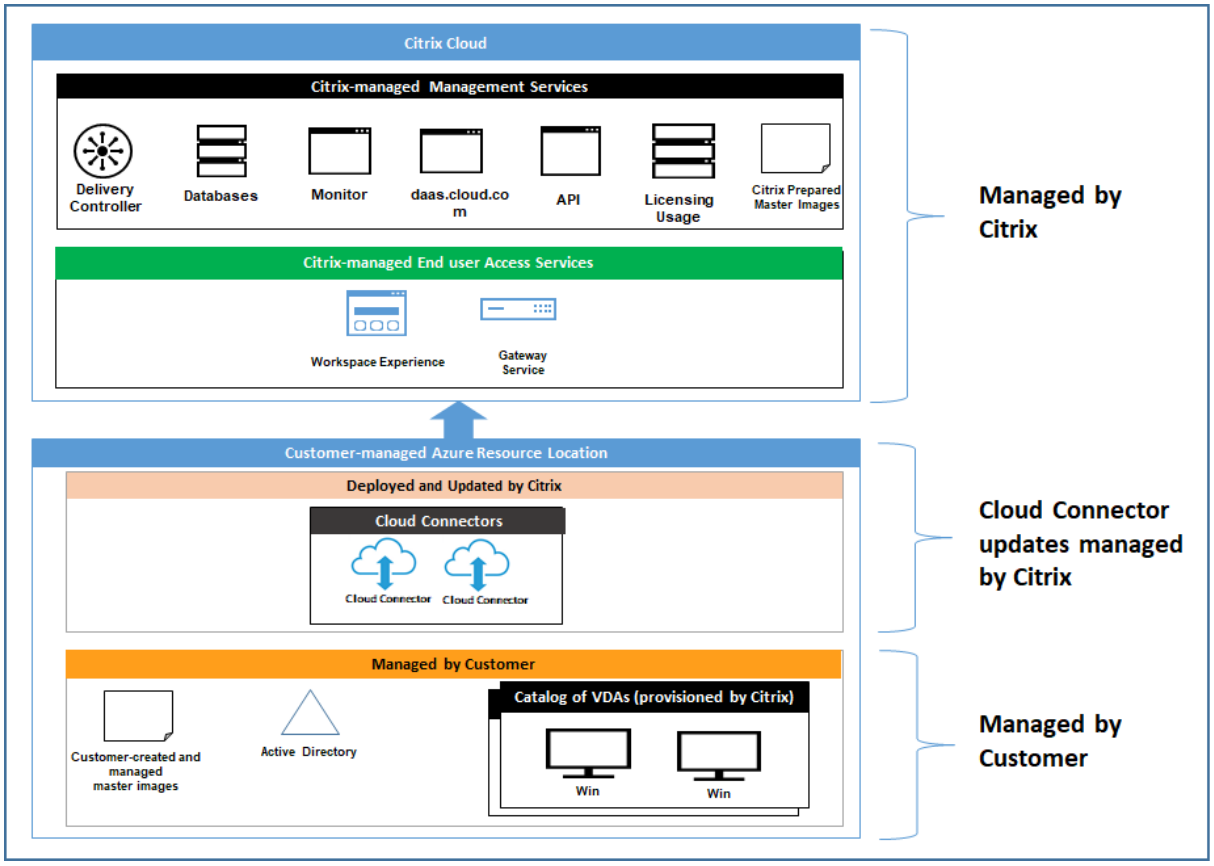
- Permitir temporariamente a entrada pela 3389 do intervalo de IP especificado pelo cliente para o bastion.
- Permitir temporariamente a entrada pela 3389 do endereço IP do bastion para qualquer endereço na VNet (VDAs e Cloud Connectors).
- Continuar e bloquear o acesso RDP entre os Cloud Connectors, os VDAs e outros VDAs.

Quando um cliente habilita o acesso RDP para a solução de um problema, as seguintes modificações do grupo de segurança são feitas na VNet gerenciada pela Citrix:

- Permitir temporariamente a entrada pela 3389 do intervalo de IP especificado pelo cliente para qualquer endereço na VNet (VDAs e Cloud Connectors).
- Continuar e bloquear o acesso RDP entre os Cloud Connectors, os VDAs e outros VDAs.

Assinaturas gerenciadas pelo cliente

Para assinaturas gerenciadas pelo cliente, a Citrix adere às responsabilidades acima durante a implantação dos recursos do Azure. Após a implantação, tudo acima é de responsabilidade do cliente, porque o cliente é o proprietário da assinatura do Azure.



Responsabilidade do cliente

VDAs e imagens de máquinas

O cliente é responsável por todos os aspectos do software instalado nas máquinas VDA, incluindo:

- Atualizações do sistema operacional e patches de segurança
- Antivírus e antimalware
- Atualizações de software do VDA e patches de segurança
- Regras adicionais de firewall de software (especialmente tráfego de saída)
- Siga as considerações de segurança e práticas recomendadas da Citrix

A Citrix fornece uma imagem preparada que se destina a ser um ponto de partida. Os clientes podem usar essa imagem para fins de prova de conceito ou demonstração ou como base para criar sua própria imagem de máquina. A Citrix não garante a segurança dessa imagem preparada. A Citrix tentará manter o sistema operacional e o software do VDA na imagem preparada atualizados e habilitará o Windows Defender nessas imagens.

Responsabilidade do cliente ao usar o emparelhamento VNet

O cliente deve abrir todas as portas especificadas na VNet gerenciada pelo cliente com máquinas ingressadas no domínio.

Quando o emparelhamento VNet é configurado, o cliente é responsável pela segurança de sua própria rede virtual e da conectividade da rede com seus recursos locais. O cliente também é responsável pela segurança do tráfego de entrada da rede virtual emparelhada gerenciada pela Citrix. A Citrix não toma nenhuma ação para bloquear o tráfego da rede virtual gerenciada pela Citrix aos recursos locais do cliente.

Os clientes têm as seguintes opções para restringir o tráfego de entrada:

- Dar à rede virtual gerenciada pela Citrix um bloco de IP que não está em uso em nenhum outro lugar na rede local do cliente ou na rede virtual conectada gerenciada pelo cliente. Isso é necessário para o emparelhamento VNet.
- Adicionar firewalls e grupos de segurança de rede do Azure à rede virtual e à rede local do cliente para bloquear ou restringir o tráfego do bloco de IP gerenciado pela Citrix.
- Implementar medidas como sistemas de prevenção de intrusões, firewalls de software e mecanismos de análise comportamental na rede virtual e na rede local do cliente, visando o bloco de IP gerenciado pela Citrix.

Responsabilidade do cliente ao usar a conectividade SD-WAN

Quando a conectividade SD-WAN é configurada, os clientes têm total flexibilidade para configurar as instâncias virtuais de SD-WAN usadas com o Citrix DaaS de acordo com seus requisitos de rede, com exceção de alguns elementos necessários para garantir a operação correta da SD-WAN na VNet gerenciada pela Citrix. As responsabilidades do cliente incluem:

- Projeto e configuração de regras de roteamento e firewall, incluindo regras de ruptura de tráfego de DNS e Internet.
- Manutenção da configuração de rede SD-WAN.
- Monitoramento do status operacional da rede.
- Implantação rápida de atualizações de software Citrix SD-WAN ou correções de segurança. Como todas as instâncias do Citrix SD-WAN em uma rede do cliente devem executar a mesma versão do software SD-WAN, as implantações de versões atualizadas de software nas instâncias SD-WAN do Citrix DaaS precisam ser gerenciadas pelos clientes de acordo com seus cronogramas e restrições de manutenção de rede.

A configuração incorreta das regras de firewall e roteamento de SD-WAN, ou o gerenciamento incorreto de senhas de gerenciamento de SD-WAN, pode resultar em riscos de segurança aos recursos virtuais no Citrix DaaS e aos recursos locais acessíveis por meio de caminhos virtuais do Citrix SD-WAN.

Outro possível risco de segurança decorre da não atualização do software Citrix SD-WAN com a versão de patch mais recente disponível. Embora o SD-WAN Orchestrator e outros serviços do Citrix Cloud forneçam os meios para lidar com esses riscos, os clientes são responsáveis por garantir que as instâncias virtuais de SD-WAN sejam configuradas adequadamente.

Proxy

O cliente pode optar por usar um proxy para o tráfego de saída do VDA. Se for usado um proxy, o cliente será responsável por:

- Configurar os parâmetros do proxy na imagem da máquina VDA ou, se o VDA estiver ingressado em um domínio, usar a Política de Grupo do Active Directory.
- Cuidar da manutenção e segurança do proxy.

Proxies não são permitidos para uso com Citrix Cloud Connectors ou outra infraestrutura gerenciada pela Citrix.

Resiliência de catálogo

A Citrix fornece três tipos de catálogos com diferentes níveis de resiliência:

- **Estático:** cada usuário é atribuído a um único VDA. Esse tipo de catálogo não oferece alta disponibilidade. Se o VDA de um usuário sair do ar, ele precisará ser colocado em um novo para se recuperar. O Azure fornece um SLA de 99,5% para VMs de instância única. O cliente ainda pode fazer backup do perfil do usuário, mas todas as personalizações feitas no VDA (como instalar programas ou configurar o Windows) serão perdidas.
- **Aleatório:** cada usuário é atribuído aleatoriamente a um servidor VDA no momento da inicialização. Esse tipo de catálogo fornece alta disponibilidade por meio de redundância. Se um VDA sair do ar, nenhuma informação será perdida porque o perfil do usuário reside em outro lugar.
- **Windows 10 multissessão:** esse tipo de catálogo opera da mesma maneira que o tipo aleatório, mas usa VDAs de estação de trabalho do Windows 10 em vez de VDAs de servidor.

Backups para catálogos ingressados no domínio

Se o cliente usar catálogos ingressados no domínio com um emparelhamento VNet, o cliente será responsável por fazer backup de seus perfis de usuário. A Citrix recomenda que os clientes configurem compartilhamentos de arquivos locais e definam políticas em seus Active Directory ou VDAs para extrair perfis de usuário desses compartilhamentos de arquivos. O cliente é responsável pelo backup e pela disponibilidade desses compartilhamentos de arquivos.

Recuperação de desastres

No caso de perda de dados do Azure, a Citrix recuperará o maior número possível de recursos na assinatura do Azure gerenciada pela Citrix. A Citrix tentará recuperar os Cloud Connectors e os VDAs. Se a Citrix não conseguir recuperar esses itens, os clientes serão responsáveis pela criação de um novo catálogo. A Citrix pressupõe que o backup das imagens da máquina seja feito regularmente e que os clientes fizeram backup de seus perfis de usuário, permitindo que o catálogo seja reconstruído.

No caso da perda de toda uma região do Azure, o cliente é responsável por reconstruir sua rede virtual gerenciada pelo cliente em uma nova região e criar um novo emparelhamento VNet ou uma nova instância SD-WAN no Citrix DaaS.

Responsabilidades compartilhadas entre a Citrix e o cliente

Citrix Cloud Connector para catálogos ingressados no domínio

O Citrix DaaS implanta pelo menos dois Cloud Connectors em cada local de recurso. Alguns catálogos podem compartilhar um local de recurso se estiverem na mesma região, emparelhamento VNet e domínio que outros catálogos para o mesmo cliente. A Citrix configura os Cloud Connectors ingressados no domínio do cliente para as seguintes configurações de segurança padrão na imagem:

- Atualizações do sistema operacional e patches de segurança
- Software antivírus
- Atualizações do software Cloud Connector

Os clientes normalmente não têm acesso aos Cloud Connectors. No entanto, eles podem adquirir acesso usando as etapas de solução de problemas do catálogo e fazendo login com as credenciais do domínio. O cliente é responsável por quaisquer alterações que fizer ao fazer login pelo bastion.

Os clientes também têm controle sobre os Cloud Connectors ingressados no domínio por meio da Política de Grupo do Active Directory. O cliente é responsável por garantir que as políticas de grupo que se aplicam ao Cloud Connector sejam seguras e sensatas. Por exemplo, se o cliente optar por desativar as atualizações do sistema operacional usando a Política de Grupo, o cliente será responsável por realizar atualizações do sistema operacional nos Cloud Connectors. O cliente também pode optar por usar a Política de Grupo para impor uma segurança mais rígida do que os padrões do Cloud Connector, por exemplo, instalando um software antivírus diferente. Em geral, a Citrix recomenda que os clientes coloquem os Cloud Connectors em suas próprias unidades organizacionais do Active Directory sem políticas, pois isso garantirá que os padrões usados pela Citrix possam ser aplicados sem problemas.

Solução de problemas

Caso o cliente tenha problemas com o catálogo no Citrix DaaS, há duas opções para a solução de problemas: usar bastions e habilitar o acesso RDP. Ambas as opções apresentam risco de segurança para o cliente. O cliente deve entender, consentir e assumir esse risco antes de usar essas opções.

A Citrix é responsável por abrir e fechar as portas necessárias para realizar operações de solução de problemas e restringir quais máquinas podem ser acessadas durante essas operações.

Com bastions ou acesso RDP, o usuário ativo que executa a operação é responsável pela segurança das máquinas que estão sendo acessadas. Se o cliente acessar o VDA ou o Cloud Connector por meio do RDP e contrair um vírus acidentalmente, o cliente será responsável. Se a equipe de suporte Citrix acessar essas máquinas, esse pessoal terá a responsabilidade de realizar as operações com segurança. A responsabilidade por vulnerabilidades expostas por qualquer pessoa que acesse o bastion ou outras máquinas na implantação (por exemplo, a responsabilidade do cliente de adicionar intervalos de IP à lista de permissão, a responsabilidade da Citrix de implementar intervalos de IP corretamente) é abordada em outro lugar neste documento.

Nos dois cenários, a Citrix é responsável por criar corretamente exceções de firewall para permitir o tráfego RDP. A Citrix também é responsável por revogar essas exceções depois que o cliente se desfaz do bastion ou encerra o acesso RDP por meio do Citrix DaaS.

Bastions A Citrix pode criar bastions na rede virtual gerenciada pela Citrix do cliente dentro da assinatura gerenciada pela Citrix do cliente para diagnosticar e reparar problemas, de forma proativa (sem notificação do cliente) ou em resposta a um problema levantado pelo cliente. O bastion é uma máquina que o cliente pode acessar por meio do RDP e usar para acessar os VDAs e Cloud Connectors (para catálogos ingressados no domínio) por meio do RDP para coletar logs, reiniciar serviços ou executar outras tarefas administrativas. Por padrão, a criação de um bastion abre uma regra de firewall externo para permitir o tráfego RDP de um intervalo de endereços IP especificado pelo cliente para a máquina bastion. Também abre uma regra de firewall interno para permitir o acesso aos Cloud Connectors e VDAs por meio do RDP. Abrir essas regras representa um grande risco de segurança.

O cliente é responsável por fornecer uma senha forte usada para a conta local do Windows. O cliente também é responsável por fornecer um intervalo de endereços IP externo que permita o acesso RDP ao bastion. Se o cliente optar por não fornecer um intervalo de IP (permitindo que qualquer pessoa tente o acesso RDP), o cliente será responsável por qualquer tentativa de acesso por endereços IP maliciosos.

O cliente também é responsável por excluir o bastion após concluir solução de problemas. O host bastion expõe a superfície de ataque adicional, assim a Citrix desliga automaticamente a máquina oito (8) horas depois que ela é ligada. No entanto, a Citrix nunca exclui um bastion automaticamente. Se o cliente optar por usar o bastion por um longo período de tempo, ele será responsável por aplicar patches e atualizá-lo. A Citrix recomenda que um bastion seja usado apenas por alguns dias antes de

excluí-lo. Se o cliente quiser um bastion atualizado, ele poderá excluir o atual e criar um novo bastion, que provisionará uma nova máquina com os patches de segurança mais recentes.

Acesso RDP Para catálogos ingressados no domínio, se o emparelhamento VNet do cliente estiver funcional, o cliente poderá habilitar o acesso RDP da sua VNet emparelhada à VNet gerenciada pela Citrix. Se o cliente usar essa opção, o cliente será responsável por acessar os VDAs e os Cloud Connectors através do emparelhamento VNet. Os intervalos de endereços IP de origem podem ser especificados para que o acesso RDP possa ser restringido ainda mais, mesmo dentro da rede interna do cliente. O cliente precisará usar credenciais de domínio para fazer login nessas máquinas. Se o cliente estiver trabalhando com o Suporte Citrix para resolver um problema, talvez seja necessário que o cliente compartilhe essas credenciais com a equipe de suporte. Depois que o problema for resolvido, o cliente será responsável por desativar o acesso RDP. Manter o acesso RDP aberto a partir da rede local ou emparelhada do cliente representa um risco à segurança.

Credenciais de domínio

Se o cliente optar por usar um catálogo ingressado no domínio, ele será responsável por fornecer ao Citrix DaaS uma conta de domínio (nome de usuário e senha) com permissões para ingressar máquinas no domínio. Ao fornecer credenciais de domínio, o cliente é responsável por aderir aos seguintes princípios de segurança:

- **Auditável:** a conta deve ser criada especificamente para o uso do Citrix DaaS, para que seja fácil de auditar para o que a conta é usada.
- **Com escopo:** a conta requer apenas permissões para associar máquinas a um domínio. Ela não deve ter permissões completas de administrador de domínio.
- **Seguro:** uma senha forte deve ser usada para a conta.

A Citrix é responsável pelo armazenamento seguro dessa conta de domínio em um Azure Key Vault na assinatura do Azure gerenciada pela Citrix do cliente. A conta será recuperada somente se uma operação exigir a senha da conta de domínio.

Mais informações

Para obter informações relacionadas, consulte:

- Guia de implantação segura para a plataforma Citrix Cloud: informações de segurança para a plataforma Citrix Cloud.
- Visão técnica geral da segurança: informações de segurança para o Citrix DaaS
- Notificações de terceiros

Métodos de entrega

June 24, 2022

Um único método de entrega provavelmente não atende 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 de imagem, além de modificações do registro. Para obter detalhes, consulte Criar catálogos de máquinas.
- **Aplicativo por streaming (Microsoft App-V):** o aplicativo é incluído em um perfil e entregue às áreas de trabalho em toda a rede sob demanda. Arquivos de aplicativos e 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 aplicativos, um administrador pode criar facilmente imagens novas e implantáveis. A camada simplifica a manutenção contínua, pois existe um sistema operacional, um agente e um aplicativo em uma única camada. Quando você atualiza 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 multi-usuário e implantado como um aplicativo e não uma área de trabalho. Um usuário acessa o aplicativo do Windows hospedado diretamente a partir de um dispositivo de ponto de extremidade ou área de trabalho VDI, 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 ponto de extremidade. A interface do aplicativo aparece dentro da sessão VDI hospedada do usuário, mesmo sendo executada no endpoint. Para obter detalhes, consulte Acesso ao aplicativo local e redirecionamento de URL.

Nas áreas de trabalho, você pode considerar áreas de trabalho publicadas do Citrix Virtual Apps ou áreas de trabalho VDI.

Áreas de trabalho e aplicativos publicados do Citrix Virtual Apps

Use máquinas com SO multissessão para entregar aplicativos publicados e áreas de trabalho publicadas do Citrix Virtual Apps.

Caso de uso:

- Você quer uma entrega barata baseada em servidor para minimizar o custo de entrega de aplicativos para muitos usuários, ao mesmo tempo em que oferece uma experiência de usuário segura e de alta definição.
- Seus usuários executam tarefas bem-definidas e não exigem personalização ou acesso offline aos aplicativos. Os usuários podem incluir trabalhadores por tarefa, como operadores de call center e trabalhadores do varejo, ou usuários que compartilham estações de trabalho.
- Tipos de aplicação: qualquer aplicação.

Benefícios e considerações:

- Solução gerenciável e dimensionável em seu data center.
- Solução de entrega de aplicativos mais rentável.
- 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 a partir do StoreFront, do menu Iniciar ou de um URL que você forneça.
- Os aplicativos são entregues virtualmente e são exibidos perfeitamente em alta definição nos dispositivos do usuário.
- Dependendo das configurações do perfil, as alterações do usuário são salvas quando a sessão do aplicativo do usuário termina. Caso contrário, as alterações serão excluídas.

Processamento, hospedagem e entrega de aplicativos:

- O processamento de aplicativos ocorre em máquinas de hospedagem, em vez de ocorrer nos dispositivos do usuário. A máquina de hospedagem pode ser uma máquina física ou virtual.
- Aplicativos e áreas de trabalho residem em uma máquina com SO multissessão.
- As máquinas ficam disponíveis através de catálogos de máquinas.
- Máquinas de catálogos de máquinas são organizadas em grupos de entrega que fornecem o mesmo conjunto de aplicativos para grupos de usuários.
- As máquinas com SO multissessão suportam grupos de entrega que hospedam áreas de trabalho ou aplicativos ou ambos.

Gerenciamento e atribuição de sessões:

- As máquinas com SO multissessão executam várias sessões a partir de uma única máquina para fornecer vários aplicativos e áreas de trabalho a vários usuários conectados simultaneamente. Cada usuário requer uma única sessão a partir da qual pode executar todos os 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 fica agora indisponível. Se ambos os usuários solicitarem mais aplicativos, nenhuma sessão adicional será necessária porque cada usuário pode executar vários aplicativos usando a mesma sessão. Se mais dois usuários efetuarem logon e solicitarem áreas de trabalho, e duas sessões estiverem disponíveis nessa máquina, a máquina agora usará quatro sessões para hospedar quatro usuários diferentes.

- Dentro do grupo de entrega ao qual um usuário está 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 fizer logon.

Aplicativos hospedados em VM

Use máquinas com SO de sessão única para fornecer aplicativos hospedados por VM

Caso de uso:

- Você deseja uma solução de entrega de aplicativos baseada em cliente que seja segura, forneça gerenciamento centralizado e ofereça suporte a muitos usuários por servidor host. Você deseja fornecer aos usuários, aplicativos que são exibidos diretamente em alta definição.
- Seus usuários são contratados internos, externos, colaboradores terceirizados e outros membros temporários de equipe. Seus usuários não precisam de 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:

- Os aplicativos e áreas de trabalho na imagem são gerenciados, hospedados e executados com segurança em máquinas dentro de seu datacenter, oferecendo uma solução de entrega de aplicativos mais econômica.
- No 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 sempre que o usuário fizer logon. As máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de várias sessões não é suportada em máquinas com SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega quando faz logon, e os usuários devem estar online para acessar seus aplicativos.

- Esse método pode aumentar a quantidade de recursos do servidor para processamento de aplicativos e aumentar a quantidade de armazenamento dos vDisks pessoais dos usuários.

Experiência do usuário:

- A mesma experiência de aplicativos que se tem ao hospedar aplicativos compartilhados em máquinas com SO multissessão.

Processamento, hospedagem e entrega de aplicativos:

- O mesmo que as máquinas com SO multissessão, exceto se trata de máquinas virtuais de SO de sessão única.

Gerenciamento e atribuição de sessões:

- As máquinas com SO de sessão única executam uma única sessão de área de trabalho a partir de uma única máquina. Quando acessa apenas aplicativos, um mesmo 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 que fizeram logon 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.

Áreas de trabalho VDI

Use máquinas com SO de sessão única para entregar áreas de trabalho VDI do Citrix Virtual Desktops.

As áreas de trabalho VDI são hospedadas em máquinas virtuais e fornecem a cada usuário um sistema operacional de área de trabalho.

As áreas de trabalho VDI requerem mais recursos do que as áreas de trabalho publicadas do Citrix Virtual Apps, mas não exigem que os aplicativos instalados neles suportem sistemas operacionais baseados em servidor. Além disso, dependendo do tipo de área de trabalho VDI que você escolher, essas áreas de trabalho podem ser atribuídas a usuários individuais. Isso permite aos usuários um alto nível de personalização.

Ao criar um catálogo de máquinas para áreas de trabalho VDI, você cria um destes tipos de áreas de trabalho:

- **Área de trabalho aleatória não persistente, também conhecida como área de trabalho VDI em pool:** cada vez que um usuário faz logon em uma dessas áreas de trabalho, esse usuário se conecta a uma área de trabalho selecionada a partir de um pool de áreas de trabalho. Esse pool é baseado em uma única imagem. Todas as alterações na área de trabalho são perdidas quando a máquina é reiniciada.

- **Área de trabalho não persistente estática:** durante o primeiro logon, uma área de trabalho é atribuída a um usuário a partir de um pool de áreas de trabalho. (Cada máquina no pool é baseada em uma única imagem.) Após o primeiro uso, cada vez que um usuário faz logon para usar uma dessas áreas de trabalho, esse usuário se conecta à mesma área de trabalho que foi atribuída na primeira utilização. Todas as alterações na área de trabalho são perdidas quando a máquina é reiniciada.
- **Área de trabalho persistente estática:** ao contrário de outros tipos de áreas de trabalho VDI, os usuários podem personalizar totalmente estas áreas de trabalho. Durante o primeiro logon, uma área de trabalho é atribuída a um usuário a partir de um pool de áreas de trabalho. Os logons subsequentes desse usuário conectam-se à mesma área de trabalho que foi atribuída na primeira utilização. As alterações na área de trabalho são mantidas quando a máquina é reiniciada.

Remote PC Access

O Remote PC Access é um recurso do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

O Remote PC Access usa os mesmos componentes do Citrix DaaS que entregam áreas de trabalho e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos que os necessários para implantar o Citrix DaaS para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

Para obter mais informações, consulte Acesso remoto ao PC.

Primeiros passos: Planeje e crie uma implantação

June 6, 2023

Se você não estiver familiarizado com os componentes, a terminologia e os objetos usados com o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), consulte Citrix DaaS.

Para uma perspectiva da jornada do cliente, acesse o Citrix Success Center. O Success Center fornece orientação para os cinco principais estágios de sua jornada Citrix: planejar, construir, implementar, gerenciar e otimizar.

- As informações do Success Center são um parceiro essencial para a documentação deste produto.
- Os artigos e guias do Success Center oferecem uma ampla perspectiva baseada em soluções. Eles também contêm links para detalhes específicos do serviço nesta documentação do produto.

Se você estiver migrando de uma implantação do Citrix Virtual Apps and Desktops, consulte Migrar para a nuvem.

> **Importante:**
>
> Para garantir que você obtenha informações importantes sobre o Citrix Cloud e os serviços Citrix que você assina, procure receber todas as notificações por e-mail.
>
> No canto superior direito do console do Citrix Cloud, expanda o menu à direita do nome do cliente e dos campos OrgID. Selecione **Configurações de conta**. Na guia **Meu perfil**, selecione todas as entradas na seção **Notificações por e-mail**.

Como usar este artigo

Para configurar a implantação do Citrix DaaS, conclua as tarefas resumidas abaixo. São fornecidos links para os detalhes de cada tarefa.

Analise todo o processo antes de iniciar a implantação, para saber o que esperar. Este artigo também contém links para outras fontes de informação úteis.

> **Nota:**
>
> Se você planeja usar a interface de Quick Deploy para provisionar máquinas do Microsoft Azure, siga as orientações de configuração em Introdução ao Quick Deploy.

Planeje e prepare

Use a orientação do Plano do Success Center para ajudar a estabelecer metas, definir casos de uso e objetivos de negócios, identificar riscos potenciais e criar um plano de projeto.

Na documentação do Citrix Tech Zone, consulte um guia de prova de conceito passo a passo para este serviço.

Registro

Registre-se para abrir uma conta da Citrix e solicite uma demonstração do Citrix DaaS.

Configurar um local de recursos

Um local de recursos contém os recursos necessários para fornecer aplicativos e áreas de trabalho aos usuários. A criação de locais de recursos permite que o DaaS use esses recursos. Para saber mais sobre os locais de recursos, consulte Conectar com o Citrix Cloud.

Antes de criar máquinas, você deve conectar um local de recursos ao DaaS:

- As máquinas ingressadas no domínio exigem que você tenha Cloud Connectors instalados no local de recursos. Nesse caso, você pode:
  - Criar catálogos ingressados no Active Directory no local
  - Criar catálogos ingressados no Azure Active Directory
  - Criar catálogos ingressados no Azure Active Directory híbrido

  Para alta disponibilidade, recomendamos que você instale dois conectores de nuvem em cada local de recursos. Consulte Instalação do Cloud Connector.

  Mais informações:

  - Quais são os locais de recursos e os Cloud Connectors?
  - Vídeo sobre a instalação de Cloud Connectors:

- Máquinas não ingressadas no domínio não precisam de Cloud Connectors, mas exigem que você tenha o Rendezvous V2 ativado. O protocolo Rendezvous permite que os VDAs ignorem os Cloud Connectors para se conectarem de forma direta e segura com o DaaS. Consulte Rendezvous V2. Nesse caso, você pode:
  - Criar catálogos não ingressados no domínio

Se você estiver usando a interface Quick Deploy para provisionar VMs do Azure, a Citrix criará o local do recurso e os Cloud Connectors para você.

Crie uma conexão com o local do recurso

Depois de adicionar um local de recurso e Cloud Connectors, crie uma conexão com o local do recursos usando a interface Full Configuration do Citrix DaaS.

Essa etapa não é necessária nos 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

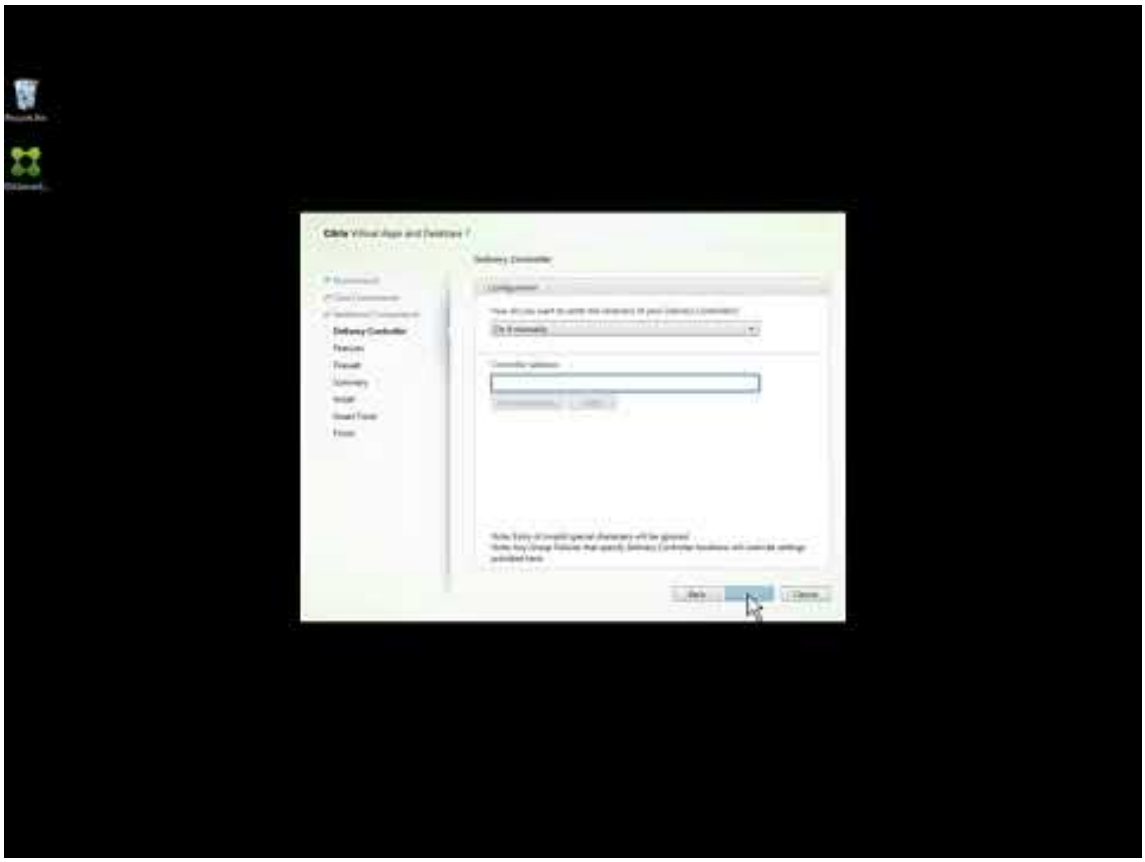
Em cada máquina que fornece aplicativos e áreas de trabalho aos usuários deve haver um Citrix Virtual Delivery Agent (VDA) instalado.

- Para uma implementação 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 acesso ao PC remoto, instale a versão principal do VDA para sistema operacional de sessão única em cada PC de escritório físico.

Instruções e mais informações:

- O que são VDAs?
- Preparação e instruções de instalação
- Instalação do VDA de linha de comando

- Vídeo sobre o download e a instalação de um VDA:

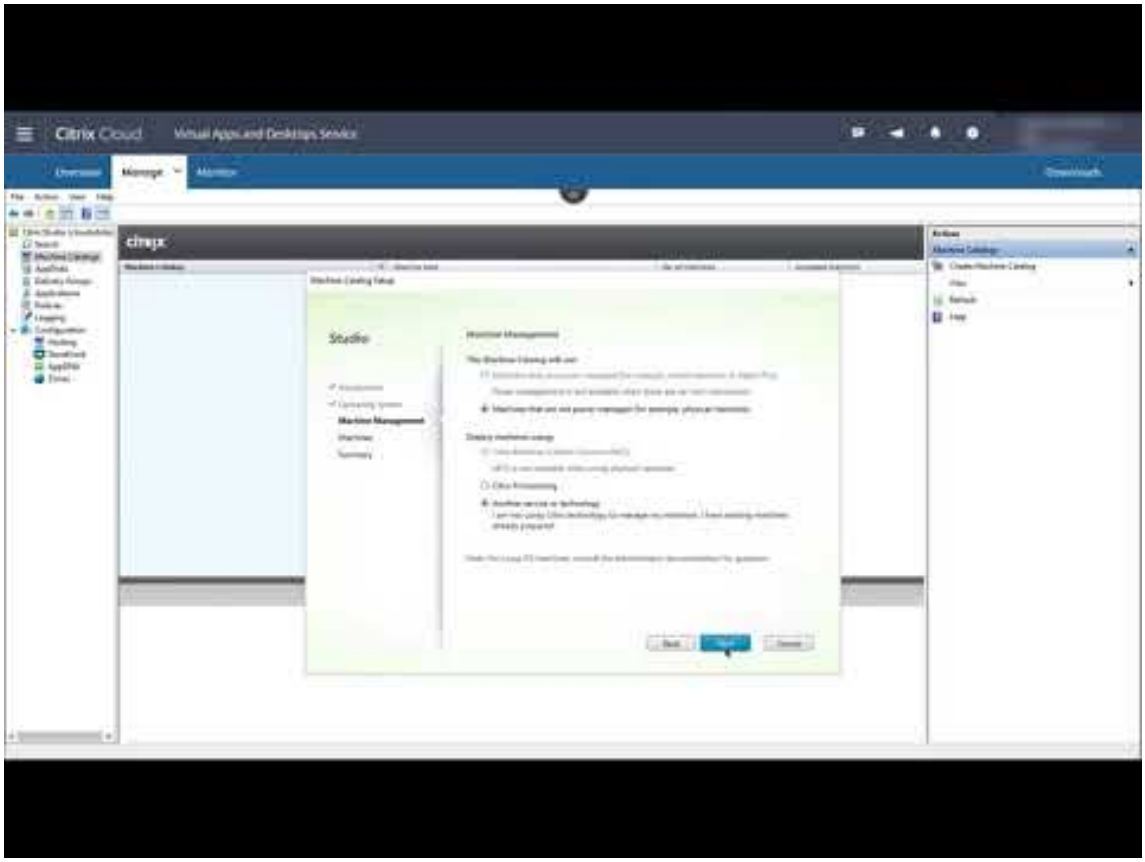


Crie um catálogo

Depois de criar uma conexão com o local do recurso (se necessário), você deve criar um catálogo. Se estiver usando a interface Full Configuration, o fluxo de trabalho o guiará automaticamente para esta etapa.

Instruções e mais informações:

- O que são catálogos?
- Crie um catálogo
- Use a interface Quick Deploy para implantar um catálogo contendo VMs do Azure.
- Vídeo sobre a criação de um catálogo usando a interface de gerenciamento Full Configuration:



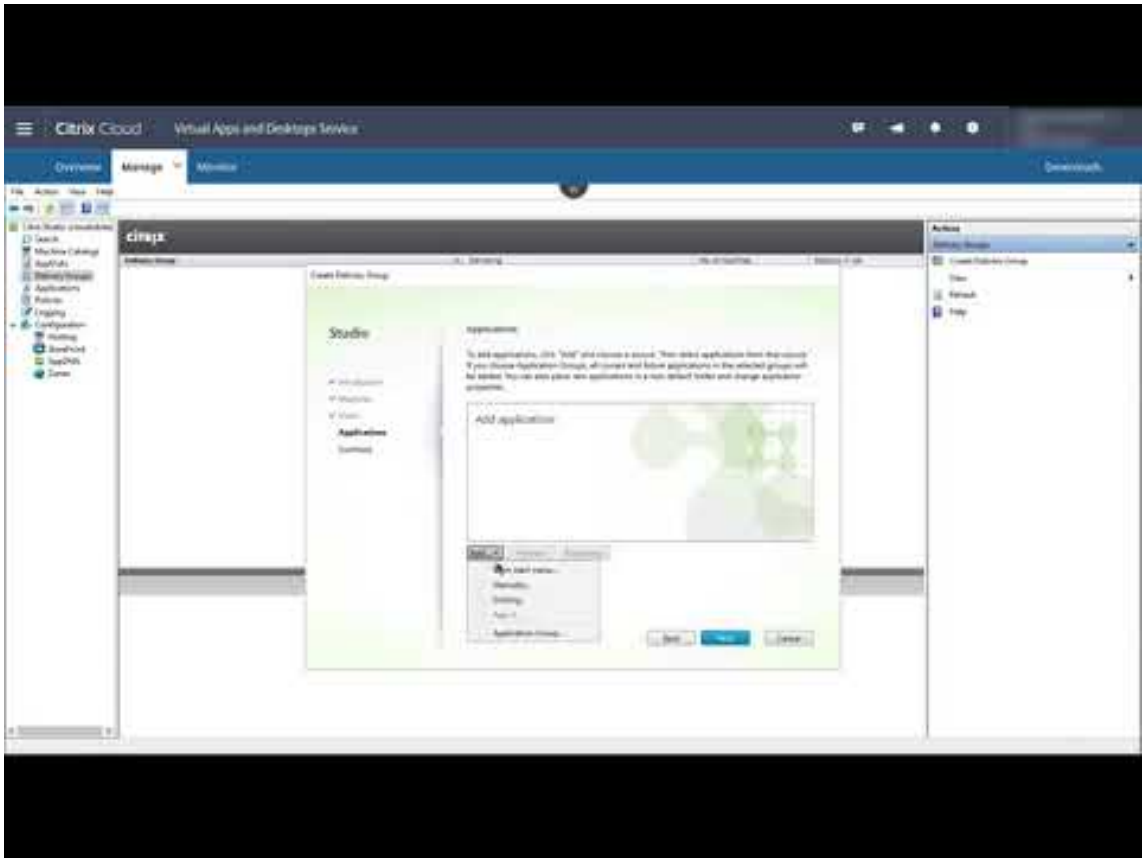
Criar um grupo de entrega

Depois de criar seu primeiro catálogo, o fluxo de trabalho **Manage** o orienta para criar um grupo de entrega.

Essa etapa não é necessária se você estiver usando a interface de Quick Deploy para provisionar VMs do Azure.

Instruções 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, siga as orientações na área Build do Citrix Success Center. Você encontrará informações sobre o provisionamento e a configuração de outros componentes e tecnologias na solução Citrix, como:

- Políticas da Citrix
- StoreFront
- App Layering
- Serviço de 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 Microsoft RDS License Server.

Iniciar aplicativos e desktops

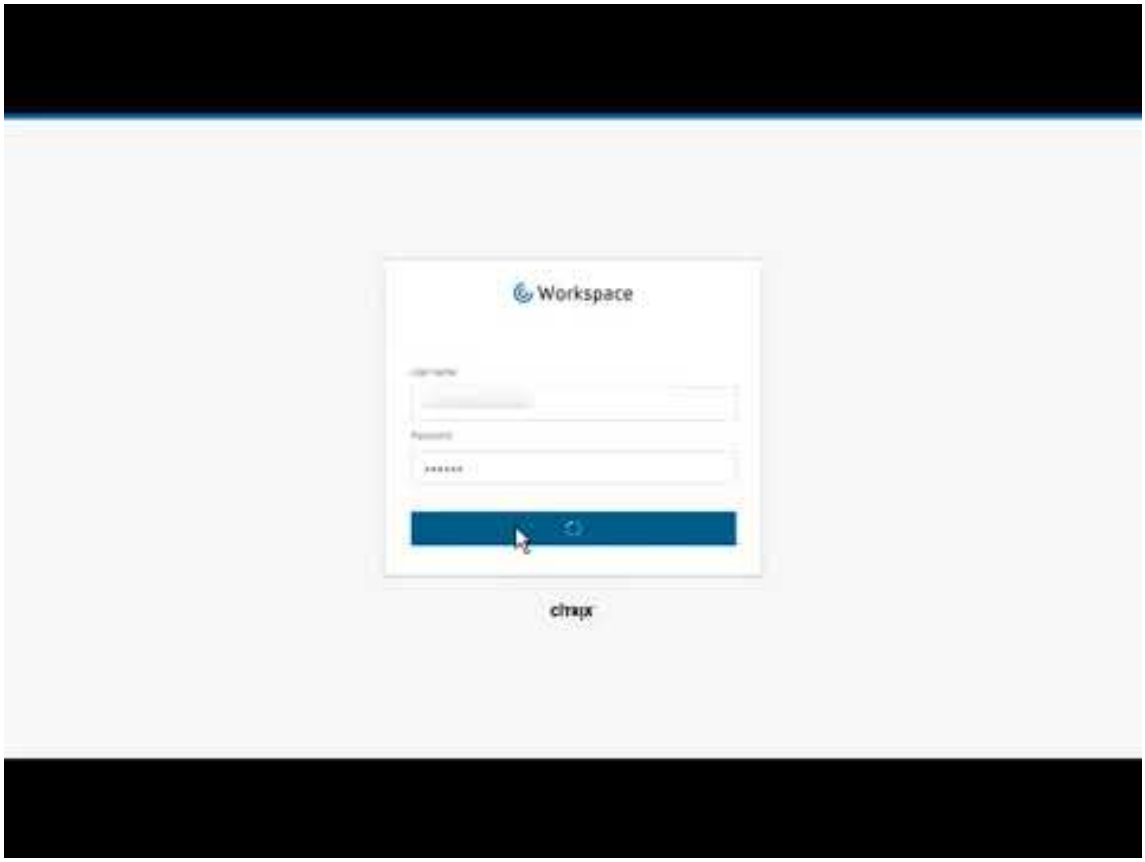
Depois de configurar a implantação, a publicação ocorre automaticamente. Os aplicativos e áreas de trabalho que você configurou estão disponíveis para os usuários em seu Citrix Workspace. Um usuário simplesmente navega até o URL do Workspace e seleciona um aplicativo ou área de trabalho, que é iniciado imediatamente.

Envie o URL do Workspace para seus usuários. Você pode encontrar o URL do espaço de trabalho em dois locais:

- No console do Citrix Cloud, selecione **Workspace Configuration** no menu no canto superior esquerdo. A guia **Access** contém o URL do Workspace.
- Na página **Overview** do Citrix DaaS, o URL do espaço de trabalho aparece próximo à parte inferior da página.

Mais informações:

- Vídeo sobre usuários iniciando aplicativos e áreas de trabalho a partir do espaço de trabalho:



Mais informações

A série Citrix Cloud Learning oferece cursos educacionais organizados pelo seu caminho:

- Se você é novo no Citrix DaaS, consulte New to Citrix DaaS Learning Path.
- Se você estiver migrando de uma implantação do Citrix Virtual Apps and Desktops, consulte Migrating Citrix DaaS to Citrix Cloud Learning Path.

Inscreva-se no Citrix DaaS

June 24, 2022

Introdução

Você pode assinar o Citrix DaaS por meio da Citrix ou do Azure Marketplace.

Se você planeja usar o Citrix Managed Azure, também pode solicitar o Citrix Azure Consumption Fund por meio da Citrix ou do Azure Marketplace.

- Ao fazer o pedido pela Citrix, você pode solicitar o Citrix DaaS e o Citrix Azure Consumption Fund ao mesmo tempo.
- Ao fazer o pedido por meio do Azure Marketplace, você primeiro faz o pedido do Citrix DaaS. Em seguida, você pode fazer o pedido do Citrix Azure Consumption Fund.

Se solicitar apenas o Citrix DaaS agora, você poderá solicitar o Citrix Azure Consumption Fund posteriormente, seja por meio do Azure Marketplace ou do seu representante de conta Citrix.

Demonstrações e avaliações

Você pode avaliar o Citrix DaaS mediante solicitação através da Citrix. Você pode converter uma avaliação em uma assinatura de serviço paga.

Durante uma avaliação, você pode opcionalmente usar uma assinatura do Citrix Managed Azure para catálogos, imagens e conexões de rede. Se você tiver recursos gerenciados pela Citrix no momento da conversão para uma assinatura paga, você deve comprar o consumo ou excluir os recursos gerenciados pela Citrix. Se você não comprar o consumo, os recursos serão excluídos automaticamente, o que pode afetar os usuários.

Se você atualmente assina um serviço Citrix DaaS

Geralmente, uma conta do Citrix Cloud permite que você registre apenas um dos serviços do Citrix DaaS (ou uma edição) por vez, por Citrix OrgID. Por exemplo, você pode assinar o Citrix DaaS Premium edition OU o Citrix DaaS for Azure, mas não ambos.

Se você atualmente assina um Citrix DaaS e deseja assinar este serviço, você tem duas opções:

- Registrar-se nesse serviço usando uma conta diferente do Citrix Cloud (OrgID).
- Desativar o Citrix DaaS que você já tem e, em seguida, solicitar este serviço. Para obter instruções para desinstalação, consulte CTX239027.

Pedidos pela Citrix

Você pode solicitar este serviço (e o Citrix Azure Consumption Fund) por meio do Citrix Cloud ou por meio de seu representante de conta Citrix.

Por meio do Citrix Cloud:

- Siga as orientações em Fazer login no Citrix Cloud para obter uma conta do Citrix Cloud e um ID da organização.
- Você pode solicitar uma demonstração do Citrix DaaS. No bloco Citrix DaaS, clique em **Request Demo**. Forneça as informações solicitadas.

  Um representante da Citrix entrará em contato com você para discutir seus requisitos, ambiente e planos. Dependendo da avaliação do nosso representante, você estará autorizado a participar de uma demonstração de administrador ou de um teste de prova de conceito. Para obter mais informações, consulte as Avaliações do Citrix Cloud Service.

Quando você está autorizado para uma avaliação, o texto no bloco Citrix DaaS no console do Citrix Cloud muda para **Manage**.

Pedido pelo Azure Marketplace

Você pode solicitar as seguintes ofertas da Citrix por meio do Azure Marketplace:

- Citrix DaaS para Azure
- Edição Citrix DaaS Advanced
- Edição Citrix DaaS 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 do Citrix Managed Azure, solicite o Citrix Azure Consumption Fund depois de solicitar o Citrix DaaS ou o Workspace Premium Plus.

Com o Citrix Azure Consumption Fund, você é cobrado mensalmente pelo seu consumo, que pode variar dependendo dos recursos de hospedagem escolhidos e das horas de uso. Você pode reavaliar o seu consumo por meio do Citrix Cloud.

No Azure Marketplace:

- Você não pode combinar o Citrix DaaS e o fundo de consumo em um único pedido.
- O processo de pedido do Citrix Azure Consumption Fund é essencialmente o mesmo que solicitar o Citrix DaaS, mas você deve ter solicitado o Citrix DaaS anteriormente.

Requisitos para pedidos por meio do Azure Marketplace

- O OrgID da sua conta do Citrix Cloud.
  - Se você tem uma conta do Citrix Cloud, mas não sabe o OrgID, procure no canto superior direito do console do Citrix Cloud. Ou encontre-o no e-mail que você recebeu quando criou a conta.
  - Se você não tiver uma conta do Citrix Cloud, siga as orientações em Fazer login no Citrix Cloud.
- Uma conta do Azure e pelo menos uma assinatura do Azure na conta.

Procedimento para fazer pedidos por meio do Azure Marketplace

Siga este procedimento para solicitar um Citrix DaaS ou Workspace Premium Plus por meio do Azure Marketplace. (Se você quiser usar o Citrix Managed Azure, faça outro pedido do Citrix Azure Consumption Fund, depois de solicitar o serviço Citrix DaaS.)

1. Faça login no Azure Marketplace usando suas credenciais de conta do Azure.
2. Pesquise e navegue até a oferta da Citrix que você deseja solicitar.
3. Selecione **Get it now**.
4. Na mensagem **One more thing**, preencha as informações necessárias, marque a caixa de seleção de consentimento e selecione **Continue**.
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 **Set up + subscribe**.
6. Na guia **Basics**:
   - **Subscription:** indica o plano que você selecionou.
   - **Resource group:** selecione ou crie um grupo de recursos.
   - **Name:** insira um nome para seu pedido de assinatura para que você possa identificá-lo facilmente mais tarde.
   - As informações em **Plan** mostram o preço do plano selecionado, com base no prazo de cobrança. Para alterar o prazo do plano, selecione **Change plan**. Selecione o prazo desejado e selecione **Change plan**.

7. Na guia **Review + subscribe**, revise as informações de contato e atualize-as, se necessário. Revise as informações básicas da assinatura. Selecione **Subscribe**.
8. Na página **Subscription in progress**, selecione **Configure account now**. (Se o botão estiver desativado, aguarde um momento.) Você é direcionado para uma página de ativação da Citrix.
9. Na página de ativação:
   - Use o link **Sign in** para fazer login no Citrix Cloud. Um login bem-sucedido preenche automaticamente o campo **Organization ID**.
   - **Quantity:** informe o número de usuários. (O pedido inicial deve ser de pelo menos 25.) O preço estimado é exibido.
   - Aceite os termos e condições e selecione **Activate Order**.

Depois de fazer o pedido pelo Azure Marketplace

A Citrix lhe envia um e-mail quando o serviço é 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.

O preenchimento de um pedido do Citrix Azure Consumption Fund não leva muito tempo. Quando a Citrix é notificada sobre o pedido, aparece uma faixa no console Citrix DaaS, indicando que uma assinatura do Citrix Managed Azure será preparada para você.

Não exclua o recurso Citrix DaaS no Azure. A exclusão desse recurso cancela a sua assinatura.

Pedidos pelo Google Cloud Marketplace

Você pode solicitar as seguintes ofertas da Citrix por meio do Google Cloud Marketplace:

- Citrix DaaS Standard para Google Cloud
- Citrix DaaS Premium para Google Cloud

Você precisa do seguinte para fazer o pedido por meio do Google Cloud Marketplace:

- O OrgID da sua conta do Citrix Cloud.
  - Se você tem uma conta do Citrix Cloud, mas não sabe o OrgID, procure no canto superior direito do console do Citrix Cloud. Ou encontre-o no e-mail que você recebeu quando criou a conta.
  - Se você não tiver uma conta do Citrix Cloud, siga as orientações em Fazer login no Citrix Cloud.
- Uma conta do Google Cloud e pelo menos uma assinatura do Google Cloud na conta.

Para fazer seu pedido:

1. Entre no Google Cloud Marketplace
2. Siga as instruções na página Citrix DaaS for Google Cloud para fazer sua compra.

A Citrix lhe envia um e-mail quando o serviço é 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 a sua assinatura.

O próximo passo

Depois que seu pedido for processado, continue com as próximas etapas em Planeje e crie uma implantação.

Por exemplo:

- Se você ainda não configurou seu hipervisor ou o serviço da nuvem, ou o Active Directory, consulte Configurar um local de recurso.
- Se o seu ambiente de host e o Active Directory já estiverem configurados, consulte Criar uma conexão.

Citrix HDX Plus para Windows 365

November 10, 2022

O Citrix HDX Plus para Windows 365 permite que você integre o Citrix Cloud ao Windows 365 para usar as tecnologias Citrix HDX para uma experiência aprimorada e mais segura do Windows 365 Cloud PC, além de outros serviços do Citrix Cloud para maior capacidade de gerenciamento.

Para obter mais informações, consulte Citrix HDX Plus para Windows 365

Citrix DaaS para Google Cloud

November 17, 2022

O Citrix DaaS para Google Cloud permite implantar áreas de trabalho e aplicativos do Google Cloud usando a interface de gerenciamento Full Configuration do Citrix DaaS. O Citrix DaaS para Google Cloud está disponível nas edições Standard e Premium.

Para obter informações sobre os recursos suportados, consulte a Matriz de recursos do Citrix Virtual Apps and Desktops.

Você pode solicitar o Citrix DaaS para Google Cloud no Google Cloud Marketplace.

Depois de solicitar o Citrix DaaS, faça login no Citrix Cloud. No menu superior esquerdo, selecione **My Services > DaaS**.

Siga as orientações de configuração nesta documentação do produto. Usando a interface Full Configuration, você pode criar conexões, catálogos e grupos de entrega, da mesma forma que faria ao usar essa interface com outras edições de produto. (Essas edições atualmente não têm uma interface de gerenciamento Quick Deploy.)

Algumas exibições na interface Full Configuration podem diferir das exibidas na documentação. Por exemplo, ao criar uma conexão em uma edição do Citrix Virtual Apps and Desktops para Google Cloud, os tipos de conexão disponíveis incluem os hipervisores compatíveis e o Google Cloud. Outros serviços em nuvem não estão disponíveis.

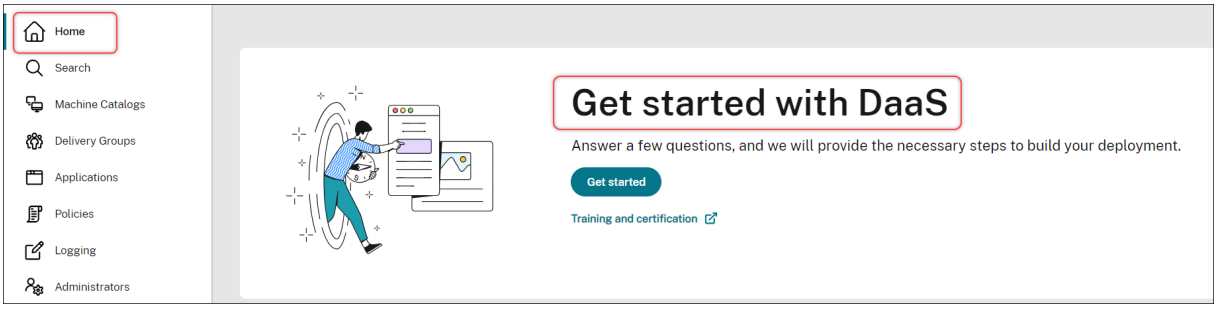
Da mesma forma, use as informações na documentação do produto que se aplicam aos hipervisores compatíveis e ao Google Cloud.

Para obter instruções passo a passo sobre como implantar e configurar o Citrix DaaS no Google Cloud, consulte este artigo da Citrix Tech Zone: Citrix virtualization on 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.

Usar o Guia de introdução do DaaS (prévia)

December 6, 2023

O guia de introdução do DaaS simplifica o processo de implantação do DaaS para administradores novos e experientes. Usando o guia, você pode configurar rapidamente suas implantações de DaaS respondendo a uma série de perguntas.



Este artigo mostra os processos de configuração de cinco cenários típicos de implantação de DaaS.

Benefícios

Os benefícios de usar este guia incluem:

- **Fácil de começar**. Este guia conecta etapas essenciais de implantação por meio de um fluxo de trabalho passo a passo conduzido por questionários. Se você for um novo administrador, poderá configurar rapidamente sua implantação enquanto aprende conceitos e terminologia por meio de ajuda contextual.
- **Simplifica as configurações complexas**. Este guia fornece parâmetros pré-configurados sempre que necessário além de acesso à interface de Full Configuration para configurações avançadas. Se você for um administrador experiente, poderá usar o guia como ponto de partida para configurações complexas.

Cenários de implantação compatíveis

Este guia fornece implantações rápidas para estes cenários:

O que entregar?	As máquinas já existem?	Tipo de máquina	Observação
Áreas de trabalho e aplicativos virtuais	Não	Máquinas virtuais (provisionadas pelo DaaS)	Energia gerenciada
Áreas de trabalho e aplicativos virtuais	Sim	Máquinas virtuais ou PCs blade	Energia gerenciada
Áreas de trabalho e aplicativos virtuais	Sim	Máquinas físicas ou virtuais	Sem gerenciamento de energia
PCs de escritório	Sim	Máquinas físicas	Energia gerenciada
PCs de escritório	Sim	Máquinas físicas	Sem gerenciamento de energia

Consulte as seções a seguir para obter instruções detalhadas:

- Entregar aplicativos e áreas de trabalho do zero (energia gerenciada)
- Entregar aplicativos e áreas de trabalho usando máquinas existentes (energia gerenciada)
- Entregar aplicativos e áreas de trabalho usando máquinas existentes (sem gerenciamento de energia)
- Entregar PCs de escritório (energia gerenciada)
- Entregar PCs de escritório (sem gerenciamento de energia)

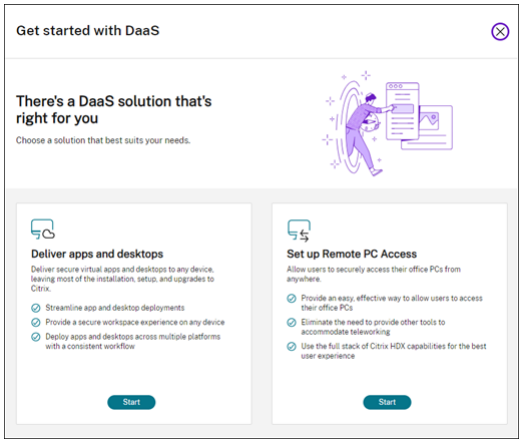
Terminologia

A seguir estão os termos específicos do DaaS:

- **Local de recursos.** Contém os recursos necessários para fornecer aplicativos e áreas de trabalho aos usuários.
- **Conexões de host.** Conecta o DaaS a um host (hipervisor ou serviço de nuvem) em um local de recursos. 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 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. Podem ser virtuais ou físicas, dependendo de 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 áreas de trabalho estão disponíveis para esses usuários.
- **Perfil da máquina.** Especifica as propriedades das máquinas virtuais. As VMs em um catálogo podem herdar propriedades de um perfil de máquina.

Acesso ao guia

1. Vá para a página **DaaS > Home**.
2. Localize **Get started with DaaS**.
3. Clique em **Get started** para iniciar seu processo de implantação.



> **Nota:**
>
> Você pode sair do processo a qualquer momento clicando em **Close**: o guia salva suas configurações automaticamente. Para continuar sua configuração, clique em **Continue**. Para começar do zero, clique em **Start over**.

Entregar aplicativos e áreas de trabalho do zero (energia gerenciada)

Esta seção orienta você pelo processo de implantação da criação de VMs e entrega de aplicativos e áreas de trabalho usando as VMs.

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](/en-us/citrix-cloud/citrix-cloud-management/identity-access-management#identity-providers.

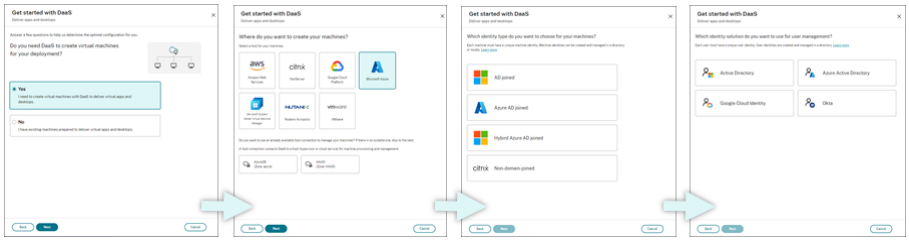
- Função: Full Administrator ou Cloud Administrator
- Permissões necessárias no hipervisor ou serviço de nuvem de destino.

  Para obter mais informações, consulte as seções correspondentes em Criar e gerenciar conexões.

- Credenciais de administrador para criação de conta da VM

Preparação

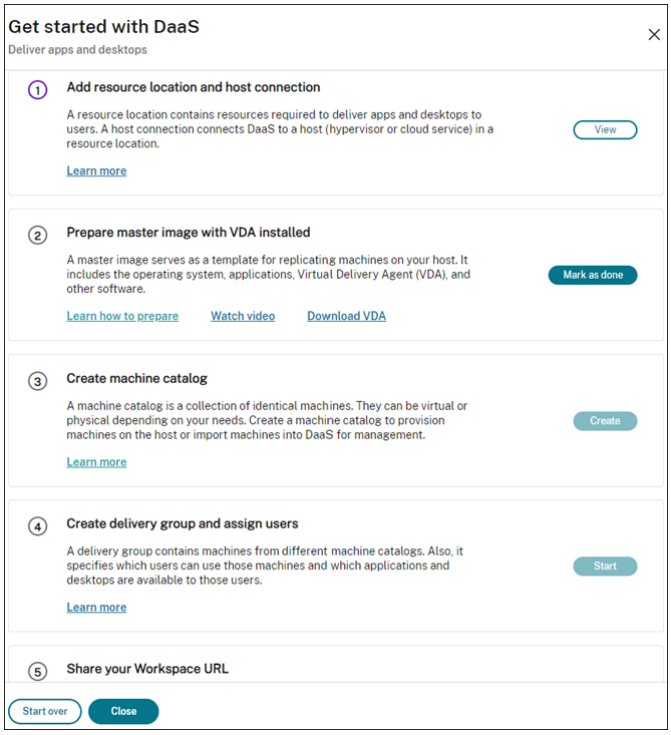
Responda às perguntas na tela para concluir as seguintes configurações no nível de infraestrutura. Consulte a tabela a seguir para obter detalhes.



Nº	Configuração	Descrição
1	Especifique se a criação da VM é necessária	Selecione **Yes**.
2	Selecione o tipo de host	Selecione um tipo de host para sua implantação. Opções: AWS, XenServer (antigo 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: AD joined, Azure AD joined, Hybrid Azure AD joined e Non-domain-joined
4	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários. Opções: Active Directory, Azure Active Directory, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações no nível de infraestrutura, as etapas específicas desse cenário de implantação aparecem da seguinte forma.



Siga as instruções na tela para concluir as configurações.

Etapa 1: adicionar um local de recursos e conexões de host Configure o local de recursos instalando Cloud Connectors e configure as conexões a hipervisores ou serviços de nuvem no local.

1. Dê um nome ao local de recursos.
2. Baixe e instale Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.
4. Adicione e configure conexões de host do local de recursos. As configurações detalhadas de uma conexão incluem:
   - Detalhes da conexão, como 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.

Etapa 2: preparar imagens mestre para suas máquinas Prepare imagens mestre em VMs no seu local de recursos. Para obter mais informações, consulte Preparar uma imagem mestre no hipervisor ou no serviço de nuvem.

Etapa 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. Dê um nome ao catálogo.
2. Selecione o tipo de máquina.

   Opções: Multi-session, Single-session static (áreas de trabalho pessoais) e Single-session random (áreas de trabalho em pool).
3. Selecione uma conexão de host.

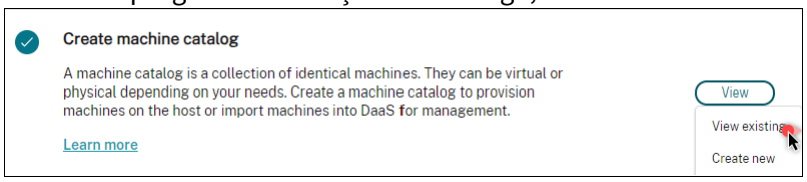
   As opções se originam de todas as conexões de host que você configurou para seus locais de recursos na Etapa 1.
4. Selecione uma imagem mestre.
5. Selecione um perfil de máquina.

   > **Nota:**
   >
   > Atualmente, o suporte ao perfil de máquina está disponível para serviços em nuvem do Azure, GCP e AWS, e o uso do perfil de máquina é opcional para GCP.
6. Defina quantas máquinas você deseja criar.
7. Defina a identidade das máquinas.

   Por padrão, é exibido o tipo de identidade da máquina que você selecionou na fase de preparação. Forneça as configurações de identidade necessárias para as VMs, como domínio, unidade organizacional e esquema de nomenclatura.
8. Insira as credenciais de administrador necessárias para a criação da máquina.
9. Clique em **Create**.

   > **Dica:**
   >
   > O botão **Create** só estará disponível depois que você fornecer todas as configurações necessárias.

Para ver 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, verifique os catálogos existentes para garantir que pelo menos um catálogo tenha sido criado com sucesso. Caso contrário, você não poderá 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 áreas de trabalho você deseja disponibilizar para usuários atribuídos

1. Dê um nome ao 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 áreas de trabalho disponíveis para esse 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 forneça as configurações necessárias, como caminho, diretório de trabalho e outras
   - (Visível somente em máquinas com SO multissessão) Para entrega em área de trabalho, mantenha a opção **Enable desktop delivery** selecionada.
4. Adicione usuários que possam acessar aplicativos e áreas de trabalho nesse grupo.

Etapa 5: compartilhar a URL do Workspace com seus usuários Vá para **Workspace Configuration > Access** e compartilhe a URL do Workspace com seus usuários.

Entregar aplicativos e áreas de trabalho usando máquinas existentes (energia gerenciada)

Esta seção orienta você pelo processo de implantação de entrega de aplicativos e áreas de trabalho usando máquinas existentes (com energia gerenciada).

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: Full Administrator ou Cloud Administrator

Preparação

Responda às perguntas na tela para concluir as seguintes configurações no nível de infraestrutura.

Nº	Definição	Descrição
1	Especifique se a criação da VM é necessária	Selecione **No**.
2	Selecione se o gerenciamento de energia é necessário	Selecione **Machines that are power managed (for example, virtual machines or blade PCs)**.
3	Selecione a plataforma do host	Selecione a plataforma do host em que 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.

Nº	Definição	Descrição
		Opções: Active Directory, Azure Active Directory, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações em nível de infraestrutura, as etapas específicas desse cenário de implantação aparecem. Siga as instruções na tela para concluir as configurações.

Etapa 1: adicionar um local de recursos e conexões de host Configure o local de recursos instalando Cloud Connectors e configure as conexões a hipervisores ou serviços de nuvem no seu local.

1. Dê um nome ao local de recursos.
2. Baixe e instale Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.
4. Adicione e configure conexões de host do local de recursos. Exemplos de configurações de conexão incluem o endereço da conexão, o nome do usuário e a senha.

> **Nota:**
>
> O DaaS gerencia a energia das máquinas em locais de recursos 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. Dê um nome ao catálogo
2. Selecione o tipo de máquina.

   Opções: Multi-session, Single-session static (áreas de trabalho pessoais) e Single-session random (áreas de trabalho em pool).
3. Selecione um local de recursos.
4. Importe máquinas para o catálogo.
   As máquinas são organizadas pela conexão do host. Escolha uma conexão de host para importar máquinas associadas.
5. Clique em **Create**.

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
- Especificar quais aplicativos e áreas de trabalho você deseja disponibilizar para usuários atribuídos

1. Dê um nome ao grupo.
2. Selecione um catálogo de máquinas conforme necessário e especifique quantas máquinas estão disponíveis para o grupo de entrega.
3. Especifique os aplicativos e áreas de trabalho disponíveis para esse 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 forneça as configurações necessárias, como caminho, diretório de trabalho e outras
   - (Visível somente em máquinas com SO multissessão) Para entrega em área de trabalho, mantenha a opção **Enable desktop delivery** selecionada.
4. Adicione usuários ao grupo.

Etapa 4: compartilhar a URL do Workspace com seus usuários Vá para **Workspace Configuration > Access** e compartilhe a URL do Workspace com seus usuários.

Entregar aplicativos e áreas de trabalho usando máquinas existentes (sem gerenciamento de energia)

Esta seção orienta você pelo processo de implantação de entrega de aplicativos e áreas de trabalho usando máquinas existentes (sem 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](/en-us/citrix-cloud/citrix-cloud-management/identity-access-management#identity-providers

- Função: Full Administrator ou Cloud Administrator

Preparação

Responda às perguntas na tela para concluir as seguintes configurações no nível de infraestrutura.

Nº	Definição	Descrição
1	Especifique se a criação da VM é necessária	Selecione **No**.
2	Selecione se o gerenciamento de energia é necessário	Selecione **Machines that are not power managed (for example, physical machines)**.
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários. Opções: Active Directory, Azure Active Directory, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações em nível de infraestrutura, as etapas específicas desse cenário de implantação aparecem. Siga as instruções na tela para concluir as configurações.

Etapa 1: adicionar um local de recursos Configure o seu local de recursos instalando o Cloud Connectors.

1. Dê um nome ao local de recursos.
2. Baixe e instale Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.

> **Nota:**
>
> A criação de conexões de host é necessária somente quando você deseja gerenciar a energia das máquinas.

Etapa 2: Crie um catálogo de máquinas Crie um catálogo de máquinas e importe suas máquinas para ele.

1. Dê um nome ao catálogo

2. Selecione o tipo de máquina.

   Opções: Multi-session, Single-session static (áreas de trabalho pessoais) e Single-session random (áreas de trabalho em pool).

3. Selecione um local de recursos.
4. Importe máquinas para o catálogo.

   Para facilitar a pesquisa na máquina, use nomes parciais de computador e seleção de diretórios.

5. Clique em **Create**.

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
- Especificar quais aplicativos e áreas de trabalho você deseja disponibilizar para usuários atribuídos

1. Dê um nome ao grupo.
2. Selecione um catálogo de máquinas conforme necessário e especifique quantas máquinas estão disponíveis para o grupo de entrega.
3. Especifique os aplicativos e áreas de trabalho disponíveis para esse 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 forneça as configurações necessárias, como caminho, diretório de trabalho e outras
   - (Visível somente em máquinas com SO multissessão) Para entrega em área de trabalho, mantenha a opção **Enable desktop delivery** selecionada.

4. Adicione usuários ao grupo.

Etapa 4: compartilhar a URL do Workspace com seus usuários Vá para **Workspace Configuration > Access** e compartilhe a URL do Workspace com seus usuários.

Entregar PCs de escritório (energia gerenciada)

Esta seção orienta você pelo processo de implantação da entrega de PCs de escritório (com energia gerenciada).

Pré-requisitos

Antes de começar, você precisa:

- Nomes das máquinas dos PCs.
- O Citrix Virtual Delivery Agent (VDA) instalado em cada PC. (Essa etapa pode ser realizada após a criação do catálogo.)

  Para obter mais informações, consulte Download VDA.

Preparação

Responda às perguntas na tela para concluir as seguintes configurações no nível de infraestrutura.

Nº	Etapa	Descrição
1	Selecione o tipo de alocação da máquina.	Selecione como as máquinas são atribuídas. Opções: Static auto-assigned, Static preassigned e Random pool unassigned
2	Determine se é permitido que os usuários liguem as máquinas	Selecione **I want remote users to power on machines by themselves**.
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários. Opções: Active Directory, Azure Active Directory, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações em nível de infraestrutura, as etapas específicas desse cenário de implantação aparecem. Siga as instruções na tela para concluir as configurações.

Etapa 1: adicionar um local de recursos e conexões de host Configure seu local de recursos instalando o Cloud Connectors e adicione uma conexão do tipo **Remote PC Wake on LAN**.

1. Dê um nome ao local de recursos.

2. Baixe e instale Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.
4. Clique em **Add new** para adicionar uma conexão:

   a) Selecione um local de recursos (zona).
   b) Selecione **Remote PC Wake on LAN** em **Connection type**.
   c) Insira um nome para a conexão.

> **Nota:**
>
> O DaaS gerencia a energia das máquinas por meio das conexões configuradas. Você deve configurar as conexões do tipo **Remote PC Wake on LAN** ao criar catálogos do Remote PC Access para máquinas com energia gerenciada.

Etapa 2: criar um catálogo Remote PC Access Crie um catálogo de máquinas e importe seus PCs do escritório para ele.

1. Dê um nome ao catálogo
2. Selecione um local de recursos.
3. Selecione um tipo de alocação de máquina. Por padrão, o tipo que você selecionou 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 **Create**.

Etapa 3: criar grupos de entrega e atribuir usuários Crie um grupo de entrega para agrupar as máquinas que você deseja entregar e especifique quem pode acessá-las.

1. Dê um nome ao grupo.
2. Selecione um catálogo de máquinas conforme necessário. Somente os catálogos **Remote PC Access** são exibidos.
3. Atribua usuários ao grupo.

Etapa 4: compartilhar a URL do Workspace com seus usuários Vá para **Workspace Configuration > Access** e compartilhe a URL do Workspace com seus usuários.

Entregar PCs de escritório (sem gerenciamento de energia)

Esta seção orienta você no processo de implantação de entrega de PCs de escritório (sem gerenciamento de energia).

Pré-requisitos

Antes de começar, você precisa:

- Nomes das máquinas dos PCs.
- O Citrix Virtual Delivery Agent (VDA) instalado em cada PC. (Essa etapa pode ser realizada após a criação do catálogo.)

  Para obter mais informações, consulte Download VDA.

Preparação

Responda às perguntas na tela para concluir as seguintes configurações no nível de infraestrutura.

Nº	Definição	Descrição
1	Selecione o tipo de alocação da máquina.	Selecione como as máquinas são atribuídas. Opções: Static auto-assigned, static preassigned e random pool unassigned
2	Determine se é permitido que os usuários liguem as máquinas	Desmarque **I want remote users to power on machines by themselves**.
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários. Opções: Active Directory, Azure Active Directory, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações em nível de infraestrutura, as etapas específicas desse cenário de implantação aparecem. Siga as instruções na tela para concluir as configurações.

Etapa 1: adicionar um local de recursos Configure o seu local de recursos instalando o Cloud Connectors.

1. Dê um nome ao local de recursos.

2. Baixe e instale Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.

> **Nota:**
>
> A criação de conexões de host é necessária somente quando você deseja gerenciar a energia das máquinas.

Etapa 2: criar um catálogo Remote PC Access Crie um catálogo e importe seus PCs do escritório para ele.

1. Dê um nome ao catálogo
2. Selecione um local de recursos.
3. Selecione um tipo de alocação. Por padrão, o tipo que você selecionou na fase de preparação é exibido.
4. Importe suas máquinas.
5. Clique em **Create**.

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. Dê um nome ao grupo.
2. Selecione um catálogo de máquinas conforme necessário. Somente os catálogos **Remote PC Access** são exibidos.
3. Atribua usuários para o grupo.

Etapa 4: compartilhar a URL do Workspace com seus usuários Vá para **Workspace Configuration > Access** e compartilhe a URL do Workspace com seus usuários.

Identidades de máquina

November 9, 2023

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 Azure AD. A Citrix oferece suporte à hospedagem de aplicativos e áreas de trabalho virtuais em máquinas ingressadas no Active Directory, ingressadas no Azure Active Directory, ingressadas no Hybrid Azure Active Directory 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
AD joined	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 Azure AD	As identidades são criadas e gerenciadas no Azure AD. As máquinas provisionadas são ingressadas no Azure AD usando as identidades de máquina atribuídas. Não é possível importar VMs para o Citrix DaaS.
Hybrid Azure AD joined	As identidades são criadas no Active Directory local e sincronizadas com o Azure AD por meio do Azure AD Connect. As máquinas provisionadas são ingressadas no Active Directory local e no Azure AD. As máquinas são então ingressadas no Azure AD híbrido. Para importar uma VM ingressada no Azure AD 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. Não é possível importar VMs para o Citrix DaaS.

Configurações suportadas

A seguir estão os detalhes das configurações suportadas para cada cenário.

Infraestrutura compatível

Identidade da máquina	Citrix DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
AD joined	Sim	Sim	Sim	Sim	Sim
Ingressado no Azure AD	Sim	Sim	Não	Sim	Não
Hybrid Azure AD joined	Sim	Sim	Sim	Sim	Sim
Non-domain-joined	Sim	Sim	Sim	Sim	Sim

> **Nota**
>
> Nem o cache de host local nem a continuidade de serviço estão disponíveis para hosts de sessões não ingressadas no domínio ao usar o Storefront.

Provedores de identidade de autenticação de espaço de trabalho compatíveis

Identidade da máquina	Azure Active Directory	Active Directory	Active Directory e Token	Okta	SAML	Citrix Gateway	Autenticação Adapta-tiva
AD joined	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Ingressado no Azure AD	Sim	Não	Não	Não	Não	Não	Não
Hybrid Azure AD joined	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Non-domain-joined	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Ingressado no Active Directory

July 4, 2023

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. Para obter mais informações sobre os níveis funcionais suportados pela floresta e pelo domínio, consulte Níveis funcionais do Active Directory.

Para obter informações sobre como criar catálogos ingressados no Active Directory (AD) usando o Citrix DaaS, consulte Criar catálogos de máquinas.

Azure Active Directory ingressado

August 17, 2023

Este artigo descreve os requisitos para criar catálogos ingressados do Azure Active Directory (AAD) usando o Citrix DaaS, além dos requisitos descritos na seção de requisitos do sistema Citrix DaaS.

Requisitos

- Plano de controle: consulte Configurações suportadas
- Tipo de VDA: sessão única (somente áreas de trabalho) ou multissessão (aplicativos e áreas de trabalho)
- Versão do VDA: 2203 ou posterior
- Tipo de provisionamento: Machine Creation Services (MCS) persistentes e não persistentes usando fluxo de trabalho de perfil de máquina
- Tipo de atribuição: dedicada e em pool
- Plataforma de hospedagem: somente Azure
- Rendezvous V2 deve estar habilitado

Limitações

- A continuidade do serviço não tem suporte.
- O logon único a áreas de trabalho virtuais não é aceito. Os usuários devem inserir as credenciais manualmente ao fazer login em suas áreas de trabalho.
- O login com o Windows Hello na área de trabalho virtual não tem suporte. Somente nome de usuário e senha são suportados no momento. Se os usuários tentarem fazer login usando um método do Windows Hello, eles recebem um erro informando que não são o usuário intermediado e a sessão é desconectada. Os métodos associados incluem PIN, chave FIDO2, MFA e assim por diante.
- Aceita apenas os ambientes de nuvem do Microsoft Azure Resource Manager.

- A primeira vez que uma sessão de área de trabalho virtual é iniciada, a tela de entrada do Windows pode mostrar o prompt de logon do 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, em seguida, clique na tela de bloqueio para revelar a tela de logon novamente. Nesse ponto, o usuário pode selecionar **Other user** e fornecer suas credenciais. Esse é o comportamento de cada nova sessão quando as máquinas são não persistentes.

Considerações

Configuração da imagem

- Considere otimizar sua imagem do Windows usando a ferramenta Citrix Optimizer.

Ingressado no Azure AD

- Considere desativar o Windows Hello para que os usuários não sejam solicitados a configurá-lo quando fizerem login em suas áreas de trabalho virtuais. Se você estiver usando o VDA 2209 ou posterior, isso é feito automaticamente. Em versões anteriores, você pode fazer isso de duas maneiras:
  - Política de grupo ou política local
    - Navegue até **Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business**.
    - Defina **Use Windows Hello for Business** como:
      - **Disabled** ou
      - **Enabled** e selecione **Do not start Windows Hello provisioning after sign-in**.
  - Microsoft Intune
    - Crie um perfil de dispositivo que desative o Windows Hello for Business. Consulte a documentação da Microsoft para obter detalhes.
    - Atualmente, a Microsoft oferece suporte ao registro do Intune somente de máquinas persistentes, o que significa que você não pode gerenciar máquinas não persistentes com o Intune.
- Os usuários devem receber acesso explícito no Azure para fazer login nas máquinas usando suas credenciais AAD. Isso pode ser facilitado adicionando a atribuição de função no nível do grupo de recursos:
  1. Faça login no portal do Azure.
  2. Selecione **Resource Groups**.

3. Clique no grupo de recursos em que as cargas de trabalho da área de trabalho virtual residem.
4. Selecione **Access control (IAM)**.
5. Clique em **Add role assignment**.
6. Procure por **Virtual Machine User Login**, selecione-o na lista e clique em **Next**.
7. Selecione **User, group, or service principal**.
8. Clique em **Select members** e selecione os usuários e grupos aos quais você deseja fornecer acesso às áreas de trabalho virtuais.
9. Clique em **Select members**.
10. Clique em **Review + assign**.
11. Clique em **Review + assign** mais uma vez.

> **Nota:**
>
> Se você optar por permitir que o MCS crie o grupo de recursos para as áreas de trabalho virtuais, adicione essa atribuição de função após a criação do catálogo de máquinas.

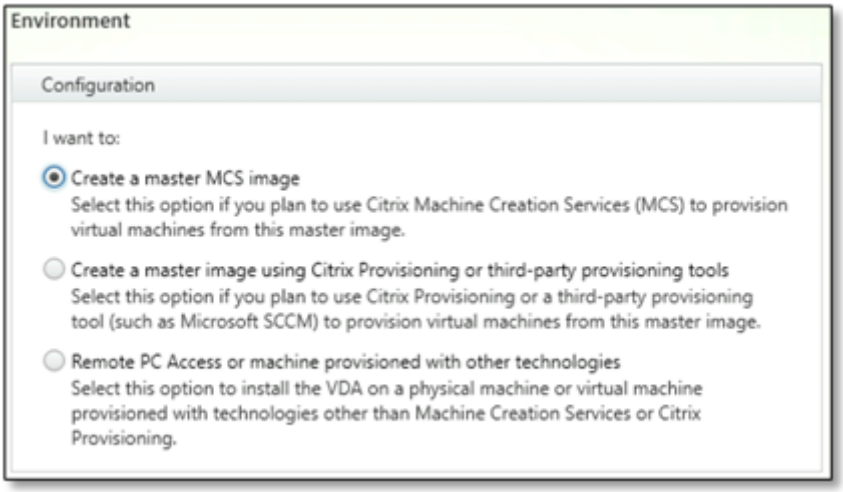
- As VMs mestre podem ser ingressadas no Azure AD ou não ingressadas no domínio. Essa funcionalidade requer a versão 2212 ou posterior do VDA.

Instalação e configuração do VDA

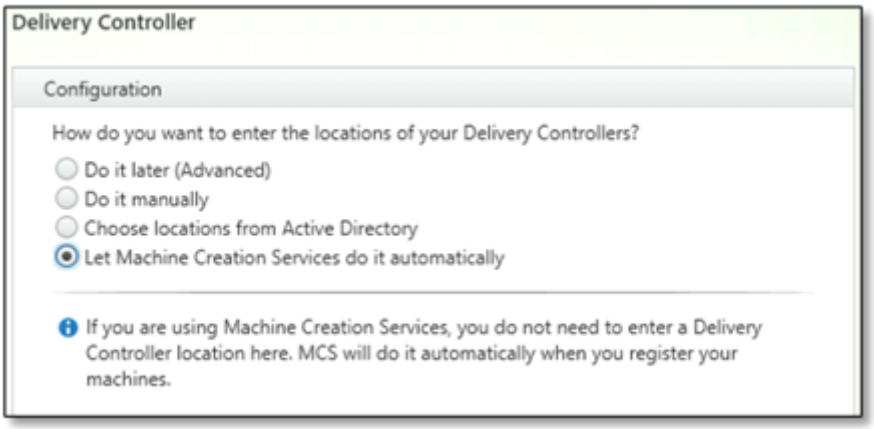
Siga as etapas para instalar o VDA:

1. Tenha o cuidado de selecionar as seguintes opções no assistente de instalação:

   - Na página Ambiente, selecione **Create a master MCS image**.



   - Na página Delivery Controller, selecione **Let Machine Creation Services do it automatically**.



2. Depois que o VDA for instalado, adicione o seguinte valor de registro:
   - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo de valor: DWORD
   - Nome do valor: GctRegistration
   - Dados de valor: 1
3. Para a 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. Essa tarefa de agendar uma tarefa na VM mestre só é necessária para o VDA versão 2212 ou anterior.

```
reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
    /d Citrix /f
<!--NeedCopy-->
```

4. Se você ingressar a VM mestre no Azure AD e remover o ingresso manualmente pelo utilitário `dsregcmd`, certifique-se de que o valor de `AADLoginForWindowsExtensionJoined` em HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension é zero.

O que fazer a seguir

Quando a localização do recurso e a conexão de hospedagem estiverem disponíveis, continue com a criação do catálogo de máquinas. Para obter mais informações sobre como criar catálogos de máquinas ingressados do Azure Active Directory, consulte Criar catálogos ingressados no Azure Active Directory.

Microsoft Intune

July 4, 2023

Este artigo descreve os requisitos para criar catálogos habilitados para o Microsoft Intune usando o Citrix DaaS, além dos requisitos descritos na seção de requisitos do sistema Citrix DaaS.

O 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 Navegadores e sistemas operacionais suportados no Intune.

O Microsoft Intune funciona usando a funcionalidade do Azure AD.

> **Importante:**
>
> Antes de habilitar esse recurso, verifique se o seu ambiente do Azure atende aos requisitos de licenciamento para usar o Microsoft Intune. Para obter mais informações, consulte a documentação da Microsoft: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses. Não ative o recurso se você não tiver a licença apropriada do Intune.

Requisitos

- Plano de controle: Citrix DaaS
- Tipo de VDA: VDA com SO de sessão única
- Versão do VDA: 2203 ou posterior
- Tipo de provisionamento: Machine Creation Services (MCS) persistente e não persistente usando somente fluxo de trabalho de perfil de máquina
- Tipo de atribuição: dedicada
- Plataforma de hospedagem: somente Azure

Limitações

- Oferece suporte somente a VMs persistentes ingressadas no Azure AD de sessão única
- Oferece suporte somente a VMs persistentes ingressadas no Azure AD híbrido de sessão única usando credencial de usuário ou credencial de dispositivo com recurso de cogerenciamento. Para obter mais informações, consulte Registrar um dispositivo Windows automaticamente usando a Política de Grupo.
- Não pule a preparação de imagens ao criar ou atualizar catálogos de máquinas.

Considerações

- Crie um perfil de dispositivo que desative o Windows Hello for Business.
- Use o VDA versão 2212 ou posterior se o Microsoft Intune precisar gerenciar uma VM mestre.

O que fazer a seguir

Para obter informações sobre como criar catálogos habilitados para o Microsoft Intune, consulte Criar catálogos habilitados para o Microsoft Intune.

Ingressado no Azure Active Directory híbrido

April 14, 2023

Este artigo descreve os requisitos para criar catálogos ingressados do Hybrid Azure Active Directory (HAAD) usando o Citrix DaaS, além dos requisitos descritos na seção de requisitos do sistema Citrix DaaS.

As máquinas ingressadas no Azure AD híbrido usam o AD local como o provedor de autenticação. Você pode atribuí-las a grupos ou usuários de domínio no AD local. Para habilitar a experiência de SSO fluida do Azure AD, você precisa ter os usuários do domínio sincronizados com o Azure AD.

> **Nota:**
>
> As VMs ingressadas do Hybrid Azure AD são suportadas em infraestruturas de identidade federadas e gerenciadas.

Requisitos

- Plano de controle: consulte Configurações suportadas
- Tipo de VDA: sessão única (somente áreas de trabalho) ou multissessão (aplicativos e áreas de trabalho)
- Versão do VDA: 2212 ou posterior
- Tipo de provisionamento: Machine Creation Services (MCS), persistente e não persistente
- Tipo de atribuição: dedicada e em pool
- Plataforma de hospedagem: qualquer hipervisor ou serviço em nuvem

Limitações

- Se o Serviço de autenticação federada (FAS) da Citrix for usado, o logon único será direcionado para o AD local em vez de para o Azure AD. Nesse caso, é recomendável configurar a autenticação baseada em certificado do Azure AD para que o token de atualização principal (PRT) seja gerado no login do usuário, o que facilita o logon único nos recursos do Azure AD na sessão. Caso contrário, o PRT não estará presente e o SSO aos recursos do Azure AD não funcionará.

Para obter informações sobre como obter o logon único (SSO) do Azure AD para VDAs ingressados híbridos usando o Citrix Federated Authentication Service (FAS), consulte VDAs ingressados híbridos.

- Não pule a preparação de imagens ao criar ou atualizar catálogos de máquinas. Se você quiser pular a preparação da imagem, certifique-se de que as VMs mestre não sejam ingressadas no Azure AD ou no Hybrid Azure AD.

Considerações

- A criação de máquinas ingressadas no Azure Active Directory 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 no Azure AD híbrido é gerenciado pela Citrix. Você precisa desabilitar `autoWorkplaceJoin` controlado pelo Windows nas VMs mestre da seguinte forma. A tarefa de desabilitar manualmente `autoWorkplaceJoin` só é necessária para o VDA versão 2212 ou anterior.

  1. Execute `gpedit.msc`.
  2. Navegue para **Computer Configuration > Administrative Templates > Windows Components > Device Registration**.
  3. Defina **Register domain joined computers as devices** como **Disabled**.

- Selecione a Unidade Organizacional (UO) que está configurada para ser sincronizada com o Azure AD ao criar as identidades de máquina.
- Para a VM mestre baseada no Windows 11 22H2, crie uma tarefa agendada na VM mestre que execute os seguintes comandos na inicialização do sistema usando a conta SYSTEM. Essa tarefa de agendar uma tarefa na VM mestre só é necessária para o VDA versão 2212 ou anterior.

```
$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')
    {

```



```
15            break;
16        }
17
18
19       if ($provider -eq 1)
20       {
21
22           Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
                Provider" -Value "Citrix" -Force
23           Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
                autoWorkplaceJoin" -Value 1 -Force
24           Start-Sleep 5
25           dsregcmd /join
26           break
27        }
28
29      }
30
31
32     Start-Sleep 1
33    }
34
35   <!--NeedCopy-->
```

O que fazer a seguir

Para obter mais informações sobre como criar catálogos ingressados do Hybrid Azure Active Directory, consulte Criar catálogos ingressados no Hybrid Azure Active Directory.

Non-domain-joined

November 21, 2023

Este artigo descreve os requisitos para criar catálogos não ingressados no domínio usando o Citrix DaaS, além dos requisitos descritos na seção de requisitos do sistema Citrix DaaS.

Requisitos

- Plano de controle: consulte Configurações suportadas
- Tipo de VDA: sessão única (somente áreas de trabalho) ou multissessão (aplicativos e áreas de trabalho)
- Versão do VDA: 2203 ou posterior
- Tipo de provisionamento: Machine Creation Services (MCS), persistente e não persistente

- Tipo de atribuição: dedicada e em pool
- Plataforma de hospedagem: todas as plataformas suportadas pelo MCS
- Rendezvous V2 deve estar habilitado
- Cloud Connectors: serão necessários apenas se você planeja provisionar máquinas não ingressadas no domínio em hipervisores locais ou se quiser usar o Active Directory como provedor de identidade no Workspace.

Limitações

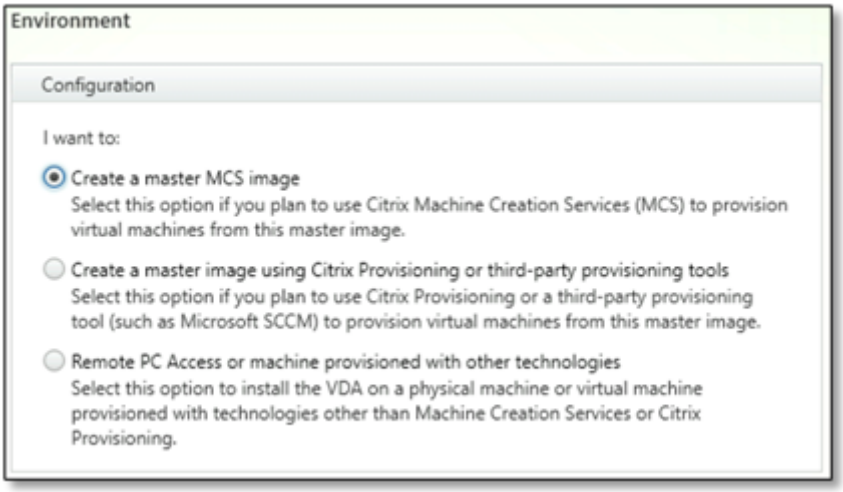
- A continuidade do serviço não tem suporte.
- Sempre que usamos um VDA multissessão não ingressado no domínio, os dados do perfil do usuário local não são retidos, eles são excluídos no logoff.

Instalação e configuração do VDA

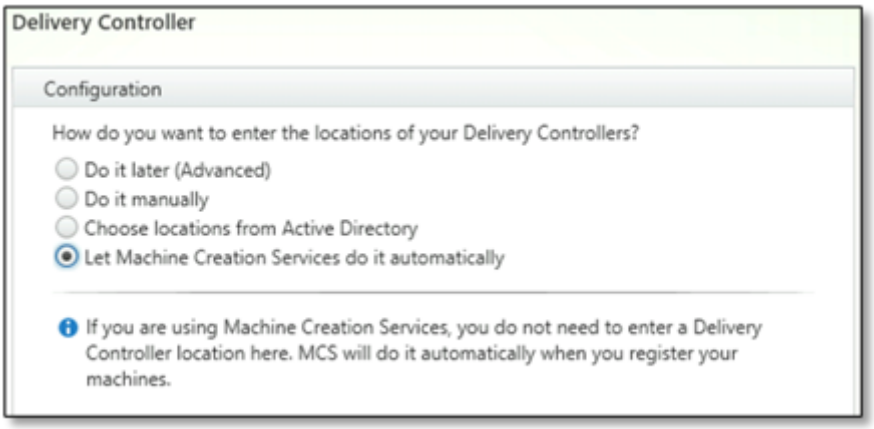
Siga as etapas para instalar o VDA:

1. Tenha o cuidado de selecionar as seguintes opções no assistente de instalação:

    - Na página Ambiente, selecione **Create a master MCS image**.



    - Na página Delivery Controller, selecione **Let Machine Creation Services do it automatically**.



2. Depois que o VDA for instalado, adicione o seguinte valor de registro:

   - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo de valor: DWORD
   - Nome do valor: GctRegistration
   - Dados de valor: 1

O que fazer a seguir

Quando a localização do recurso e a conexão de hospedagem estiverem disponíveis, continue com a criação do catálogo de máquinas. Para obter mais informações sobre a criação de catálogos de máquinas não ingressados no domínio, consulte Criar catálogos não ingressados no domínio.

Configurar locais de recursos

May 15, 2023

Os locais de recursos contém os recursos necessários para fornecer aplicativos e áreas de trabalho aos usuários. Você gerencia os recursos a partir do Citrix Cloud. Normalmente, os recursos incluem:

- Controlador de domínio do Active Directory.
- Hipervisores ou serviços de nuvem, conhecidos como *hosts*.
- Virtual Delivery Agents (VDAs). VDAs são as máquinas que contêm os aplicativos ou a área de trabalho. Cada máquina também tem um Citrix VDA instalado. O termo *VDA* geralmente se refere ao software VDA e à máquina na qual ele está instalado.
- Citrix Gateway (opcional): para permitir o acesso externo seguro aos aplicativos e áreas de trabalho oferecidos aos usuários, adicione um dispositivo Citrix Gateway VPX ao local do recurso. Em seguida, configure o Citrix Gateway.

- Servidores Citrix StoreFront (gerenciados pelo cliente).
- Para se comunicar com o Citrix Cloud, cada local de recursos deve conter um Citrix Cloud Connector. Recomenda-se um mínimo de dois conectores de nuvem por local de recursos, para disponibilidade.

Um local de recursos é considerado uma zona em um ambiente Citrix DaaS. Para obter mais informações, consulte Zonas.

Para saber mais sobre os tipos de recursos, consulte Conectar-se ao Citrix Cloud.

Requisitos do host

O hipervisor ou serviço de nuvem em que você provisiona VMs que fornecem aplicativos ou áreas de trabalho aos usuários pode ter permissões exclusivas ou requisitos de configuração.

- Se o hipervisor ou serviço de nuvem exigir redes virtuais ou outros itens, siga as orientações em sua documentação.
- Crie a nuvem privada virtual (VPC) apropriada ou as redes virtuais para as máquinas que você adicionará ao seu local de recursos, se necessário. Por exemplo, ao usar a AWS, configure uma VPC com sub-redes públicas e privadas.
- Crie as regras apropriadas para proteger o tráfego de entrada e saída da Internet e o tráfego entre máquinas na rede virtual. Por exemplo, ao usar a AWS, é necessário que o security group da VPC tenha as regras apropriadas configuradas para que as máquinas na VPC sejam acessíveis somente para os endereços IP especificados.

Os seguintes tipos de host são suportados:

- Ambientes de virtualização da Amazon Web Services (AWS)
- Ambientes de virtualização do Citrix Hypervisor
- Ambientes de virtualização do Google Cloud Platform
- Ambientes de virtualização do Microsoft Azure Resource Manager
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager
- Ambientes de virtualização da Nutanix
- Soluções de nuvem e parceiros da Nutanix
- Ambientes de virtualização do VMware
- Soluções de nuvem e parceiros da VMware

Active Directory

Provisione um servidor Windows, instale os Serviços de Domínio Active Directory e promova-o a um controlador de domínio. Para obter orientação, consulte a documentação do Microsoft Active Directory.

- Você deve ter pelo menos um controlador de domínio executando o Active Directory Domain Services.
- Não instale nenhum componente Citrix em um controlador de domínio.
- Não use uma barra (/) ao especificar nomes de unidades organizacionais na interface de gerenciamento Full Configuration.

Para obter mais informações, consulte:

- Níveis funcionais do Active Directory
- Gerenciamento de identidade e acesso no Citrix Cloud.

Conectores de nuvem

O Cloud Connector é um grupo de serviços do Citrix Cloud que permite a comunicação entre os VDAs, o StoreFront gerenciado pelo cliente e o Delivery Controller baseado em nuvem. Você pode instalar Cloud Connectors interativamente ou a partir da linha de comando.

Para obter informações completas sobre o Cloud Connector, consulte:

- Citrix Cloud Connector
- Detalhes técnicos, que incluem requisitos do sistema
- Configuração de proxy e firewall
- Instalação
- Atualizações do conector

Considerações sobre tamanho e escala

Ao avaliar o Citrix DaaS quanto a dimensionamento e escalabilidade, leve em consideração todos os componentes. Pesquise e teste a configuração dos Cloud Connectors e do StoreFront gerenciado pelo cliente para seus requisitos específicos. O subdimensionamento das máquinas pode afetar negativamente o desempenho do sistema.

O artigo a seguir contém informações de teste de tamanho e escala. Este artigo fornece detalhes das capacidades máximas testadas, além de recomendações de práticas recomendadas para a configuração da máquina do Cloud Connector.

- Considerações de tamanho e escala de Cloud Connectors

Adicionar um tipo de recurso ou ativar um domínio não usado no Citrix Cloud

Adicionar um tipo de recurso:

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Resource Locations**.
3. Selecione **+ Resource Locations** para adicionar um novo local de recursos.
4. Insira um nome para o novo local de recursos e clique em **Save**. Para obter informações sobre considerações de nomenclatura, consulte Restrições de nomes.
5. Na nova localização do recurso, selecione **Cloud Connectors**.
6. Baixe e instale o software Cloud Connector em pelo menos dois servidores no domínio em que residem seus recursos do Citrix DaaS.
   - Durante a instalação, selecione o local de recursos que você criou nas etapas 3 e 4.
   - Após a instalação, o Citrix Cloud adiciona os servidores ao local de recursos e registra os domínios nos quais você instalou os Cloud Connectors.
7. Verifique se os domínios registrados estão ativos:
   - No menu Citrix Cloud, selecione **Identity Access Management**.
   - Selecione **Domains**. Uma lista de domínios em que 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 descrito na Etapa 7, o domínio está em um estado "não usado". Se você especificar um domínio não usado 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 usado"neste artigo.

Para obter mais informações, consulte CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error"when creating adding new machine accounts.

Ativar um domínio não usado:

1. Na guia **Domain**, em **Identity and Access Management**, selecione **Show Unused Domains**. Depois de selecionar essa opção, o rótulo muda para **Hide Unused Domains**.
2. Localize o domínio não usado na lista. Os domínios não usados exibem uma barra cinza no lado esquerdo da entrada do domínio e no menu de reticências de opção única no lado direito.
3. Selecione o menu de reticências e selecione **Use domain**. A barra cinza fica verde e o menu de reticências muda para **Disable**.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para configurar o local de recursos para tipos específicos de host:
  - Ambientes de nuvem AWS
  - Ambientes de virtualização do Citrix Hypervisor
  - Ambientes do Google Cloud
  - Ambientes de nuvem do Microsoft Azure Resource Manager
  - Ambientes de virtualização do Microsoft System Center Virtual Machine Manager
  - Ambientes de virtualização da Nutanix
  - Soluções de nuvem e parceiros da Nutanix
  - Ambientes de virtualização do VMware
  - Soluções de nuvem e parceiros da VMware
- Para uma implantação completa, crie uma conexão a um local de recursos.
- Revise todas as etapas do processo de instalação e configuração

Ambientes de nuvem AWS

January 17, 2023

Este artigo o orienta na configuração de sua conta da Amazon Web Services (AWS) como um local de recursos que você pode usar com o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops). O local de recursos inclui um conjunto básico de componentes, ideal para uma prova de conceito ou outra implantação que não exija recursos distribuídos por várias zonas de disponibilidade. Depois de concluir essas tarefas, você pode instalar VDAs, provisionar máquinas, criar catálogos de máquinas e criar grupos de entrega.

Quando concluir as tarefas deste artigo, o local de recursos incluirá os seguintes componentes:

- Uma nuvem privada virtual (VPC) com sub-redes públicas e privadas dentro de uma única zona de disponibilidade.
- Uma instância que é executada como um controlador de domínio do Active Directory e um servidor DNS, localizada na sub-rede privada da VPC.
- Duas instâncias ingressadas no 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. Essa instância é usada para iniciar conexões RDP com as instâncias na sub-rede privada para fins

administrativos. Depois de concluir a configuração do local de recursos, você pode encerrar a instância para que ela não fique mais prontamente acessível. Quando for necessário gerenciar outras instâncias na sub-rede privada, como as instâncias do VDA, você pode reiniciar a instância do host bastion.

Visão geral da tarefa

Configure uma nuvem privada virtual (VPC) com sub-redes pública e privada. Quando você concluir essa tarefa, a AWS implanta gateways NAT com um endereço Elastic IP na sub-rede pública. Isso permite que 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.

Configure 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 associará esses grupos de segurança a cada instância na sua VPC.

Crie um conjunto de opções de DHCP. Com uma Amazon VPC, os serviços DHCP e DNS são fornecidos por padrão, o que afeta a forma como você configura o DNS no 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 os servidores de domínio e nome entregues às instâncias por meio do 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 na sua VPC. Para garantir que os registros Host (A) e de Pesquisa inversa (PTR) sejam registrados automaticamente quando as instâncias ingressarem no domínio, configure as propriedades do adaptador de rede para cada instância adicionada à sub-rede privada.

Adicione um host bastion, um controlador de domínio e Citrix Cloud Connectors à VPC. Por meio do host bastion, você pode fazer logon em instâncias na sub-rede privada para configurar o domínio, associar instâncias ao domínio e instalar o Citrix Cloud Connector.

Tarefa 1: Configurar a VPC

1. No console de gerenciamento da AWS, selecione **VPC**.
2. No VPC Dashboard, selecione **Create VPC**.
3. Selecione **VPC and more**.
4. Em NAT gateways ($) selecione **In 1 AZ** ou **1 per AZ**.
5. Para a instância NAT, especifique o tipo de instância e o par de chaves que você deseja usar. O par de chaves permite que você se conecte com segurança à instância posteriormente.
6. Nas opções de DNS, deixe **Enable DNS hostnames** selecionada.

7. Selecione **Create VPC**. A AWS cria as sub-redes pública e privada, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

> **Nota:**
>
> Alterar o nome de uma AWS Virtual Private Cloud (VPC) no console da AWS quebra a unidade de hospedagem existente no Citrix Cloud. Quando a unidade de hospedagem quebra, você não pode criar catálogos ou adicionar máquinas a catálogos existentes. Do problema conhecido: PMCS-7701

Tarefa 2: Configurar grupos de segurança

Essa tarefa cria e configura os seguintes grupos de segurança para a sua VPC:

- Um grupo de segurança público, com o qual as instâncias em sua sub-rede pública serão associadas.
- Um grupo de segurança privado, com o qual as instâncias em sua sub-rede privada serão associadas.

Para criar os grupos de segurança

1. No VPC Dashboard, selecione **Security Groups**.
2. Crie um grupo de segurança para o grupo de segurança pública. Selecione **Create Security Group** e insira uma marca de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Yes, Create**.

Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Inbound Rules** e selecione Edit para criar as seguintes regras:

Tipo	Origem
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	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
443 (HTTPS)	0.0.0.0/0

Tipo	Origem
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Quando tiver terminado, selecione **Save**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Destino
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Quando tiver terminado, selecione **Save**.

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, será necessário definir portas TCP para incluir; selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Origem
ALL Traffic	Selecione o grupo de segurança NAT.
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	Selecione o grupo de segurança público.
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.

Tipo	Origem
TCP 389	Selecione o grupo de segurança público.
UDP 389	Selecione o grupo de segurança público.
443 (HTTPS)	Selecione o grupo de segurança público.
TCP 1494 (ICA/HDX)	Selecione o grupo de segurança público.
TCP 2598 (Session Reliability)	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 tiver terminado, selecione **Save.**
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Destino
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Quando tiver terminado, selecione **Save**.

Tarefa 3: Executar instâncias

As etapas a seguir criam quatro instâncias do EC2 e descriptografam a senha de administrador padrão gerada pela Amazon.

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No EC2 Dashboard, selecione **Launch Instance**.
3. Selecione uma imagem de máquina do Windows Server e um tipo de instância.
4. Na página Configure Instance Details, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Subnet**, faça as seguintes seleções para cada instância:
    - Bastion host: selecione a sub-rede pública.

- Domain controller and Connectors: selecione a sub-rede privada.

6. Em **Auto-assign Public IP address**, faça as seguintes seleções para cada instância:
   - Bastion host: selecione **Enable.**
   - Domain controller and Connectors: selecione **Use default setting** ou **Disable**.
7. Em **Network Interfaces**, insira um endereço IP primário dentro do intervalo de IP da sub-rede privada para o controlador de domínio e as instâncias do Cloud Connector.
8. Na página Add Storage, modifique o tamanho do disco, se necessário.
9. Na página Tag Instance, insira um nome amigável para cada instância.
10. Na página Configure Security Groups, selecione **Select an existing security group** e faça as seguintes seleções para cada instância:
    - Bastion host: selecione o grupo de segurança público.
    - Domain controller and Cloud Connectors: selecione o grupo de segurança privado.
11. Revise suas escolhas e selecione **Launch**.
12. Crie um novo par de chaves ou selecione um par existente. Se você criar um novo par de chaves, baixe seu arquivo de chave privada (.pem) e mantenha-o em local seguro. Você deve fornecer sua chave privada ao adquirir a senha de administrador padrão para a instância.
13. Selecione **Launch Instances**. Selecione **View Instances** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-executada 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 **Connect**.
    b) Selecione **Get Password** e forneça o seu arquivo de chave privada (.pem) quando solicitado.
    c) Selecione **Decrypt Password**. A AWS exibe a senha padrão.
15. Repita as etapas de 2 a 14 até criar quatro instâncias: uma instância de host bastion na sub-rede pública e três instâncias na sub-rede privada para uso como o controlador de domínio e dois Cloud Connectors.

Tarefa 4: Criar um conjunto de opções de DHCP

1. No VPC Dashboard, selecione **DHCP Options Sets**.
2. Insira as seguintes informações:
   - Name tag: insira um nome amigável para o conjunto.

- Domain name: insira o nome de domínio totalmente qualificado que você usa ao configurar a instância do controlador de domínio.
- Domain name servers: insira o endereço IP privado que você atribuiu à instância do controlador de domínio e a cadeia de caracteres **AmazonProvidedDNS**, separados por vírgula.
- NTP servers: deixe este campo em branco.
- NetBIOS name servers: insira o endereço IP privado da instância do controlador de domínio.
- NetBIOS node type: insira **2**.

3. Selecione **Yes, Create.**
4. Associe o novo conjunto à sua VPC:
   a) No VPC Dashboard, selecione **Your VPCs** e, em seguida, selecione a VPC que você configurou anteriormente.
   b) Selecione **Actions > Edit DHCP Options Set**.
   c) Quando solicitado, selecione o novo conjunto que você criou e, em seguida, selecione **Save**.

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 para a conta de administrador.
2. Na instância do host bastion, inicie a Conexão de Área de Trabalho Remota e conecte-se ao endereço IP privado da instância que deseja configurar. Quando solicitado, insira as credenciais de administrador para a instância.
3. Para todas as instâncias na sub-rede privada, defina as configurações de DNS:
   a) Selecione **Iniciar > Painel de controle > Rede e Internet > Central de Rede e Compartilhamento > Alterar as 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 ativadas e selecione **OK**:
      - Registrar os endereços desta conexão no DNS
      - Usar o sufixo DNS desta conexão no registro do DNS
4. Para configurar o controlador de domínio:
   a) Usando o Server Manager, adicione a função Active Directory Domain Services 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 especificado ao criar o conjunto de opções de DHCP. Reinicie a instância quando solicitado.

5. Para configurar o primeiro Cloud Connector:

   a) Associe a instância ao domínio e reinicie quando solicitado. Na instância do host bastion, reconecte-se à instância usando o RDP.
   b) Faça login no Citrix Cloud. Selecione **Resource Locations** no menu superior esquerdo.
   c) Baixe o Cloud Connector.
   d) Quando solicitado, execute o arquivo `cwcconnector.exe` e forneça as suas credenciais do Citrix Cloud. Siga o assistente.
   e) Quando terminar, selecione**Atualizar** para exibir a página de locais de recursos. Quando o Cloud Connector é registrado, a instância aparece na página.

6. Repita a Etapa 5 para configurar o segundo Cloud Connector.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com a AWS.
- Revise todas as etapas do processo de instalação e configuração

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do Citrix Hypervisor

December 21, 2022

O Citrix Hypervisor simplifica seu gerenciamento operacional, garantindo uma experiência de usuário de alta definição para cargas de trabalho intensivas.

Para configurar o seu Citrix Hypervisor, consulte Configurar tipo de recurso.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o Citrix Hypervisor.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes do Google Cloud

May 2, 2023

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) permite provisionar e gerenciar máquinas no Google Cloud.

Requisitos

- Conta do Citrix Cloud. O recurso descrito neste artigo está disponível somente no Citrix Cloud.
- Assinatura do Citrix DaaS. Para obter detalhes, consulte Introdução.
- Um projeto do Google Cloud. O projeto armazena todos os recursos de computação associados ao catálogo de máquinas. Pode ser um projeto existente ou um projeto novo.
- Habilite quatro APIs no seu projeto do Google Cloud. Para obter detalhes, consulte Habilitar as APIs do Google Cloud.
- Conta de serviço do Google Cloud. A conta de serviço é autenticada no Google Cloud para permitir o acesso ao projeto. Para obter detalhes, consulte Configurar e atualizar contas de serviço.
- Ative o acesso privado do Google. Para obter detalhes, consulte Ativar o acesso privado do Google.

Habilitar as APIs do Google Cloud

Para usar a funcionalidade do Google Cloud por meio da interface Full Configuration do Citrix Virtual Apps and Desktops, ative estas APIs no seu projeto do Google Cloud:

- API do Compute Engine

- API do Cloud Resource Manager
- API do Identity and Access Management (IAM)
- API do Cloud Build

No console do Google Cloud, conclua estas etapas:

1. No menu superior esquerdo, selecione **APIs and Services > Dashboard**.
2. Na tela **Dashboard**, confirme que a API de Compute Engine está ativada. Caso contrário, siga estes passos:
   a) Navegue 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) Navegue 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 **Identity and Access Management (IAM) API** e **Cloud Build API**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para 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 services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com
3. Clique em **Authorize** se o Cloud Shell solicitar.

Configurar e atualizar contas de serviço

O Citrix Cloud usa três contas de serviço separadas no projeto do Google Cloud:

- *Conta de serviço do Citrix Cloud*: essa conta de serviço permite que o Citrix Cloud acesse o projeto do Google, provisione e gerencie máquinas. A conta do Google Cloud é autenticada no Citrix Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar essa conta de serviço manualmente.

  Você pode identificar essa conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

  Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a essa conta de serviço:

  - Compute Admin
  - Storage Admin
  - Cloud Build Editor
  - Service Account User
  - Cloud Datastore User

- *Conta de serviço Cloud Build*: essa conta de serviço é provisionada automaticamente depois que você ativa todas as APIs mencionadas em Habilitar as APIs do Google Cloud.

  Você pode identificar essa conta de serviço pelo endereço de e-mail que começa com **ID do projeto** e a palavra **cloudbuild**. Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

  Conceda as seguintes funções a essa conta de serviço:

  - Cloud Build Service Account
  - Compute Instance Admin
  - Service Account User

- *Conta de serviço do Cloud Compute*: essa conta de serviço é adicionada pelo Google Cloud às instâncias criadas no Google Cloud quando a API do Compute é ativada. Essa 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 **Storage Admin** que exige as seguintes permissões:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Você pode identificar essa conta de serviço pelo endereço de e-mail que começa com **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, navegue para **IAM & Admin > Service accounts**.
2. Na página **Service accounts**, selecione **CREATE SERVICE ACCOUNT**.
3. Na página **Create service account**, insira as informações necessárias e selecione **CREATE AND CONTINUE**.
4. Na página **Grant this service account access to project**, clique no menu suspenso **Select a role** e selecione as funções necessárias. Clique em **+ADD ANOTHER ROLE** se quiser adicionar mais funções.

   > **Nota:**
   >
   > Ative todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUE**.
6. Na página **Grant users access to this service account**, adicione usuários ou grupos para conceder acesso para realizarem ações na conta de serviço.
7. Clique em **DONE**.
8. Navegue até o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Confirme que as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Grant this service account access to project** e **Grant users access to this service account** são opcionais. Se você optar por ignorar essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM & Admin > IAM**.
- Para exibir funções associadas a uma conta de serviço, adicione as funções sem ignorar as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

Chave da conta de serviço do Citrix Cloud Ao criar uma conta de serviço, existe a opção de criar uma chave para a conta. Você precisa dessa chave ao criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credencial (.json). O arquivo é baixado automaticamente e salvo 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, a interface Full Configuration do Citrix não pode analisá-la.

> **Dica:**
>
> Crie chaves usando a página **Service accounts** 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, navegue para **IAM & Admin > IAM**.
2. Na página **IAM > PERMISSIONS**, localize a conta de serviço que você criou, identificável pelo endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso à entidade de segurança da conta de serviço.
4. Na página **Edit access to "project-id"** da opção de entidade de segurança selecionada, selecione **ADD ANOTHER ROLE** para adicionar as funções necessárias à sua conta de serviço, uma por uma, e selecione **SAVE**.

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, navegue para **IAM & Admin > IAM**.
2. Na página do **IAM**, localize a conta de serviço do Cloud Build, identificável pelo endereço de e-mail que começa com **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 **Edit access to "project-id"** da opção de entidade de segurança selecionada, selecione **ADD ANOTHER ROLE** para adicionar as funções necessárias à sua conta de serviço Cloud Build, uma por uma, e selecione **SAVE**.

> **Nota:**
>
> Habilite todas as APIs para obter a lista completa de funções.

Gerenciamento do bucket e permissões de armazenamento

O Citrix DaaS melhora o processo de relatar falhas de compilação na nuvem do serviço Google Cloud. Esse serviço executa compilações no Google Cloud. O Citrix DaaS cria um intervalo de armazenamento chamado `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` onde os serviços do Google Cloud capturam informações de registro de compilação. Uma opção é definida nesse bucket que exclui o conteúdo após um período de 30 dias. Esse 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 ignorará os erros e prosseguirá com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de compilação aumenta e exigem limpeza manual.

Ativar o acesso privado do Google

Quando uma VM não tem um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Quando você ativa 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 ativado, 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 na sua sub-rede possa acessar as APIs do Google sem um endereço IP público para provisionamento do MCS:

1. No Google Cloud, acesse a **configuração da rede VPC**.
2. Na tela Subnet details, ative **Private Google access**.

Para obter mais informações, consulte Como configurar o acesso privado do Google.

> **Importante:**
>
> Se a sua rede está configurada para impedir o acesso da VM à Internet, certifique-se de que a sua organização assuma os riscos associados à ativação do acesso privado do Google para a sub-rede à qual a VM está conectada.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com ambientes de nuvem do Google.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do HPE Moonshot (prévia)

December 6, 2023

O Citrix DaaS gerencia suas cargas de trabalho do HPE Moonshot por meio de um plug-in HPE Moonshot gerenciado pela Citrix e presente no plano de controle do DaaS. Com esse plug-in, você pode criar conexões com seu chassi HPE Moonshot, criar catálogos e gerenciar a energia das máquinas no catálogo.

Requisito

Ative a opção de alternância do recurso **moonshotpluginenabled** em **DaaS > Home > Preview features**.

Etapas principais

1. Configurar seus ambientes HPE.
2. Criar uma conexão com o chassi HPE Moonshot.

   > **Nota:**
   >
   > Depois de ativar a opção de alternância do recurso, o plug-in HPE Moonshot gerenciado pela Citrix é instalado automaticamente. Portanto, você pode continuar usando o catálogo de máquinas existente usando o plug-in Moonshot gerenciado pela Citrix em vez do plug-in HPE Moonshot gerenciado pela HPE.

3. Criar 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. Criar um grupo de entrega.
5. Migre o restante dos nós não gerenciados do HPE Moonshot para o catálogo gerenciado ou grupo de entrega.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o HPE Moonshot.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões
- Criar catálogos de máquinas

Ambientes de nuvem do Microsoft Azure Resource Manager

December 21, 2022

Ao usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais na implantação do serviço Citrix Virtual Apps ou Citrix Virtual Desktops, familiarize-se com o seguinte:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Consent framework: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Service principal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Para configurar seu Microsoft Azure Resource Manager, consulte Configurar local de recursos.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o Microsoft Azure.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas
- CTX219211: Set up a Microsoft Azure Active Directory account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Ambientes de virtualização do Microsoft System Center Virtual Machine Manager

February 23, 2023

Siga estas instruções 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 suportadas do VMM.

Você pode usar Machine Creation Services ou Citrix Provisioning (anteriormente Provisioning Services) para provisionar:

- VMs de SO de servidor ou desktop de 1ª geração
- VMs Windows Server 2012 R2, Windows Server 2016 e Windows 10 de 2ª geração (com ou sem inicialização segura)

Instalar e configurar um hipervisor

Instale o servidor Microsoft Hyper-V e o VMM em seus servidores.

Verifique as seguintes informações da conta:

Em **Manage > Full Configuration**, a conta especificada ao criar uma conexão deve ser um administrador do VMM ou um administrador delegado do VMM para as máquinas Hyper-V relevantes. Se

essa conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados na interface **Full Configuration** 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 em que 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 hosts, use a função de administrador delegado no console do Microsoft System Center Virtual Machine Manager (VMM).

1. Em **Create User Roles Wizard**, selecione **Fabric Administrator** (administrador delegado) como uma função de usuário.
2. Em **Members**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Scope**, selecione os grupos de hosts aos quais deseja que o administrador delegado tenha acesso.
4. Crie uma nova **Run As Account** usando credenciais de usuário administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

Instale o console do VMM

Instale um console do System Center Virtual Machine Manager em cada servidor que tem 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 falhará se as versões forem diferentes.

Provisionamento do Azure Stack HCI por meio do SCVMM

Azure Stack HCI é uma solução de cluster de infraestrutura hiperconvergente (HCI) que hospeda cargas de trabalho virtualizadas do Windows e do Linux e o seu armazenamento em um ambiente híbrido local.

Os serviços híbridos do Azure aprimoram o cluster com recursos como monitoramento baseado em nuvem, recuperação de site e backups de VM. Você também pode ter uma visão centralizada de todas as suas implantações de do Azure Stack HCI no portal do Azure.

Integrar o Azure Stack HCI ao SCVMM

Para integrar o Azure Stack HCI ao SCVMM, você precisa primeiro criar um cluster do Azure Stack HCI e, em seguida, integrar esse cluster ao SCVMM.

1. Para criar o cluster do Azure Stack HCI, consulte o documento da Microsoft Conectar o Azure Stack HCI ao Azure.
2. Para integrar o cluster do Azure Stack HCI ao SCVMM, faça o seguinte:
   a) Faça login na máquina que está preparada para hospedar o servidor SCVMM e instale o SCVMM 2019 UR3 ou posterior.

   > **Nota:**
   >
   > Instale o console do administrador SCVMM 2019 UR3 ou posterior na máquina virtual do Cloud Connector.

   b) Na página **Settings** do console do VMM, crie uma conta Executar como.
   c) Execute os seguintes comandos do PowerShell com permissões administrativas no servidor SCVMM para adicionar o cluster do Azure Stack HCI como um host:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

   d) Agora você pode ver o cluster do Azure Stack HCI juntamente com os nós no console do VMM.
   e) Crie a conexão de hospedagem do SCVMM na interface **Full Configuration**.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o Microsoft System Center Virtual Machine Manager.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do Nutanix

December 21, 2022

Siga estas instruções quando usar o Nutanix Acropolis para fornecer máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops. O processo de configuração inclui a tarefa de instalar e registrar o plug-in Nutanix em seu ambiente do Citrix Virtual Apps and Desktops.

Para obter mais informações, consulte o Manual de instalação do plug-in Nutanix Acropolis MCS, disponível no Nutanix Support Portal.

> **Importante:**
>
> Instale o plug-in Nutanix em todos os Cloud Connectors em que o Citrix DaaS deve criar uma conexão de host com o local de recursos que tem um hipervisor Nutanix.

Instalar e registrar o plug-in Nutanix

Conclua o procedimento a seguir para instalar e registrar o plug-in Nutanix nos Cloud Connectors. Use as funções **Manage > Full Configuration** no Citrix Cloud para criar uma conexão com a Nutanix. Em seguida, crie um catálogo de máquinas que use um instantâneo da imagem mestre que você criou no ambiente Nutanix.

> **Dica:**
>
> Recomendamos que você pare e reinicie o Citrix Host Service, o Citrix Broker Service e o Machine Creation Services quando instalar ou atualizar o plug-in Nutanix.

Para obter informações sobre a instalação do plug-in Nutanix, consulte o site da documentação do Nutanix.

Para obter mais informações sobre como configurar seus ambientes de virtualização da Nutanix, consulte Configurar local de recursos.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.

- Para criar e gerenciar uma conexão, consulte Conexão com a Nutanix.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Soluções de nuvem e parceiros da Nutanix

April 14, 2023

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) oferece suporte à seguinte solução de nuvem e parceiros da Nutanix:

- Nutanix Cloud Clusters na AWS

Nutanix Cloud Clusters na AWS

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) é compatível com Nutanix Cloud Clusters na AWS. O Nutanix Clusters simplifica a forma como os aplicativos são executados em nuvens privadas ou em várias nuvens públicas. Para obter mais informações sobre o Nutanix Cloud Clusters na AWS, consulte Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Dica:**
>
> Esse suporte fornece a mesma funcionalidade de um cluster local da Nutanix. Somente um único cluster é suportado, o *Prism Element*. Para obter mais informações, veja aqui.

Requisitos

Você precisa do seguinte para usar os clusters Nutanix na AWS:

- Uma conta Nutanix.
- Uma conta da AWS com as seguintes permissões:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Criar um cluster Nutanix

Para criar um cluster Nutanix:

1. Faça login na sua conta Nutanix.
2. Localize a opção de **Nutanix cluster** e clique em **Launch**. O **Nutanix Console** é aberto. Para obter mais informações, consulte Get Started with Nutanix Cluster on AWS.
3. Escolha criar uma **new VPC**.

O processo de criação do cluster pode falhar com os seguintes erros:

- Falha ao criar o cluster dentro de um determinado período. Exclusão do cluster.
- Host Nutanix Cluster - Nó `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Nó `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

Se o cluster não tiver sido criado:

- Tente recriar um cluster em uma região diferente.
- Tenha o cuidado de excluir o Nutanix CloudFormation Stack (CFS) antes de tentar novamente.

Além de outros recursos, o Nutanix CFS cria:

- 1 VPC chamada *Nutanix Cluster xxxxxxxxxxxxx* 10.0.0.0/16
- 2 sub-redes 10.0.128.0/24 e 10.0.129.0/24
- 1 gateway de Internet
- 1 gateway NAT

Depois que o cluster for criado, recupere o endereço do **Nutanix Prism**:

1. Vá para o **Nutanix Console**.
2. No canto superior direito do console, passe o mouse sobre o link **Launch Prism Element** e copie o URL.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com soluções de nuvem e parceiros da Nutanix.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do VMware

December 21, 2022

Siga estas instruções se você usa VMware para fornecer máquinas virtuais.

Instale o vCenter Server e as ferramentas de gerenciamento apropriadas. (Não há suporte para a operação Linked Mode do vSphere vCenter.)

Se você planeja usar o Machine Creation Services (MCS), não desative o recurso Datastore Browser no vCenter Server (descrito neste artigo do VMware). Quando você desativa esse recurso, o MCS não funciona corretamente.

Para configurar seus ambientes de virtualização do VMware, consulte Configurar tipo de recurso.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o VMware.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas
- Solução VMware do Azure

Soluções de nuvem e parceiros da VMware

November 9, 2023

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) oferece suporte às seguintes soluções de nuvem e parceiros da VMware:

- Solução VMware no Azure (AVS)
- Google Cloud VMware Engine
- Nuvem VMware na 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 serviço Citrix Virtual Apps and Desktop oferece suporte ao AVS. O AVS fornece infraestrutura de nuvem contendo clusters do vSphere criados pela infraestrutura do Azure. Aproveite o Citrix Virtual Apps and Desktop Service para usar o AVS para provisionar sua carga de trabalho do VDA da mesma forma que você usaria o vSphere em ambientes locais.

Configuração do cluster AVS

Para permitir que o Citrix Virtual Apps and Desktop Service use o AVS, execute as seguintes etapas no Azure:

- Solicite uma cota de host
- Registre o provedor de recursos Microsoft.AVS
- Lista de verificação de rede
- Crie uma nuvem privada do Azure VMware Solution
- Acesse uma nuvem privada do Azure VMware Solution
- Configure a rede para sua nuvem privada VMware no Azure
- Configure o DHCP para a solução VMware do Azure
- Adicione um segmento de rede no Azure VMware Solution
- Verifique o ambiente do Azure VMware Solution

Solicitar cota de host para clientes do Azure Enterprise Agreement Na página **Help + Support** do portal do Azure, selecione **New support request** e inclua as seguintes informações:

- Issue type:Technical
- Subscription:Select your subscription
- Service:All services > Azure VMware Solution
- Resource:General question
- Summary:Need capacity
- Problem type:Capacity Management Issues
- Problem subtype:Customer Request for Additional Host Quota/Capacity

Na **Description** do ticket de suporte, inclua as seguintes informações na guia **Details** :

- POC or Production
- Region Name
- Number of hosts
- Any other details

> **Nota:**
>
> O AVS requer um mínimo de três hosts e recomenda que você use redundância de hosts N+1.

Depois de especificar os detalhes do ticket de suporte, selecione **Review + Create** para enviar a solicitação ao Azure.

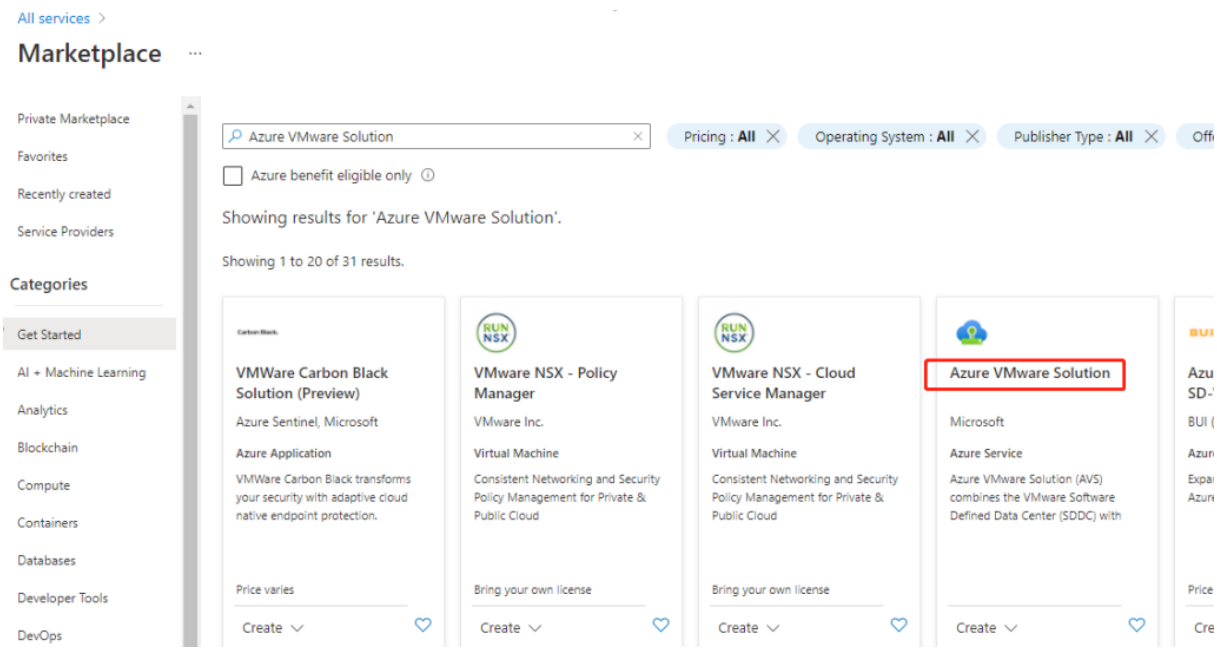
Registre o provedor de recursos Microsoft.AVS Depois de solicitar a cota do host, registre o provedor de recursos:

1. Faça login no portal do Azure.
2. No menu do portal do Azure, selecione **All services**.
3. No menu **All services**, insira a assinatura e selecione **Subscriptions**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Resource providers** e insira **Microsoft.AVS** na barra de pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

Considerações sobre rede O AVS oferece serviços de rede que exigem intervalos de endereços de rede e portas de firewall específicos. Consulte Lista de verificação de planejamento de rede da Solução VMware no Azure para obter mais informações.

Crie uma nuvem privada do Azure VMware Solution Depois de considerar os requisitos de rede para o seu ambiente, crie uma nuvem privada ASV:

1. Faça login no portal do Azure.
2. Selecione **Create a new resource**.
3. Na caixa de texto **Search the Marketplace**, digite *Azure VMware Solution* e selecione **Azure VMware Solution** na lista.



imagem

Na janela **Solução VMware do Azure**:

1. Selecione **Create**.
2. Click the **Basics** tab.
3. Insira valores para os campos, usando as informações da tabela abaixo:

Campo	Valor
Subscription	Selecione a assinatura que você planeja usar para a implantação. Todos os recursos em uma assinatura do Azure são cobrados juntos.
Resource group	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. Como alternativa, você pode criar um novo grupo de recursos para sua nuvem privada.
Localização	Selecione um local, como east us. Essa é a região que você definiu durante a fase de planejamento.
Nome do recurso	Forneça o nome da nuvem privada do Azure VMware Solution.
SKU	Selecione AV36.

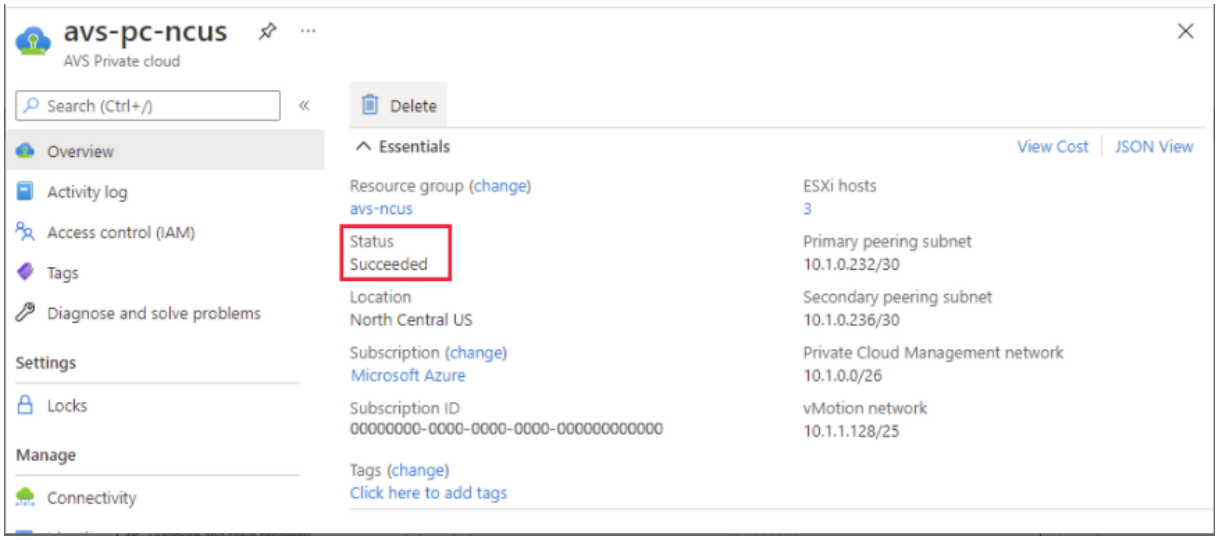
Campo	Valor
Hosts	Mostra o número de hosts alocados para o cluster de nuvem privada. O valor padrão é 3, que pode ser aumentado ou diminuído após a implantação.
Bloco de endereço	Forneça um bloco de endereço IP para a nuvem privada. O CIDR representa a rede de gerenciamento de nuvem privada e será usado para os serviços de gerenciamento de cluster, como o vCenter Server e o NSX-T Manager. Use o espaço de endereçamento /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure, nem a redes locais.
Rede virtual	Deixe isso em branco porque o circuito do Azure VMware Solution ExpressRoute é estabelecido como uma etapa pós-implantação.

Na tela **Create a private cloud** :

1. No campo **Location**, selecione a região que tem o AVS; a região do grupo de recursos é a mesma que a região AVS.
2. No campo **SKU**, selecione **AV36 Node**.
3. Especifique um endereço IP no campo **Address Block**. Por exemplo, 10.15.0.0/22.
4. Selecione **Review + Create**.
5. Depois de analisar as informações, clique em **Create**.

> **Dica:**
>
> A criação de uma nuvem privada pode levar de 3 a 4 horas. A adição de um único host ao cluster pode levar de 30 a 45 minutos.

Verifique se a implantação foi bem-sucedida. Navegue até o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Succeeded**, a implantação estará concluída.



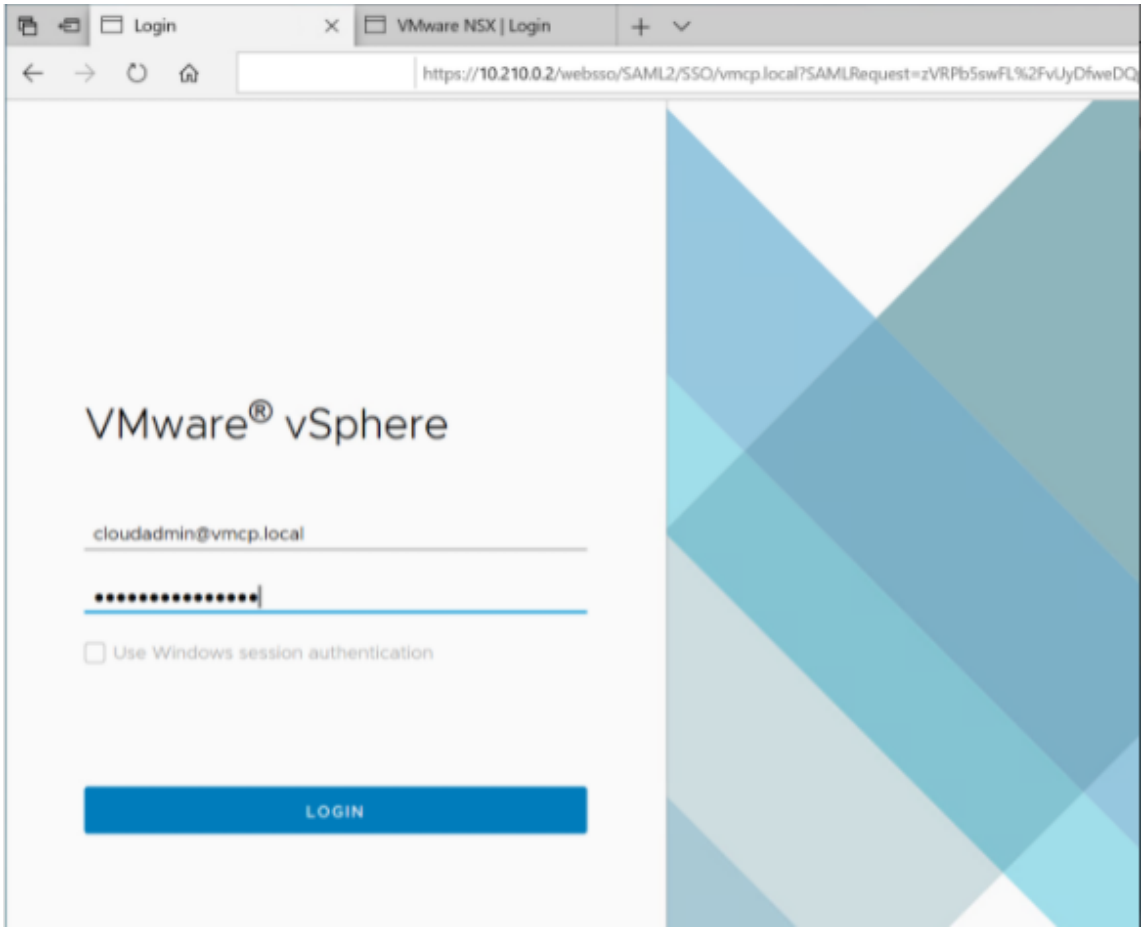
Acesse uma nuvem privada do Azure VMware Solution Depois de criar uma nuvem privada, crie uma VM do Windows e conecte-se ao vCenter local da sua nuvem privada.

Crie uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar** e, em seguida, pesquise e selecione **Microsoft Windows 10/2016/2019**.
2. Clique em **Create**.
3. Insira as informações necessárias e selecione **Review + Create**.
4. Depois que a validação for aprovada, selecione **Create** para iniciar o processo de criação da máquina virtual.

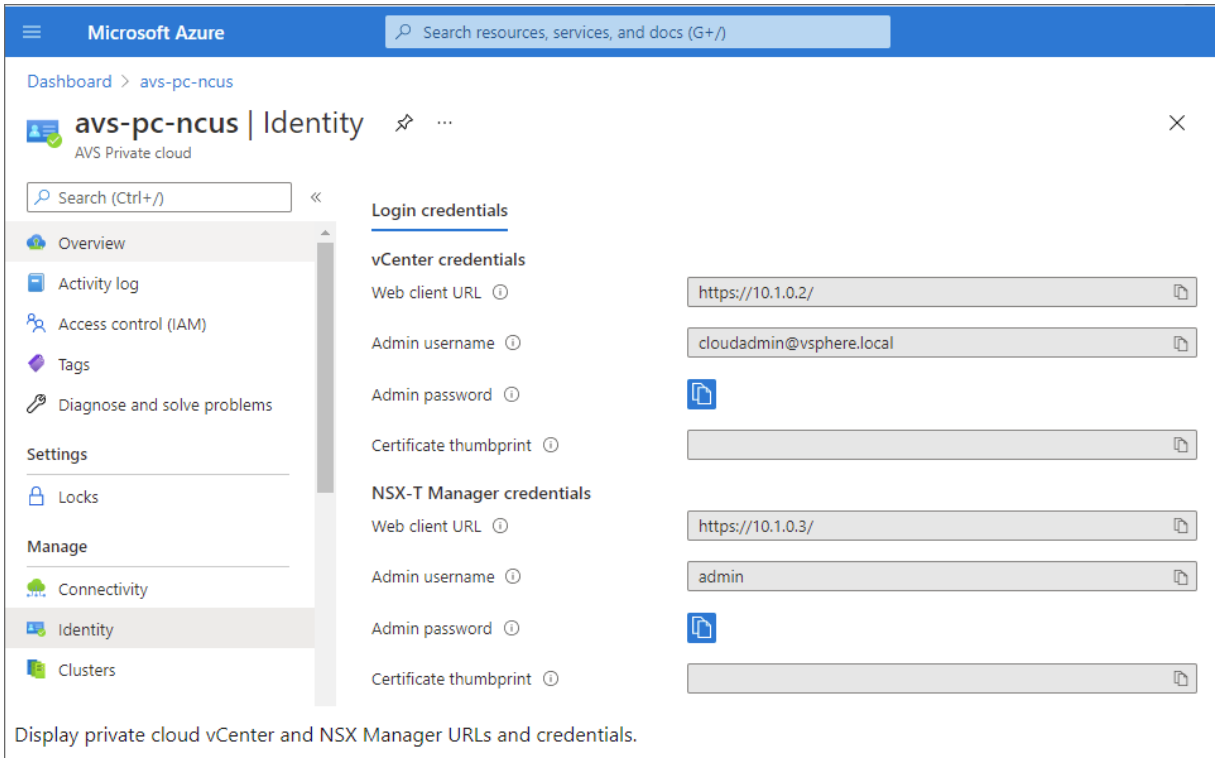
Conecte-se ao vCenter local da sua nuvem privada

1. Faça login em **vSphere Client with VMware vCenter SSO** como administrador de nuvem.



2. No portal do Azure, selecione sua nuvem privada e, em seguida, **Manage> Identity**.

Os URLs e credenciais de usuário para o vCenter de nuvem privada e o NSX-T Manager são exibidos:



Depois de confirmar URLs e credenciais do usuário:

1. Navegue até a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegue até os URLs do vCenter e do NSX-T Manager em duas guias do navegador. Na guia vCenter, insira as credenciais de usuário *cloudadmin@vmcp.local* da etapa anterior.

Configure a rede para sua nuvem privada VMware no Azure Depois de acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.

Crie uma rede virtual

1. Faça login no portal do Azure.
2. Navegue até o grupo de recursos criado anteriormente.
3. Selecione **+ Add** para definir um novo recurso.
4. Na caixa de texto **Search the Marketplace**, digite *virtual network*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Virtual Network**, selecione **Create** para configurar a rede virtual para sua nuvem privada.
6. Na página **Create Virtual Network**, insira os detalhes da sua rede virtual.
7. Na guia **Basics**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Next : IP Addresses.**

8. Na guia **IP Addresses**, no espaço de endereço IPv4, insira o endereço criado anteriormente.

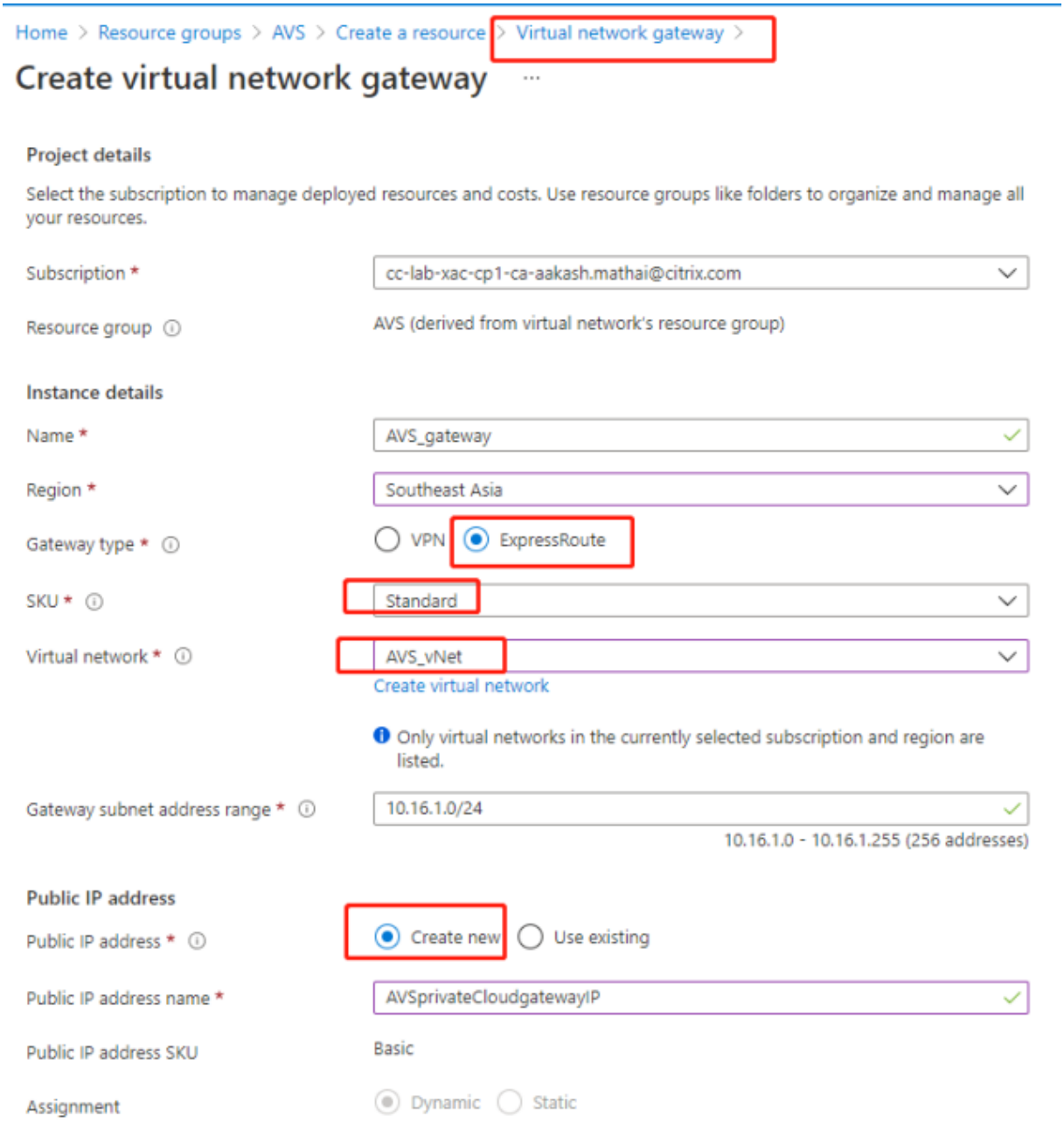
> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço usado ao criar sua nuvem privada.

Depois de entrar no espaço de endereço:

1. Selecione **+ Add subnet**.
2. Na página **Add subnet**, dê à sub-rede um nome e um intervalo de endereços apropriado.
3. Clique em **Add.**
4. Selecione **Review + create**.
5. Verifique as informações e clique em **Create**. Quando a implantação estiver concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual Depois de criar uma rede virtual, crie um gateway de rede virtual.

1. No grupo de recursos, selecione **+ Add** para adicionar um novo recurso.
2. Na caixa de texto **Search the Marketplace**, digite *virtual network gateway*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Virtual Network gateway**, clique em **Create**.
4. Na guia **Basics** da página **Create virtual network gateway**, forneça valores para os campos.
5. Clique em **Review + create**.



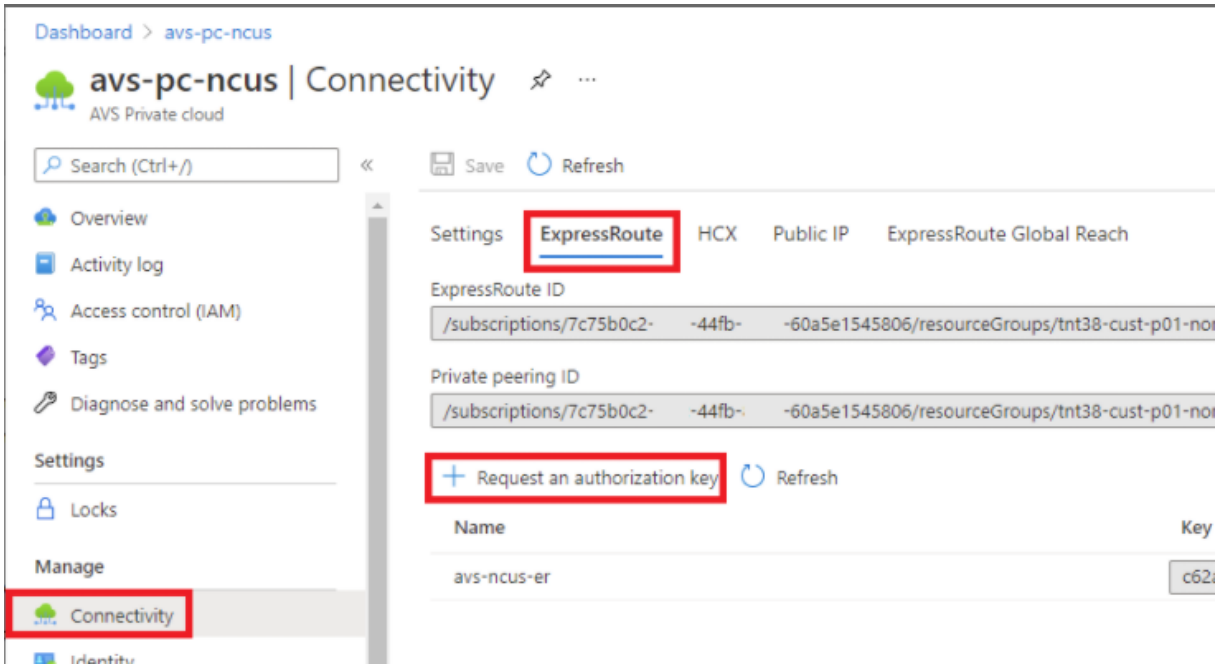
Depois de analisar a configuração do gateway de rede virtual, clique em **Create** para implantar o gateway de rede virtual.

Após a conclusão da implantação, conecte sua conexão do **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada do Azure AVS.

Conectar o ExpressRoute ao gateway de rede virtual Depois de implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada do Azure AVS:

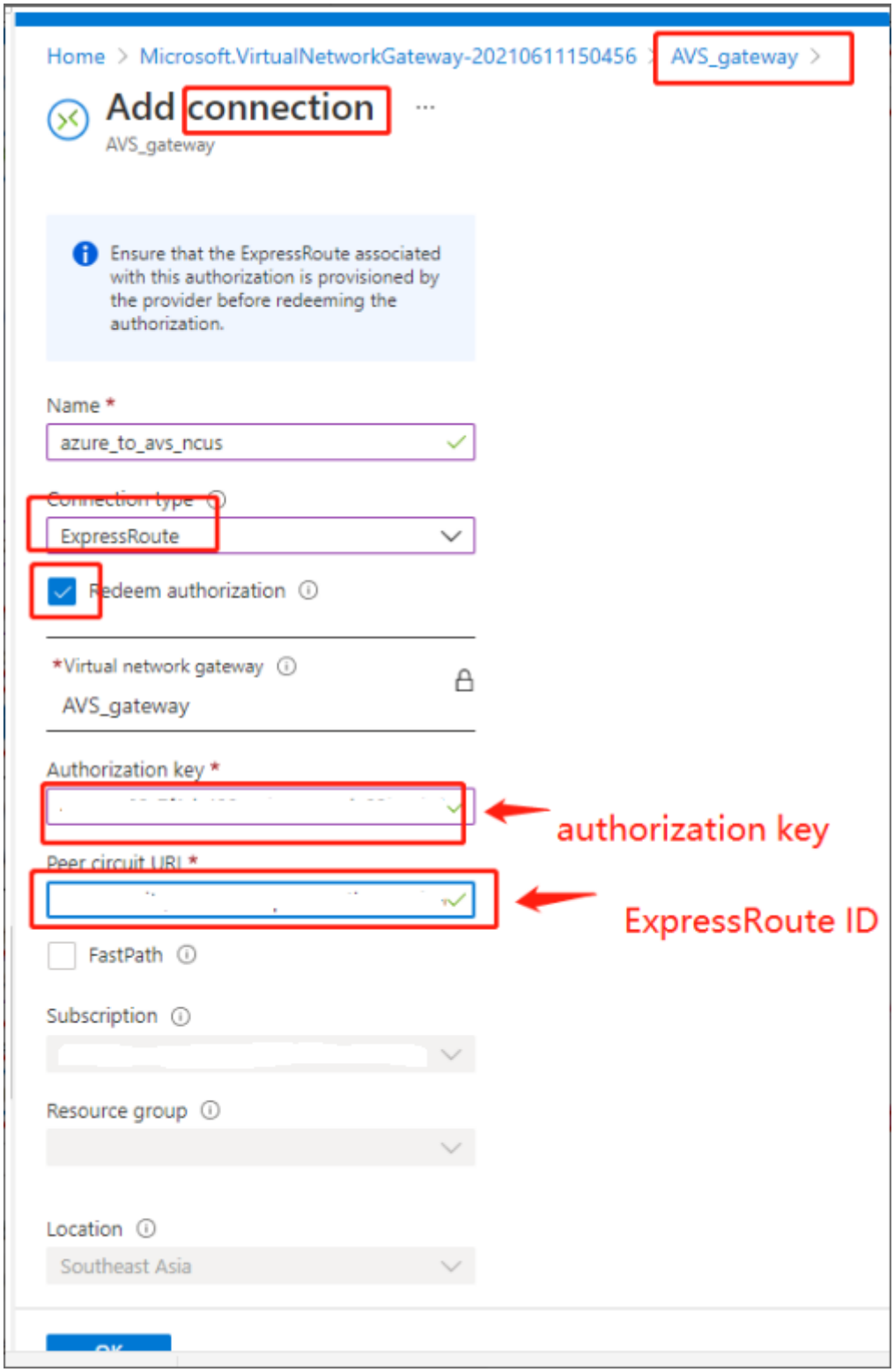
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegue até a **nuvem privada do Azure VMware Solution**. Selecione **Manage> Connectivity > ExpressRoute** e, em seguida, selecione **+ Request an authorization key.**

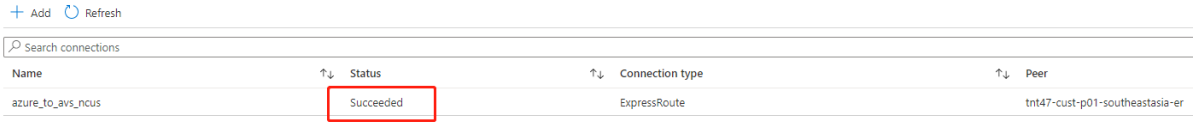


Depois de solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Create**. Pode levar cerca de 30 segundos para criar a chave. Depois de 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 peering. A chave de autorização desaparece após algum tempo, então copie-a assim que ela aparecer.
3. Navegue até o **gateway de rede virtual** que você planeja usar e selecione **Connections> + Add**.
4. Na página **Add connection**, forneça valores para os campos e selecione **OK.**



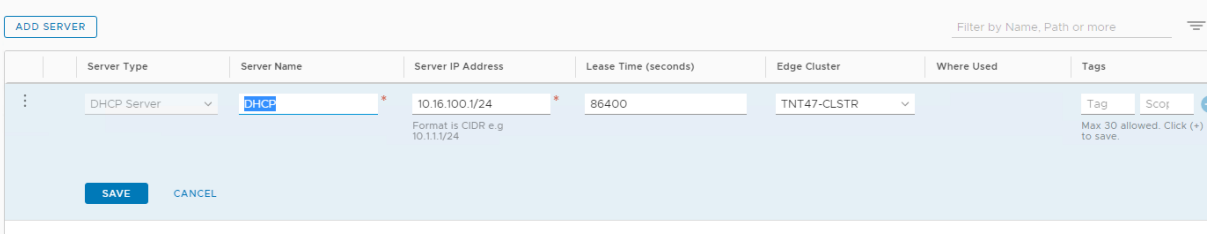
A conexão é estabelecida entre o circuito do ExpressRoute e sua rede virtual:



Configure o DHCP para a solução VMware do Azure Depois de conectar o ExpressRoute ao gateway virtual, configure o DHCP.

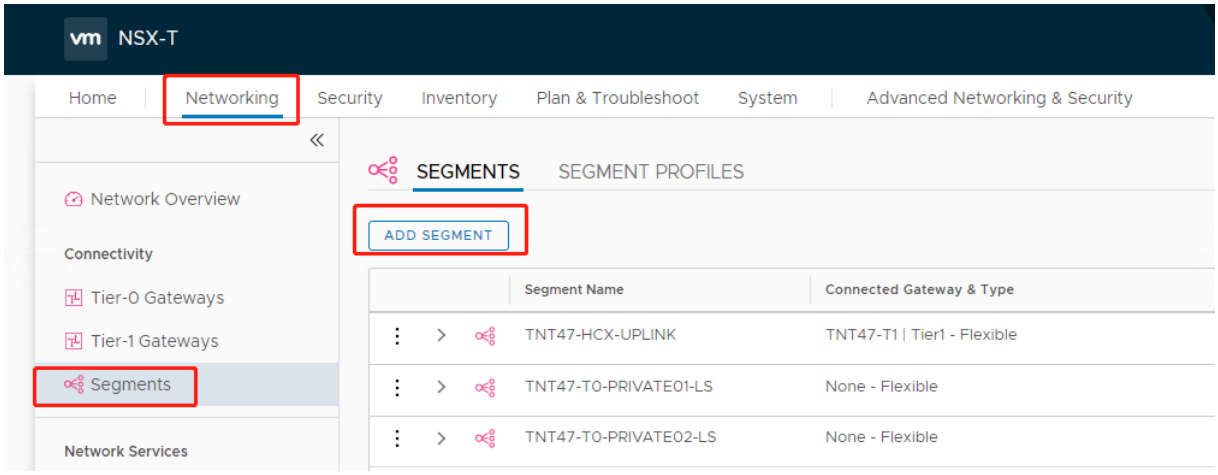
Usar o NSX-T para hospedar seu servidor DHCP No NSX-T Manager:

1. Selecione **Networking> DHCP** e, em seguida, selecione **Add Server**.
2. Selecione **DHCP** para o **Server Type**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Tier 1 Gateways**, selecione as reticências verticais no gateway de camada 1 e, em seguida, selecione **Edit**.
5. Selecione **No IP Allocation Set** para adicionar uma sub-rede.
6. Selecione **DHCP Local Server** para o **Type**.
7. Para o **DHCP Server**, selecione **Default DHCP** e clique em **Save**.
8. Clique em **Save** novamente e selecione **Close Editing**.



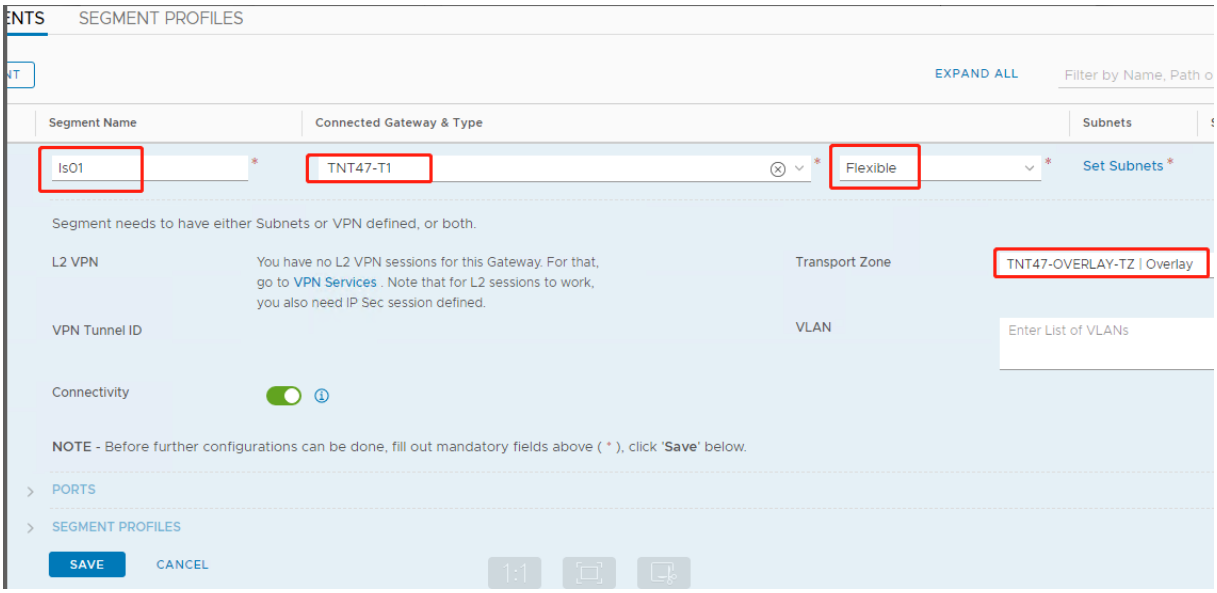
Adicione um segmento de rede no Azure VMware Solution Depois de configurar o DHCP, adicione um segmento de rede.

Para adicionar um segmento de rede, no NSX-T Manager, selecione **Networking> Segments** e clique em **Add Segment**.



Na tela **Segments profile**:

1. Insira um **nome** para o segmento.
2. Selecione o **Tier-1 Gateway (TNTxx-T1)** como o **Connected Gateway** e deixe o **Type** como **Flexible**.
3. Selecione a **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Clique em **Set Subnets**.



Na seção **Subnets** :

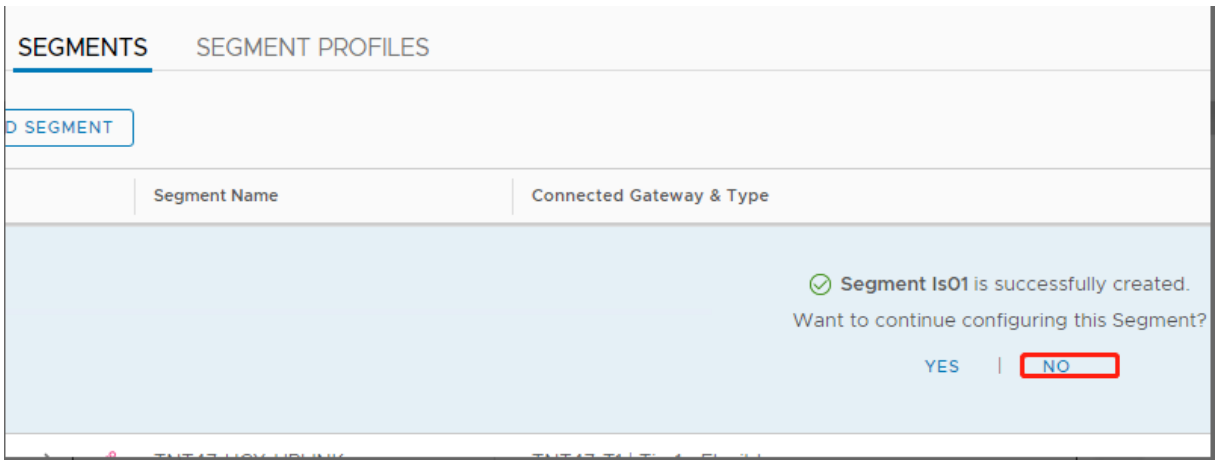
1. Digite o endereço IP do gateway.
2. Selecione **Add**.

> **Importante:**
>
> O endereço IP desse segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.

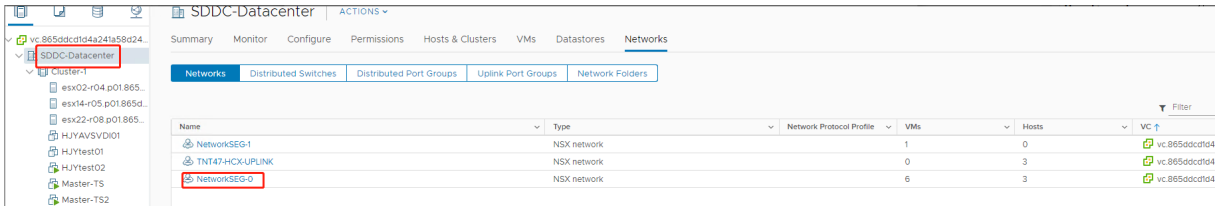
O intervalo DHCP deve pertencer ao endereço IP do segmento:

Segment name	Connected gateway	Gateway IP	DHCP range	Port/VIF	State
NetworkSEG-0	TNT47-T1	10.15.4.1/24	10.15.4.100-10.15.4.200	6	SUCCESS

Selecione **No** para recusar a opção de continuar configurando o segmento:



No vCenter, selecione **Rede > Datacenter SDDC**:



Verificar o ambiente do Azure AVS Configure uma conexão direta e um conector no grupo de recursos do Azure:

Verifique a conexão com as credenciais do vCenter:

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 precisa ter acesso ao Google Cloud VMware Engine, à cota de nós disponível do VMware Engine e a uma função do IAM apropriada. Prepare os seguintes requisitos antes de continuar a criar a sua nuvem privada:

1. Solicite acesso à API e cota de nós. Para obter mais informações, consulte Como solicitar acesso e cota da API.
2. Anote os intervalos de endereços que você deseja usar para os dispositivos de gerenciamento VMware e a rede de implantação HCX. Para obter mais informações, consulte Requisitos de rede.
3. Obtenha a função do IAM de VMware Engine Service Admin.

Criar a sua primeira nuvem privada

1. Acesse o portal do VMware Engine.
2. Na página inicial do VMware Engine, clique em **Create a private cloud**. 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 CIDR (Classless Inter-Domain Routing) 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.

6. Selecione **Review and create**.
7. Revise as configurações. Para alterar a configuração, clique em **Back**.
8. Clique em **Create** para começar a criar a nuvem privada.

À medida que o VMware Engine cria a sua nova nuvem privada, ele implanta vários componentes do VMware e define políticas de Autoscale iniciais para clusters na nuvem privada. A criação da nuvem privada pode levar de 30 minutos a 2 horas. Depois que o provisionamento é concluído, você recebe um e-mail.

Configurar o gateway VPN do Google Cloud VMware Engine Para estabelecer a conectividade inicial com o Google Cloud VMware Engine, você pode usar um gateway VPN. Essa é uma VPN cliente baseada em OpenVPN com a qual você pode se conectar ao seu vCenter SDDC (VMware Software Defined Data Center) e fazer qualquer configuração inicial necessária.

Antes de implantar um gateway VPN, configure o intervalo de **Edge Services** para a região onde o seu SDDC está implantado. Para isso:

1. Faça logon no portal do **Google Cloud VMware Engine** e acesse **Network > Regional Settings**. Clique em **Add Region**.
2. Escolha a região em que o seu SDDC está implantado e ative **Internet Access** e **Public IP Service**.
3. Forneça o intervalo dos Edge Services anotado durante o planejamento e clique em **Submit**. A ativação desses serviços leva de 10 a 15 minutos.

   Depois de concluídos, os Edge Services são exibidos como **Enabled** na página Regional Settings. A ativação dessas configurações permite que IPs públicos sejam alocados para o seu SDDC, o que é um requisito para a implantação de um gateway VPN.

Para implantar um gateway VPN:

1. No portal do **Google Cloud VMware Engine**, acesse **Network > VPN Gateways**. Clique em **Create New VPN Gateway**.
2. Forneça o nome do gateway VPN e da sub-rede cliente reservados durante o planejamento. Clique em **Next**.
3. Selecione os usuários para conceder acesso à VPN. Clique em **Next**.
4. Especifique as redes que devem ser acessíveis por VPN. Clique em **Next**.
5. Uma tela de resumo é exibida. Verifique as seleções e clique em **Submit** para criar o gateway VPN. A página VPN Gateways é exibida com o status do novo gateway VPN como **Creating**.
6. Depois que o status mudar para **Operational**, clique no novo gateway VPN.
7. Clique em **Download my VPN configuration** para baixar um arquivo ZIP contendo perfis OpenVPN pré-configurados para o gateway VPN. Perfis para conexão por meio de UDP/1194 e TCP/443 estão disponíveis. Escolha a sua preferência e importe-a para o Open VPN; depois conecte-se.
8. Vá para **Resources** e selecione o 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 VPN Gateway. Consulte Configurar o gateway VPN do Google Cloud VMware Engine.
2. Carregue a configuração da VPN baixada em Configurar o gateway VPN do Google Cloud VMware Engine.
3. Importe para a sua VPN cliente, por exemplo, OpenVPN Connect.

Para obter mais informações, consulte Como se conectar usando uma VPN.

Criar a primeira sub-rede

Acessar o NSX-T Manager no portal do VMware Engine O processo de criação de uma sub-rede acontece 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 do **Google Cloud VMware Engine**.
2. Na navegação principal, vá para **Resources**.
3. Clique no **nome da nuvem privada** correspondente à nuvem privada em que 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 origem de identidade, como o Active Directory, use as suas credenciais de origem 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 **Networking > DHCP**. O painel de rede mostra que o serviço DHCP cria um gateway Tier-0 e outro Tier-1.
2. Para começar a provisionar um servidor DHCP, clique em **Add Server**.
3. Selecione **DHCP** para o **Server Type**, forneça o nome do servidor e o endereço IP.
4. Clique em **Save** para criar o serviço DHCP.

Faça o seguinte para anexar esse serviço DHCP ao gateway Tier-1 relevante. Um gateway padrão Tier-1 já está provisionado pelo serviço DHCP :

1. Selecione **Tier 1 Gateways**, selecione as reticências verticais no gateway de camada 1 e, em seguida, selecione **Edit**.
2. No campo **IP Address Management**, selecione **No IP Allocation Set**.
3. Selecione **DHCP Local Server** para o **Type**.

4. Selecione o servidor DHCP que você criou para o **DHCP Server**.
5. Clique em **Salvar**.
6. Clique em **Close Editing**.

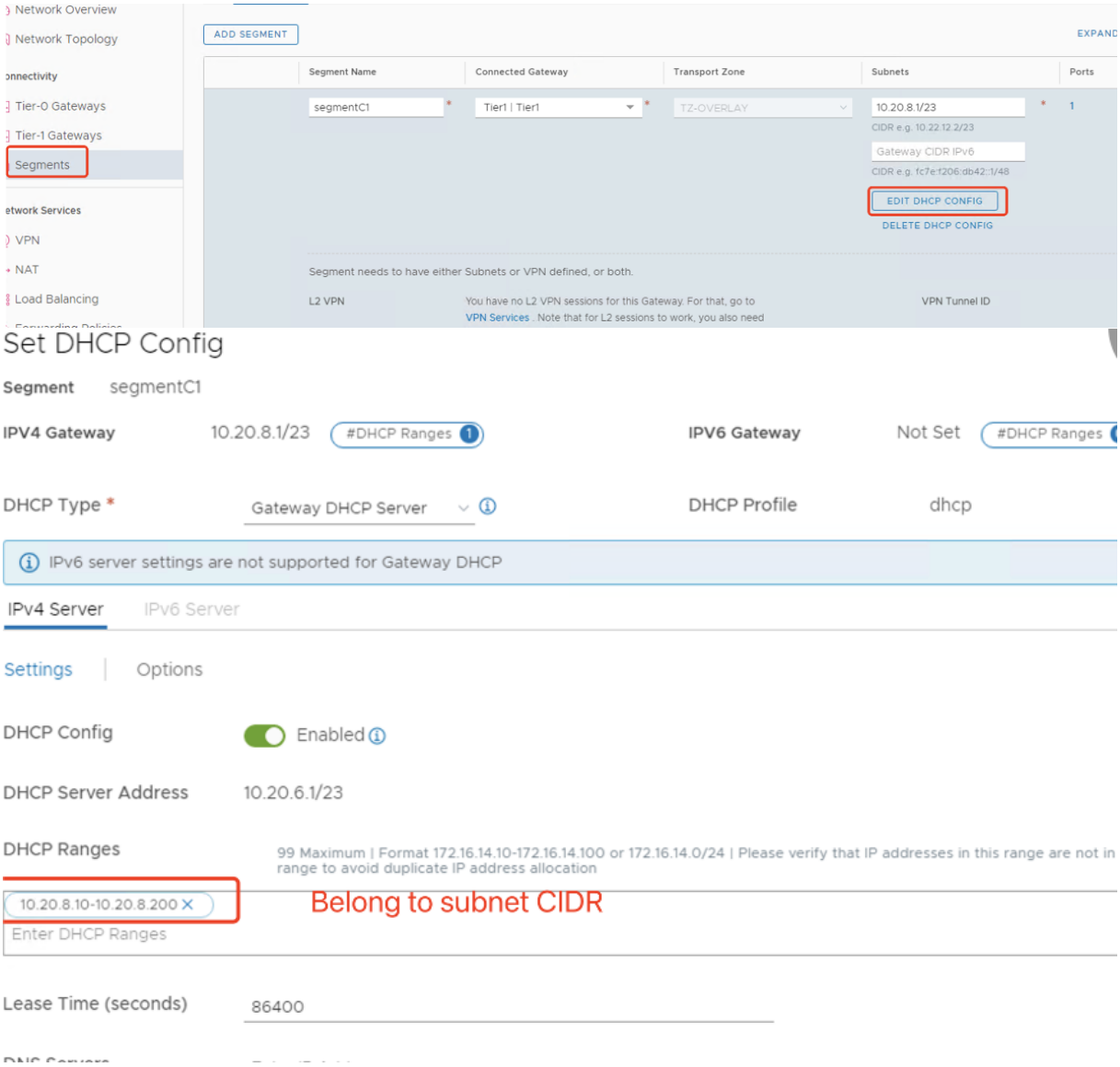
Agora você pode criar um segmento de rede no NSX-T. Para obter mais informações sobre DHCP no NSX-T, consulte a documentação do VMware para DHCP.

Criar um segmento de rede no NSX-T Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede do NSX-T para a sua nuvem privada:

1. No NSX-T Manager, vá para **Networking > Segments**.
2. Clique em **Add Segment**.
3. Insira um nome para o segmento.
4. Selecione **Tier-1** como **Connected Gateway** e deixe Type como **Flexible**.
5. Clique em **Set Subnets**.
6. Clique em **Add Subnets**.
7. Insira o intervalo de sub-rede em **Gateway IP/Prefix Length**. Especifique o intervalo de sub-rede com **.1** como o último octeto. Por exemplo, **10.12.2.1/24**.
8. Especifique os intervalos de DHCP e clique em **ADD**.
9. Em **Transport Zone**, selecione **TZ-OVERLAY** na lista suspensa.
10. Clique em **Salvar**. Agora você pode selecionar esse segmento de rede no vCenter quando criar uma VM.

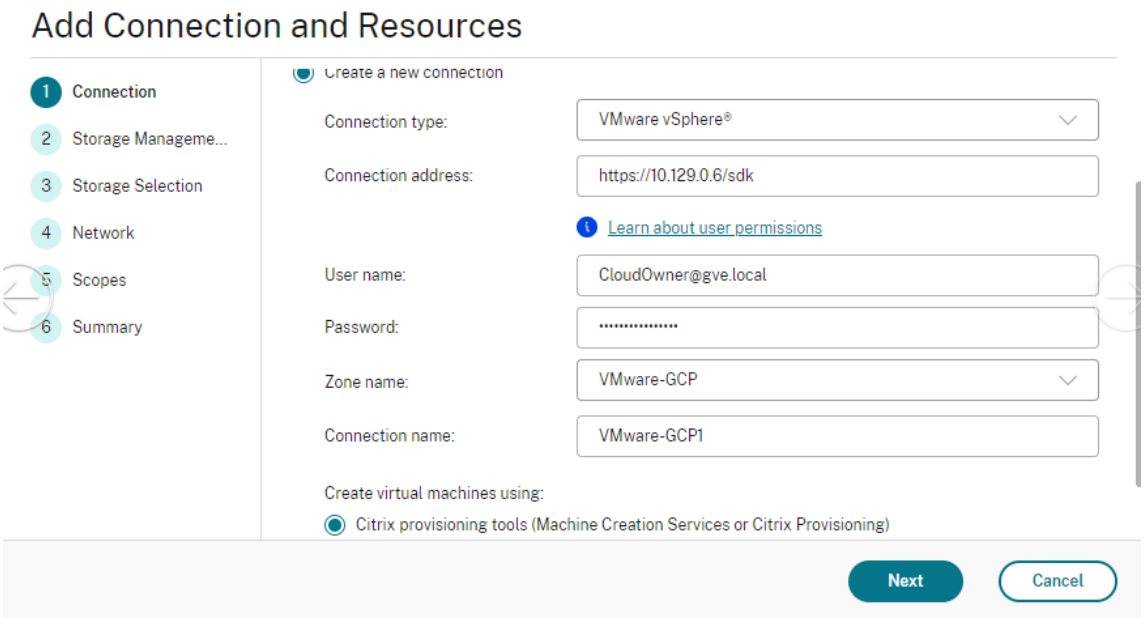
Em uma determinada região, você pode configurar no máximo 100 rotas exclusivas do VMware Engine para a sua rede VPC usando o acesso a serviços privados. Isso inclui, por exemplo, intervalos de endereços IP de gerenciamento de nuvem privada, segmentos de rede de carga de trabalho NSX-T e intervalos de endereços IP de rede HCX. Esse limite inclui todas as nuvens privadas na região.

> **Nota:**
>
> Há um problema de configuração do Google Cloud, por isso você precisa definir a configuração do intervalo DHCP várias vezes. Portanto, certifique-se de definir a configuração do intervalo DHCP após a configuração do Google Cloud. Clique em **EDIT DHCP CONFIG** para configurar os intervalos de DHCP.



Criar a conexão do Google Cloud VMware no Citrix Studio

1. Crie uma máquina no vCenter e instale o Cloud Connector na máquina.
2. Inicie o Citrix Studio.
3. Selecione o nó de hospedagem e clique em **Add Connection and Resources**.
4. Na tela **Connection**, selecione **Create a new Connection** e os seguintes detalhes:



a) Selecione **Connection type** como **VMware vSphere**.
b) Em **Connection address**, insira o endereço IP privado de vCenter.
c) Insira as credenciais do vCenter.
d) Digite um nome para a conexão.
e) Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Network**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

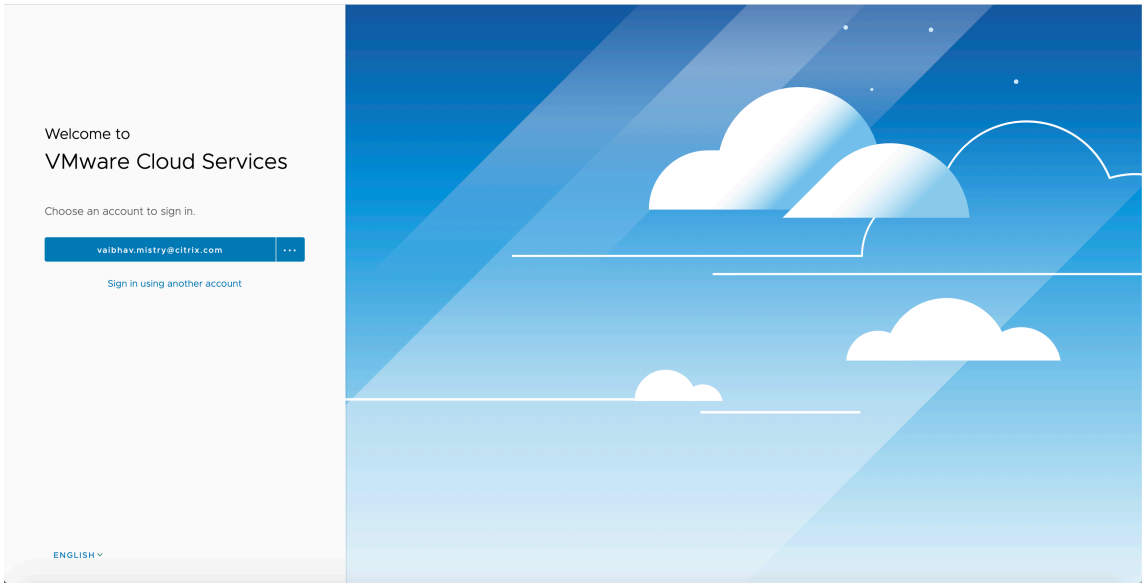
Nuvem VMware na Amazon Web Services (AWS)

A nuvem VMware na 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 Citrix DaaS.

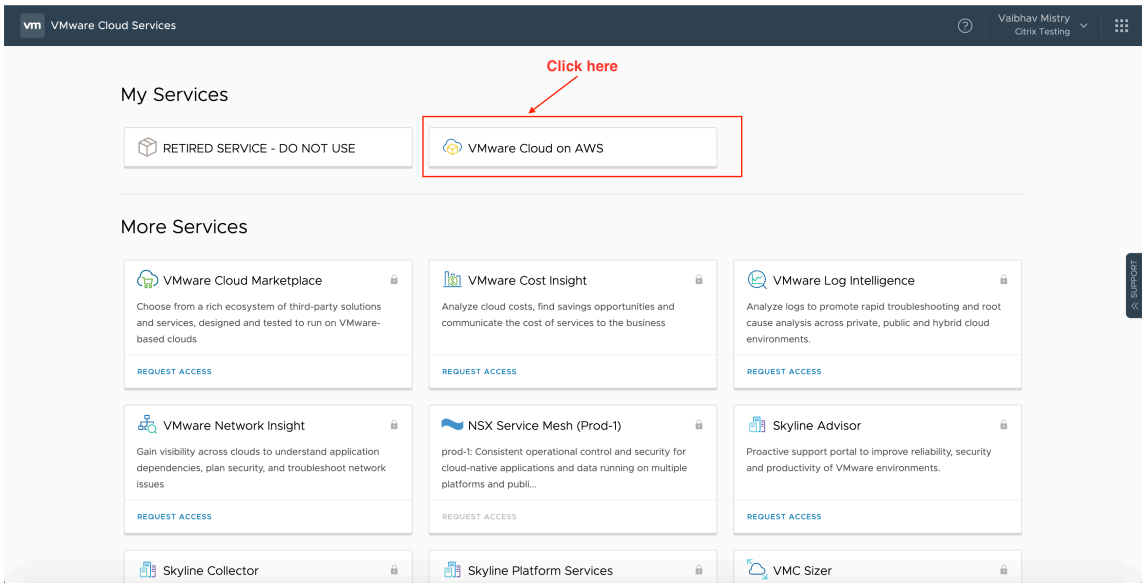
Este artigo descreve o procedimento para configurar uma nuvem VMware na AWS.

Acesse o ambiente de nuvem VMware

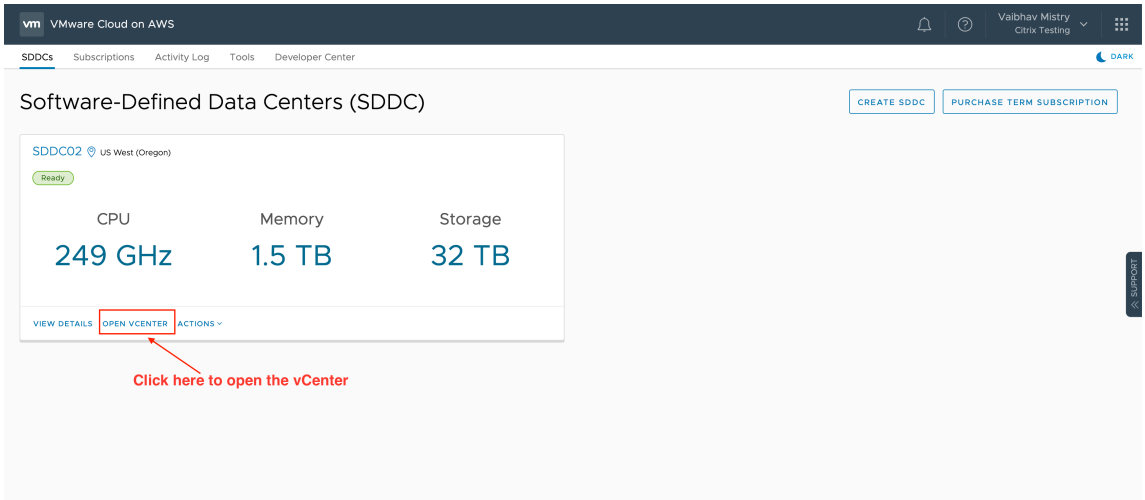
1. Faça login nos serviços de nuvem da VMware usando o URL https://console.cloud.vmware.com/.

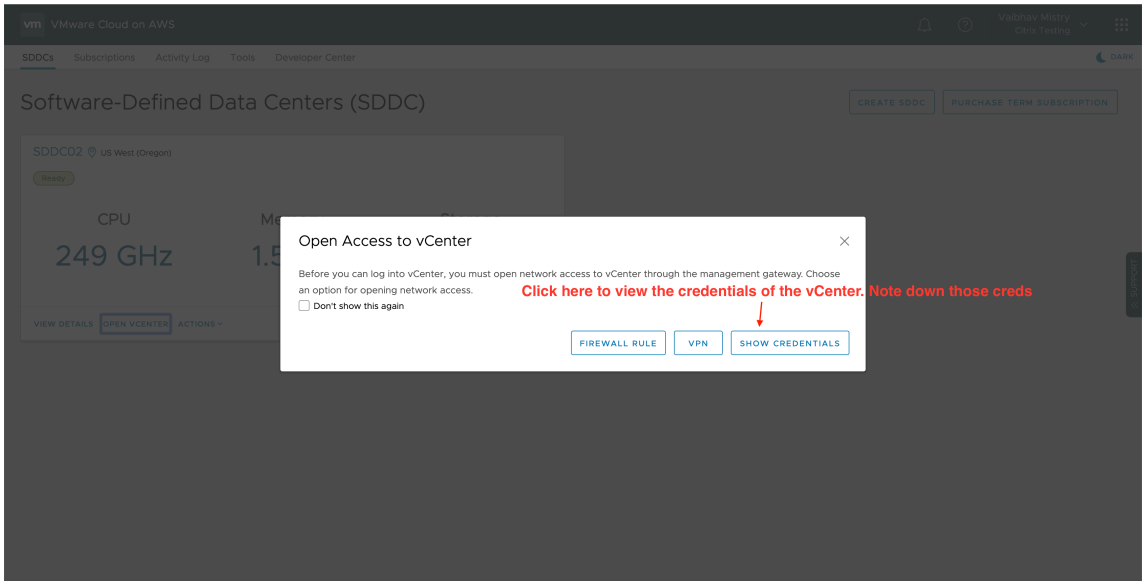


2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

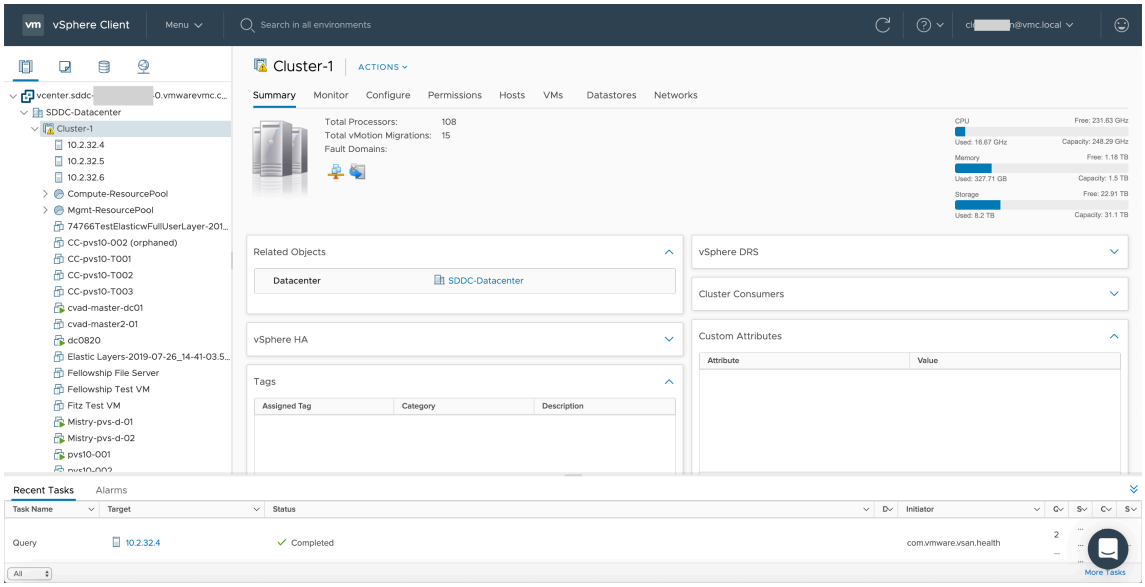


3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Observe as credenciais para uso posterior.





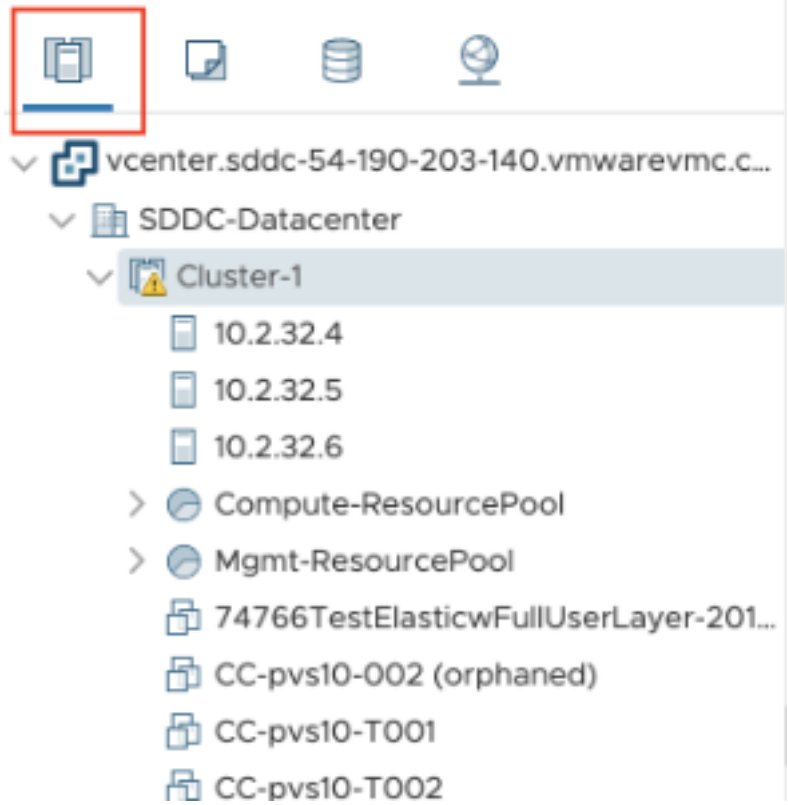
4. Abra um navegador da Web e insira a URL do vSphere Web Client.
5. Insira as credenciais conforme indicado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



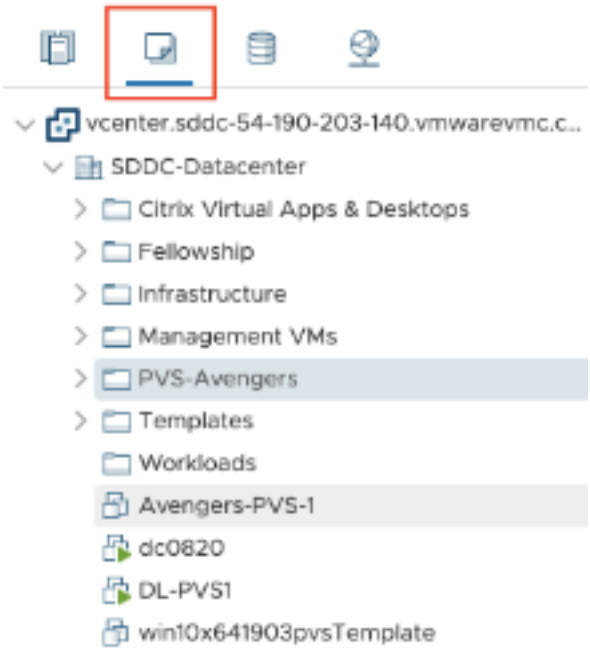
Sobre o ambiente de nuvem VMware

Há quatro visualizações na página da Web do cliente vSphere.

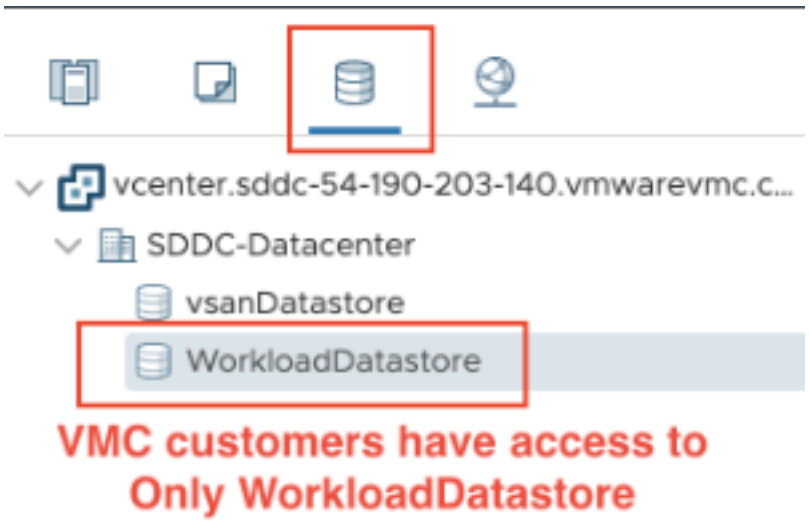
- Visualização de host e cluster: você não pode criar um novo cluster, mas o administrador da nuvem pode criar vários pools de recursos.



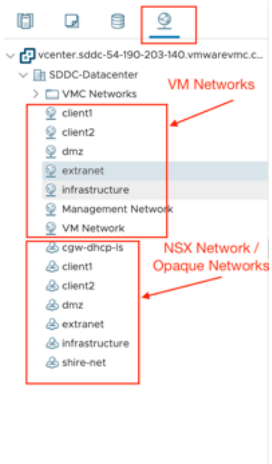
- Visualização de VM e modelo: o administrador da nuvem pode criar várias pastas.



- Exibição de armazenamento: selecione **WorkloadDatastore** storage ao adicionar a unidade de hospedagem no Citrix Studio porque você tem acesso somente ao Workload Datastore.



- Exibição de rede: os ícones são diferentes para redes em nuvem VMware e redes opacas.



Depois de configurar o cluster, consulte Ambientes de virtualização VMware para adicionar conexões e recursos.

O que fazer a seguir

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que fornecerá aplicativos ou uma área de trabalho para seus usuários.

- Para criar e gerenciar uma conexão, consulte Conexão com soluções de nuvem e parceiros do VMware.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Considerações de tamanho e escala de Cloud Connectors

March 3, 2023

Ao avaliar o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) 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 de sua implantação.

> **Nota:**
>
> Essas recomendações se aplicam ao Citrix DaaS Standard para Azure, e também ao Citrix DaaS.

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 Cache de host local (LHC).

As informações fornecidas se aplicam a implantações nas quais cada local de recursos contém cargas de trabalho VDI ou cargas de trabalho RDS. Para locais de recursos que contêm as cargas de trabalho de VDI e RDS juntas, entre em contato com Citrix Consulting Services.

O Cloud Connector vincula suas cargas de trabalho ao Citrix DaaS das seguintes maneiras:

- Fornece um proxy para a comunicação entre seus VDAs e o Citrix DaaS
- Fornece um proxy para a comunicação entre o Citrix DaaS e seu Active Directory (AD) e hipervisores
- Em implantações que incluem servidores StoreFront, o Cloud Connector atua como um agente de sessão temporário durante interrupções na nuvem, fornecendo aos usuários acesso contínuo aos recursos

É importante ter seus Cloud Connectors devidamente dimensionados e configurados para atender às suas necessidades específicas.

Cada conjunto de Cloud Connectors é atribuído a um local de recursos (também conhecido como zona). Um local de recursos é uma separação lógica que especifica quais recursos se comunicam com o conjunto de Cloud Connectors. É necessário pelo menos um local de recursos por domínio para se comunicar com o Active Directory (AD).

Cada catálogo de máquinas e conexão de hospedagem é atribuído a um local de recursos.

Para implantações com mais de um local de recursos, atribua catálogos de máquinas e VDAs aos locais de recursos para otimizar a capacidade do LHC de intermediar conexões durante interrupções. Para obter mais informações sobre como criar e gerenciar locais de recursos, consulte Conectar-se ao Citrix Cloud. Para um desempenho ideal, configure seus Cloud Connectors em conexões de baixa latência para VDAs, servidores AD e hipervisores.

Processadores e armazenamento recomendados

Para obter um desempenho semelhante ao observado nesses testes, use processadores modernos que aceitam extensões SHA. As extensões SHA reduzem a carga criptográfica na CPU. Os processadores recomendados incluem:

- Advanced Micro Devices (AMD) Zen e processadores mais recentes
- Intel Ice Lake e processadores mais recentes

Os processadores recomendados funcionam com eficiência. Você pode usar processadores mais antigos, no entanto, isso pode levar a uma maior carga da CPU. Recomendamos aumentar sua contagem de vCPUs para compensar isso.

Os testes descritos neste artigo foram realizados com os processadores AMD EPYC e Intel Cascade Lake.

Os Cloud Connectors têm uma carga criptográfica pesada durante a comunicação com a nuvem. Os Cloud Connectors que usam processadores com extensões SHA sentem uma carga menor na CPU, o que é expresso pelo menor uso da CPU pelo serviço LSASS (Local Security Authority Subsystem Service) do Windows.

A Citrix recomenda usar o armazenamento moderno com operações de E/S por segundo (IOPS) adequadas, especialmente para implantações que usam LHC. sugerimos as unidades de estado sólido (SSD), mas os níveis premium de armazenamento em nuvem não são necessários. IOPS mais altas são necessárias para cenários do LHC em que o Cloud Connector executa uma pequena cópia do banco de dados. Esse banco de dados é atualizado com alterações de configuração do site regularmente e fornece recursos de intermediação para o local de recursos nos momentos de interrupção do Citrix Cloud.

Configuração de computação recomendada para cache de host local

O Cache de host local (LHC) fornece alta disponibilidade ao permitir que as operações de intermediação de conexão em uma implantação continuem quando um Cloud Connector não pode se comunicar com o Citrix Cloud.

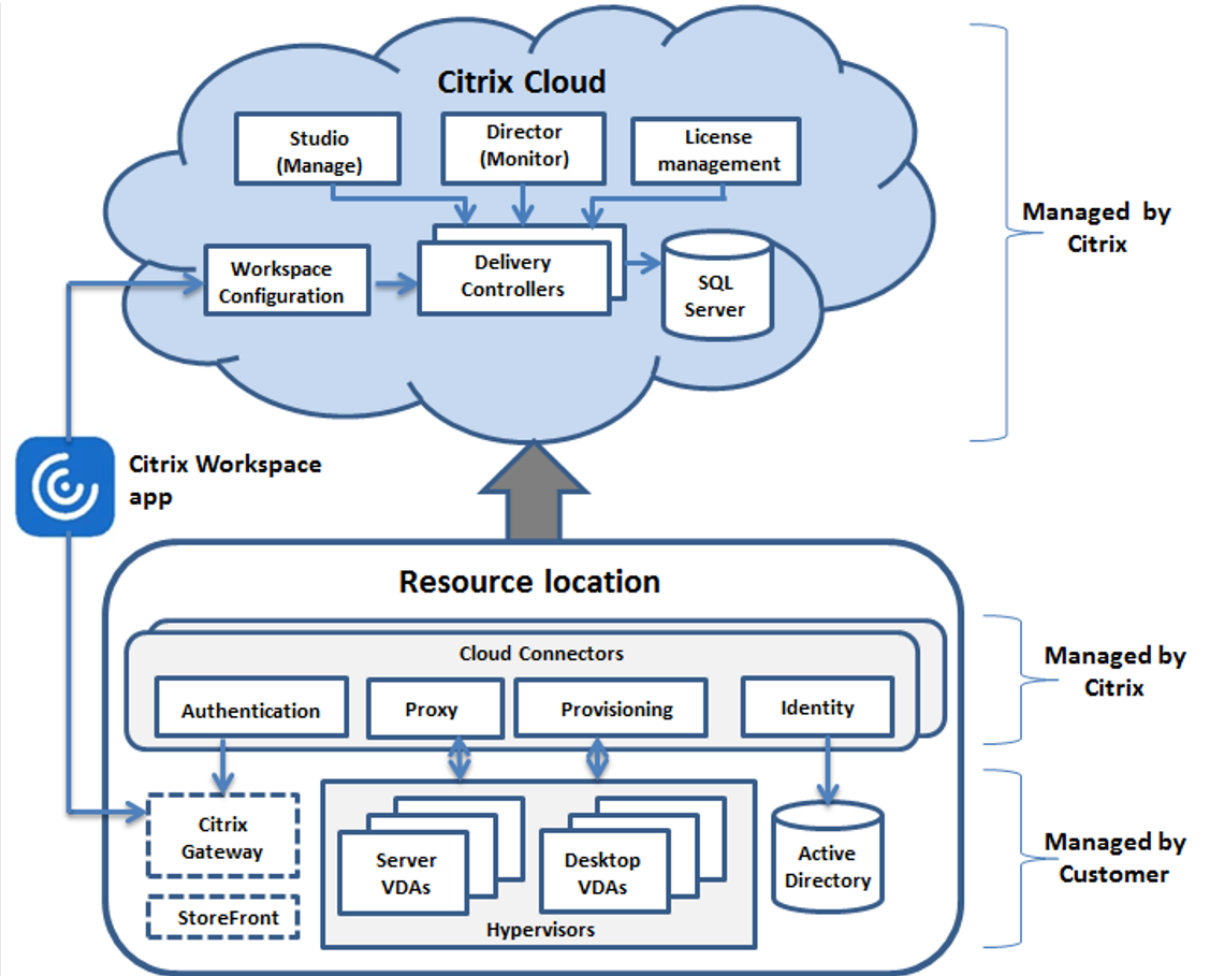
Os Cloud Connectors executam o Microsoft SQL Express Server LocalDB, que é instalado automaticamente quando você instala o Cloud Connector. A configuração da CPU do Cloud Connector, especialmente o número de núcleos disponíveis para o SQL Express Server LocalDB, afeta diretamente o desempenho do LHC. O número de núcleos de CPU disponíveis para o SQL Server Express Server LocalDB afeta o desempenho do LHC mais do que a alocação de memória. Essa sobrecarga de CPU é observada somente no modo LHC quando o Citrix DaaS não está acessível e o agente do LHC está ativo. Para qualquer implantação usando 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 SQL Express Server LocalDB, consulte Compute capacity limits by edition of SQL Server.

Se os recursos de computação disponíveis para o SQL Express Server LocalDB estiverem configurados incorretamente, o tempo de sincronização da configuração poderá aumentar e o desempenho durante as interrupções será reduzido. Em alguns ambientes virtualizados, a capacidade computacional dependerá do número de processadores lógicos e não de núcleos de CPU.

Resumo dos resultados do teste

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 de um único local de recursos. Diferentes configurações de sistema podem produzir resultados diferentes.

Esta ilustração fornece uma visão geral gráfica da configuração testada.



Esta tabela fornece um guia rápido para dimensionar a sua localização de recursos. 10.000 é o máximo para um local de recursos. Consulte Limites para obter informações sobre os limites de localização do recurso.

> **Nota:**
>
> Exceder o limite pode causar problemas de conectividade e desempenho durante uma interrupção. Portanto, você não deve exceder o limite recomendado, pois isso pode levar ao cancelamento do registro de VDAs.

Os resultados são baseados em testes internos da Citrix. As configurações descritas foram testadas com cargas de trabalho variadas, incluindo testes de início de sessão de alta taxa e tempestades de registro.

	Médio	Grande	Máximo
VDAs	1000 VDI ou 250 RDS	5000 VDI ou 500 RDS	10.000 VDI ou 1000 RDS

	Médio	Grande	Máximo
Conexões de hospedagem	20	40	40
CPUs para Connectors	4 vCPU	4 vCPU	8 vCPU
Memória para Connectors	6 GB	8 GB	10 GB

Metodologia do teste

Foram realizados testes 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. Em alguns casos, foram usadas ferramentas de simulação de propriedade da Citrix para simular VDAs e sessões. Essas ferramentas foram concebidas para exercitar os componentes 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 conduzidos na intermediação em nuvem e no modo LHC em cenários com o Citrix StoreFront.

As recomendações para o dimensionamento do Cloud Connector neste artigo são baseadas nos dados coletados nos testes.

Os seguintes testes foram executados:

- **Tempestade de início/logon 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 a intermediação na nuvem e o modo de Cache de host local.
- **Tempestade de ação de energia VDA:** um teste que simula alto volume de ações de energia VDA.

Cenários e condições de teste

Estes testes foram realizados com o LHC configurado. Para obter mais informações sobre como usar o LHC, consulte o artigo Cache de host local. 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 ou grupo de servidores StoreFront, ative a opção de verificação de integridade avançada para a loja do StoreFront. Consulte

Requisito do StoreFront no artigo Cache de host local.
- 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 os serviços básicos de SO e da Citrix. Aplicativos e serviços de terceiros podem exigir recursos adicionais.
- VDAs são máquinas virtuais ou físicas que executam o Citrix Virtual Delivery Agent.
- Todos os VDAs testados tiveram sua energia gerenciada usando o Citrix DaaS.
- Foram testadas cargas de trabalho de servidores de 1.000 a 10.000 VDI e 250-1000 RDS com 1.000-20.000 sessões.
- As sessões RDS foram testadas com até 20.000 por local de recursos.
- Os testes foram realizados usando um Cloud Connector em operações normais e durante interrupções. A Citrix recomenda usar pelo menos dois Cloud Connectors para alta disponibilidade. Quando em modo de interrupção, apenas um dos conectores é usado para registros de VDA e intermediação.
- Os testes foram realizados com o Cloud Connector configurado com os processadores Intel Cascade Lake.
- As sessões foram iniciadas por meio de um único servidor Citrix StoreFront.
- Testes de início de sessão com interrupção do LHC conduzidos após as máquinas terem se registrado novamente.

As contagens de sessões do RDS são uma recomendação e não um limite. Teste seu próprio limite de sessão do RDS em seu ambiente.

> **Nota:**
>
> A contagem de sessões e a taxa de inicialização são mais importantes para o RDS do que a contagem de VDA.

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	Registro de uso de CPU e memória	Duração do teste de início	Uso de CPU e memória no início de sessão	Taxa de inicialização
1000 VDI	Online	5 minutos	CPU máxima = 36%, média da CPU = 33%, memória máxima = 5,3 GB	2 minutos	CPU máxima = 29%, média da CPU = 27%, memória máxima = 3,7 GB	500 por minuto
1000 VDI	Interrupção	4 minutos	CPU máxima = 11%, média da CPU = 10%, memória máxima = 4,5 GB	2 minutos	CPU máxima = 42%, média da CPU = 28%, memória máxima = 4,0 GB	500 por minuto
200 RDS, 5000 sessões	Online	3 minutos	CPU máxima = 14%, média da CPU = 4%, memória máxima = 3,5 GB	9 minutos	CPU máxima = 46%, média da CPU = 21%, memória máxima = 3,7 GB	555 por minuto
200 RDS, 5000 sessões	Interrupção	3 minutos	CPU máxima = 15%, média da CPU = 5%, memória máxima = 3,7	9 minutos	CPU máxima = 51%, média da CPU = 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	Registro de uso de CPU e memória	Duração do teste de início	Uso de CPU e memória no início de sessão	Taxa de inicialização
5000 VDI	Online	3—4 minutos	CPU máxima = 45%, média da CPU = 25%, memória máxima = 7,0 GB	5 minutos	CPU máxima = 75%, média da CPU = 55%, memória máxima = 7,0 GB	1000 por minuto
5000 VDI	Interrupção	4—6 minutos	CPU máxima = 15%, média da CPU = 5%, máximo de memória = 7,5 GB	5 minutos	CPU máxima = 45%, média da CPU = 40%, memória máxima = 7,5 GB	1000 por minuto
500 RDS, 10.000 sessões	Online	3 minutos	CPU máxima = 45%, média da CPU = 25%, memória máxima = 7,0 GB	10 minutos	CPU máxima = 75%, média da CPU = 55%, memória máxima = 7,0 GB	1000 por minuto

Cargas de trabalho de teste	Condição do site	Tempo de registro do VDA	Registro de uso de CPU e memória	Duração do teste de início	Uso de CPU e memória no início de sessão	Taxa de inicialização
500 RDS, 10.000 sessões	Interrupção	3 minutos	CPU máxima = 15%, média da CPU = 5%, memória máxima = 7,5	10 minutos	CPU máxima = 45%, média da CPU = 40%, memória máxima = 7,5 GB	1000 por minuto

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	Registro de uso de CPU e memória	Duração do teste de início	Uso de CPU e memória no início de sessão	Taxa de inicialização
10.000 VDI	Online	3—4 minutos	CPU máxima = 85%, média da CPU = 10%, máximo de memória = 8,5 GB	7 minutos	CPU máxima = 66%, média da CPU = 28%, memória máxima = 7,0 GB	1400 por minuto
10.000 VDI	Interrupção	4–5 minutos	CPU máxima = 90%, média da CPU = 17%, memória máxima = 8,2 GB	5 minutos	CPU máxima = 90%, média da CPU = 45%, memória máxima = 8,5 GB	2000 por minuto

Cargas de trabalho de teste	Condição do site	Tempo de registro do VDA	Registro de uso de CPU e memória	Duração do teste de início	Uso de CPU e memória no início de sessão	Taxa de inicialização
1000 RDS, 20.000 sessões	Online	1—2 minutos	CPU máxima = 60%, média da CPU = 20%, memória máxima = 8,6 GB	17 minutos	CPU máxima = 66%, média da CPU = 25%, memória máxima = 6,8 GB	1200 por minuto
1000 RDS, 20.000 sessões	Interrupção	3—4 minutos	CPU máxima = 22%, média da CPU = 10%, memória máxima = 8,5	21 minutos	CPU máxima = 90%, média da CPU = 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 recursos. Para dar suporte a cargas de trabalho maiores, adicione mais locais de recursos.

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, garantindo que os Cloud Connectors estejam prontos para assumir a intermediação se ocorrer uma interrupção. A sincronização de configuração atualiza o banco de dados do LHC, SQL Express Server LocalDB. O processo importa os dados para um banco de dados temporário e depois alterna para o banco de dados depois de importado. Isso garante que sempre haja um banco de dados do LHC pronto para assumir o controle.

O uso de CPU, memória e disco aumenta temporariamente enquanto os dados são importados para o banco de dados temporário.

Resultados do teste:

- **Tempo de importação de dados:** 7 a 10 minutos
- **Uso de CPU:**
  - máximo = 25%
  - média = 15%
- **Uso de memória:**
  - máximo = 9 GB
  - aumento de aproximadamente 2 GB a 3 GB
- **Uso de disco:**
  - pico de leitura de disco de 4 MB/s
  - pico de gravação em disco de 18 MB/s
  - Pico de gravação em disco de 70 MB/s durante download e gravação de arquivos de configuração xml
  - Pico de leitura de disco de 4 MB/s na conclusão da importação
- **Tamanho do banco de dados do LHC:**
  - Arquivo de banco de dados de 400 a 500 MB
  - Banco de dados de log de 200 a 300 MB

Condições de teste:

- Testado em um AMD EPYC de 8 vCPUs
- O banco de dados de configuração de site importado destinava-se a 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 recursos com 10.000 VDI

Considerações adicionais sobre 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.
- O site testado usou aproximadamente 800 MB para o banco de dados e os 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. Assegure que o Cloud Connector tenha espaço em disco suficiente para os arquivos duplicados. O processo de sincronização de configuração falhará se o disco estiver cheio.

Instalar VDAs

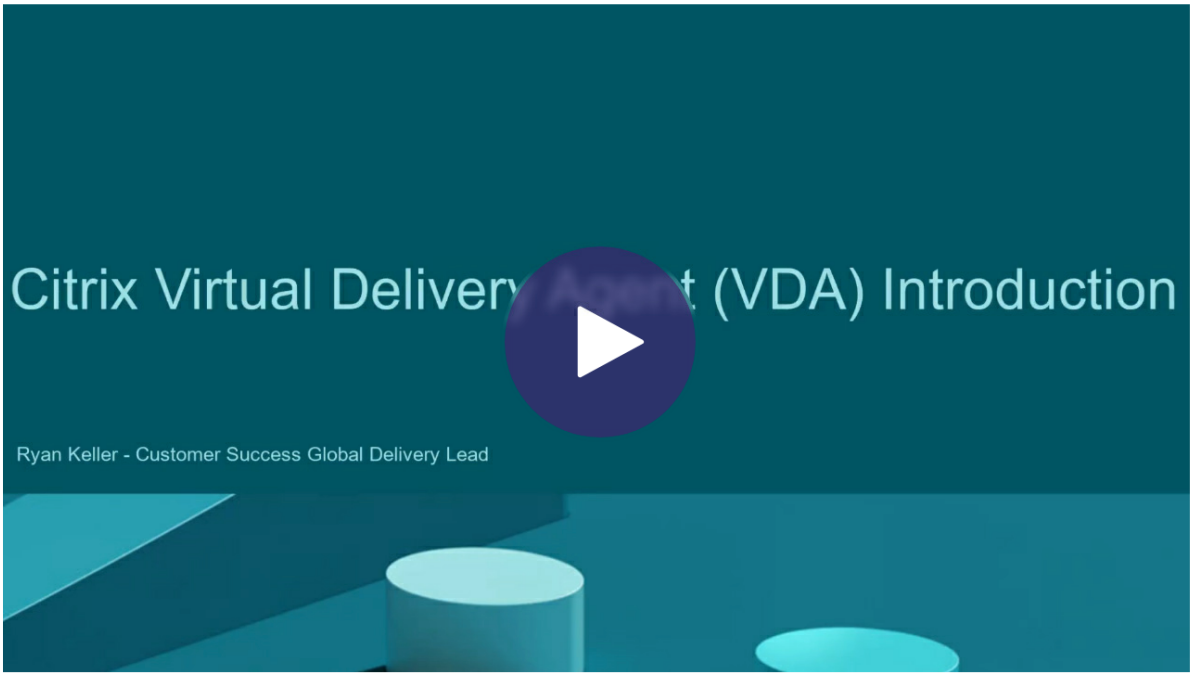
November 9, 2023

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 linhas de comando são fornecidos. Para obter detalhes, consulte Instalar VDAs usando a linha de comando.

Para obter informações sobre Linux VDAs, consulte Linux Virtual Delivery Agent.

Veja uma introdução aos VDAs.



Considerações sobre a instalação

O artigo Citrix DaaS descreve o que são VDAs e o que fazem. Veja aqui estão mais informações.

- **Analytics collection:** dados do Analytics são coletados automaticamente quando você instala ou atualiza componentes. Por padrão, esses dados são carregados automaticamente para o Citrix quando a instalação é concluída. Além disso, ao instalar componentes, você é automaticamente registrado no Programa de Aperfeiçoamento da Experiência do Usuário (CEIP) da Citrix, que carrega dados anônimos. Além disso, durante uma instalação ou atualização, você tem a oportunidade de se inscrever no Call Home.

  Se a instalação de um 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 terminar o registro no CEIP, os dados do analisador MSI coletados não serão mais enviados para a 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 quando você instala um VDA. Você pode baixar e instalar ou atualizar o aplicativo Citrix Workspace para Windows e outros aplicativos Citrix Workspace no site da Citrix. Como alternativa, você pode disponibilizar os aplicativos Citrix Workspace a partir do Workspace ou de um servidor do StoreFront.
- **Serviço de Spooler de Impressão:** o serviço de Spooler de Impressão da Microsoft deve estar ativado. Você não consegue instalar um VDA com êxito se esse serviço estiver desativado.
- **Microsoft Media Foundation:** a maioria das edições compatíveis do Windows vem com o Media Foundation já instalado. Se a máquina na qual você está instalando um VDA não tiver o Microsoft Media Foundation (como as edições N), vários recursos de multimídia não serão instalados e não funcionarão.
  - Redirecionamento Flash
  - Windows Media Redirection
  - Redirecionamento de vídeo HTML5
  - Redirecionamento de Webcam HDX RealTime

  Você pode aceitar a limitação ou encerrar a instalação do VDA e reiniciá-la mais tarde, depois de 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 aceitar a limitação.
- **Grupo de usuários local:** quando você instala o VDA, um novo grupo de usuários local chamado Direct Access Users é criado automaticamente. Em um VDA de SO de sessão única, esse grupo se aplica somente às conexões RDP. Em um VDA de SO multissessão, esse grupo se aplica às conexões ICA e RDP.
- **Requisito de endereço do Cloud Connector:** o VDA deve ter pelo menos um endereço válido do Cloud Connector (na mesma localização do recurso) com o qual se comunicar. Caso contrário, as sessões não podem ser estabelecidas. Você especifica endereços do Cloud Connector ao instalar o VDA. Para obter informações sobre outras maneiras de especificar endereços do Cloud Connector nos quais os VDAs podem se registrar, consulte Registro de VDA.
- **Considerações sobre o sistema operacional:**
  - Revise os Requisitos de sistema para as plataformas, sistemas operacionais e versões compatíveis.
  - Certifique-se de que todos os sistemas operacionais mantenham 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.

  - Diretrizes de otimização para máquinas com Windows 10 estão disponíveis em CTX216252.
  - Se você tentar instalar (ou atualizar para) um Windows VDA em um sistema operacional que não é compatível com a versão do VDA, uma mensagem descreverá as suas opções. Por exemplo, se você tentar instalar o VDA mais recente em um computador com Windows antigo, uma mensagem o guiará para CTX139030. Para obter mais informações, consulte 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 **Additional Components** 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 está ingressada no domínio antes de instalar o software VDA.

Ferramentas de suporte de VDA

Cada instalador de VDA inclui um MSI de suporte que contém ferramentas Citrix para verificar o desempenho do VDA, como sua integridade geral e a qualidade das conexões. Ativar ou desativar a instalação desse MSI na página de **componentes adicionais** da interface gráfica do instalador de VDA. Na linha de comando, desative a instalação com a opção `/exclude "Citrix Supportability Tools"`.

Por padrão, a MSI de capacidade de suporte é instalada em a `C:\Program Files (x86)\Citrix\Supportability Tools\`. Você pode alterar o local na página **Componentes** da interface gráfica do instalador de VDA ou com a opção de linha de comando `/installdir`. Tenha em mente que alterar o local irá alterá-lo para todos os componentes VDA instalados, não apenas para as ferramentas de suporte.

Ferramentas atualmente no suporte MSI:

- Citrix Health Assistant: para obter detalhes, consulte CTX207624.
- VDA Cleanup Utility: para obter detalhes, consulte CTX209255.

Se você não instalar as ferramentas quando instalar o VDA, o artigo CTX contém um link para o download do pacote atual.

Reinicializações durante a instalação do VDA

Uma reinicialização é necessária no 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 suportada do Microsoft .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas de SO multissessão Windows, instale e ative os serviços de função do 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 da linha de comando sem a opção `/noreboot`, a máquina reinicializa automaticamente após a instalação do pré-requisito.
- Se você estiver usando a interface da linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Após cada reinicialização, a instalação do VDA continua. Se você estiver instalando a partir da linha de comando, poderá impedir a retomada automática com a opção `/noresume`.

Quando está atualizando um VDA para a versão 7.17 ou uma versão posterior suportada, ocorre uma reinicialização durante a atualização. Essa reinicialização não pode ser evitada.

Restaurar em caso de falha de instalação ou atualização

> **Nota:**
>
> Esse recurso está disponível apenas para VDAs de sessão única.

Se uma instalação ou atualização do VDA de sessão única falhar e o recurso "restaurar em caso de falha"estiver ativado, a máquina será retornada a um ponto de restauração definido antes do início da instalação ou atualização.

Quando uma instalação ou atualização do VDA de sessão única começa com esse recurso ativado, 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 será retornada ao estado do ponto de restauração. A pasta `%temp%/Citrix` contém registros de implantação e outras informações sobre a restauração.

Por padrão, este recurso está desativado.

Se você planeja habilitar esse recurso, verifique se a restauração do sistema não está desativada por meio de uma configuração de GPO (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

Para habilitar esse recurso ao instalar ou atualizar um VDA de sessão única:

- Ao usar a interface gráfica de um instalador VDA (como usar o **Autostart** ou o comando `XenDesktopVDASetup.exe` sem opções de restauração ou silencioso), marque a caixa de seleção **Enable automatic restore if update fails** na página **Summary**.

Se a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será mantido.

- 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 mantido.

Instaladores de VDA

Os instaladores de VDA podem ser baixados diretamente do console do Citrix Cloud.

Por padrão, os arquivos nos instaladores de extração automática são extraídos para a pasta `Temp`. Os arquivos extraídos para a pasta `Temp` são excluídos automaticamente após a conclusão da instalação. Alternativamente, você pode usar o comando `/extract` com um caminho absoluto.

Três instaladores autônomos de VDA estão disponíveis para download.

VDAServerSetup.exe instala um VDA de SO multissessão.

VDAWorkstationSetup.exe instala um VDA de SO de sessão única.

VDAWorkstationCoreSetup.exe instala um VDA de SO de sessão única que é otimizado para implantações do Remote PC Access ou instalações básicas de VDI. O Remote PC Access usa máquinas físicas. As instalações básicas de VDI são VMs que não estão sendo usadas como uma imagem. Este instalador implanta apenas os serviços principais necessários para conexões VDA. Portanto, ele suporta apenas um subconjunto das opções que são válidas com o instalador VDAWorkstationSetup.

Este instalador da versão atual não instala nem contém os componentes usados para:

- App-V.
- Profile Management. Excluir o Citrix Profile Management da instalação afeta as exibições do Monitor.
- Machine Identity Service.
- Citrix Workspace app for Windows.
- Citrix Supportability Tools.
- Citrix Files for Windows.
- Citrix Files for Outlook.
- MCSIO write cache for storage optimization.

Este instalador não instala nem contém um aplicativo Citrix Workspace para Windows.

Este instalador instala automaticamente o MSI de redirecionamento de conteúdo do navegador. A instalação automática se aplica à versão de VDA 2003 e versões suportadas posteriores.

Usar `VDAWorkstationCoreSetup.exe` é equivalente a usar o instalador `VDAWorkstationSetup.exe` para instalar um VDA de SO de sessão única com uma destas opções:

- Na interface gráfica: selecionar a opção **Remote PC Access** na página **Environment**.
- Na interface de linha de comando: especificar a opção `/remotepc`.
- Na interface da linha de comando: especificar `/components vda` e `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`.

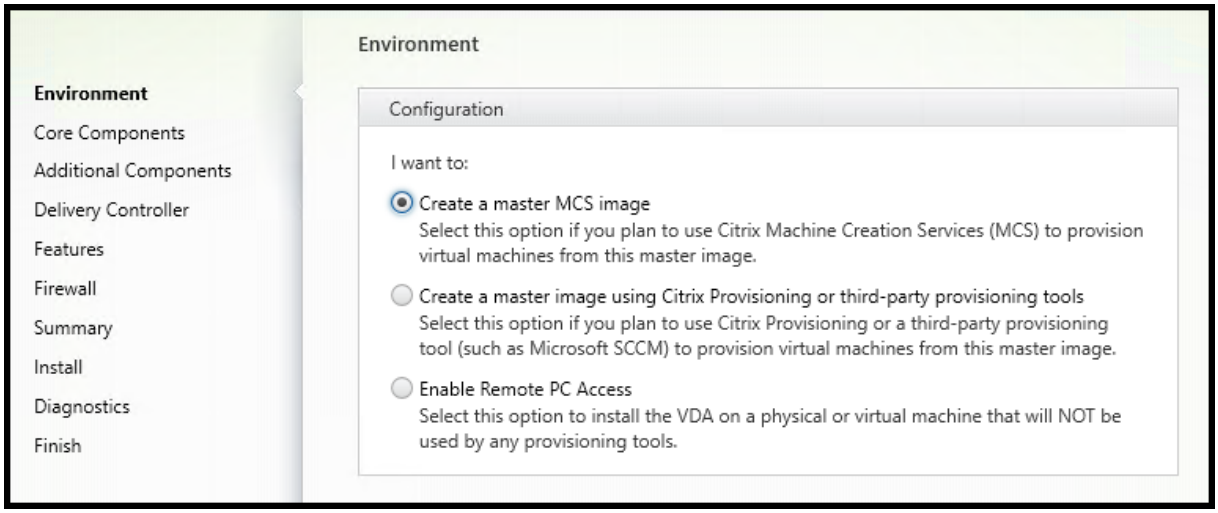
Se você instalar um VDA com o instalador `VDAWorkstationCoreSetup.exe` e, posteriormente, atualizar esse VDA usando o instalador `VDAWorkstationSetup.exe`, poderá instalar opcionalmente os componentes e recursos omitidos.

Etapa 1. Baixe o software do produto e inicie o assistente

1. Na máquina em que você está instalando o VDA, faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione Citrix DaaS na lista **My Services**.
3. No lado direito, clique em **Downloads** e selecione **Download VDA**. Você é redirecionado para a página de download do VDA. Encontre o instalador do VDA desejado e selecione **Download File**.
4. Após a conclusão do download, clique com o botão direito do mouse no arquivo e selecione **Executar como administrador**. O assistente de instalação é iniciado.

Como alternativa às etapas 1 a 3, você pode baixar o VDA diretamente da página de download da Citrix.

Etapa 2. Especifique como o VDA será usado



Na página **Environment**, especifique como planeja usar o VDA, indicando se você usará essa máquina como uma imagem para provisionar máquinas. A opção escolhida afeta quais ferramentas do Citrix Provisioning são instaladas automaticamente (se houver) e os valores padrão na página **Additional Components** do instalador de VDA.

Escolha uma das seguintes opções:

- **Create a master MCS image:** selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar Machine Creation Services para provisionar VMs. Esta opção instala o Machine Identity Service. Esta é a opção padrão.

  Opção de linha de comando: `/mastermcsimage` ou `/masterimage`

- **Create a master image using Citrix Provisioning or third-party provisioning tools:** selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar o Citrix Provisioning ou ferramentas de provisionamento de terceiros (como o Microsoft System Center Configuration Manager). Use essa opção para VMs provisionadas anteriormente que foram inicializadas a partir de um disco de leitura/gravação do Citrix Provisioning.

  Opção de linha de comando: `/masterpvsimage`

- (Aparece apenas em máquinas de SO multissessão) **Enable brokered connections to a server:** selecione esta opção para instalar um VDA em uma máquina física ou virtual que não será usada como uma imagem.

  Opção de linha de comando: `/remotepc`

- (Aparece apenas em máquinas de SO multissessão) **Enable Remote PC Access:** selecione esta opção para instalar um VDA em uma máquina física para usar com o Remote PC Access.

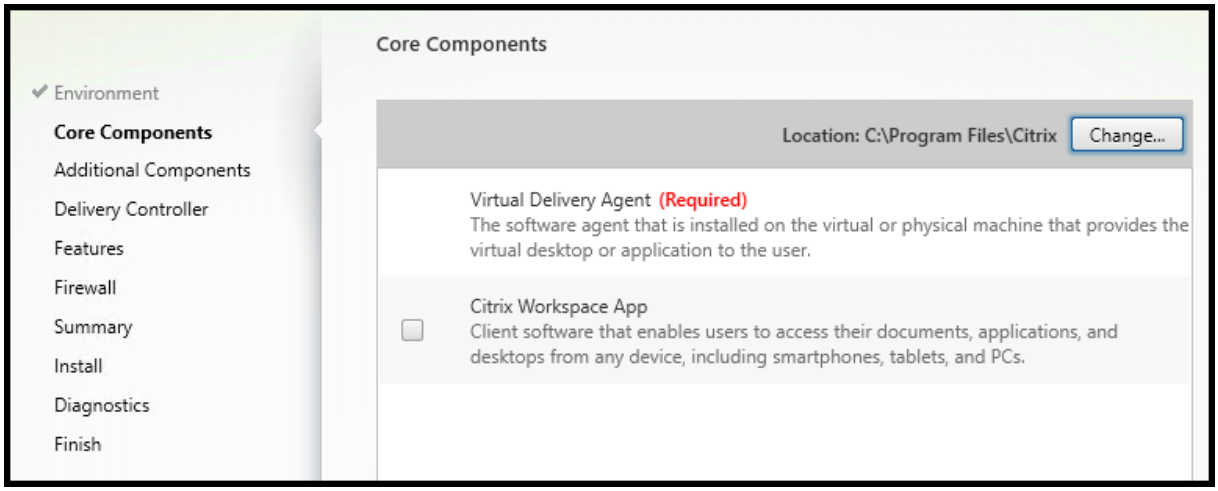
  Opção de linha de comando: `/remotepc`

Selecione **Next**.

Esta página não aparece:

- Ao atualizar um VDA.
- Ao usar o instalador `VDAWorkstationCoreSetup.exe`.

Etapa 3. Selecione os componentes para instalar e o local de instalação



Na página **Core components**:

- **Location:** por padrão, os componentes são instalados em `C:\Program Files\Citrix`. Esse padrão é adequado para a maioria das implantações. Se você especificar um local diferente, tal local deverá ter permissões de execução do serviço de rede.

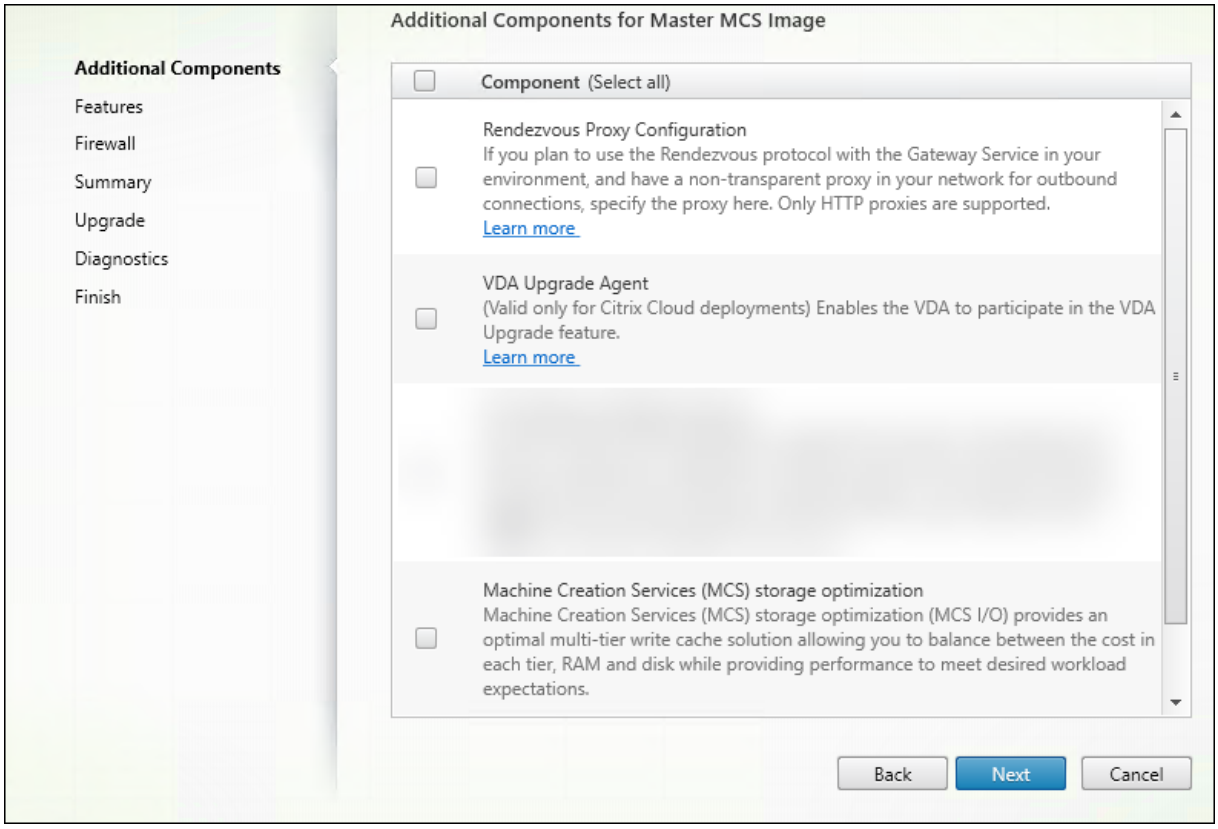
  Opção de linha de comando: `/installdir`

- **Components:** por padrão, o aplicativo Citrix Workspace para Windows não é instalado com o VDA. Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`, o aplicativo Citrix Workspace para Windows nunca será instalado, portanto, essa caixa de seleção não é exibida.

  Opção de linha de comando: `/components vda,plugin` para instalar o VDA e o aplicativo Citrix Workspace para Windows

Selecione **Next**.

Etapa 4. Instale componentes adicionais



A página **Additional Components** contém caixas de seleção para ativar ou desativar a instalação de outros recursos e tecnologias com o VDA. Em uma instalação de linha de comando, você pode usar a opção `/exclude` ou `/includeadditional` para omitir ou incluir um ou mais componentes disponíveis.

A tabela a seguir indica a configuração padrão dos itens nessa página. A configuração padrão depende da opção selecionada na página **Environment**.

Página Additional Components	Página Environment: “Master image with MCS”ou “Master image with Citrix Provisioning …”selecionado	Página Environment: “Enable brokered connections to server”(para SO multissessão) ou “Remote PC Access”(para SO de sessão única) selecionado
Citrix Personalization for App-V	Não selecionado	Não selecionado
User Personalization Layer	Não selecionado	Não é mostrado porque não é válido para este caso de uso
Citrix Supportability tools	Selecionado	Não selecionado

Página Additional Components	Página Environment: “Master image with MCS”ou “Master image with Citrix Provisioning …”selecionado	Página Environment: “Enable brokered connections to server”(para SO multissessão) ou “Remote PC Access”(para SO de sessão única) selecionado
Citrix Profile Management	Selecionado	Não selecionado
Citrix Profile Management WMI Plug-in	Selecionado	Não selecionado
Citrix VDA Upgrade Agent	Não selecionado	Não selecionado
Citrix Backup and Restore	Não selecionado	Não selecionado
Citrix Files para Windows	Não selecionado	Não selecionado
Citrix Files para Outlook	Não selecionado	Não selecionado
Otimização de armazenamento de Machine Creation Services (MCS)	Não selecionado	Não selecionado
Rendezvous protocol configuration	Não selecionado	Não selecionado

Esta página não aparece quando:

- O instalador `VDAWorkstationCoreSetup.exe` é usado. Além disso, as opções de linha de comando para os componentes adicionais não são válidas com esse instalador.
- Um VDA é atualizado e todos os componentes adicionais já estão instalados. Se alguns dos componentes adicionais já estiverem instalados, a página listará apenas os componentes que não estão instalados.

A lista de componentes pode incluir:

- **Citrix Personalization for App-V:** instale este componente se usar aplicativos de pacotes do Microsoft App-V. Para obter detalhes, consulte App-V.

  Opção de linha de comando: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar a instalação de componentes, `/exclude "Citrix Personalization for App-V – VDA"` para prevenir a instalação de componentes

- **Citrix User Personalization Layer:** instala o MSI para a camada de personalização do usuário. Para obter detalhes, consulte Camada de personalização do usuário.

  Este componente aparece somente ao instalar um VDA em um computador Windows 10 de sessão única.

Opção de linha de comando: `/includeadditional "User Personalization Layer"` para habilitar a instalação de componentes, `/exclude "User Personalization Layer"` para prevenir a instalação de componentes

- **Citrix Supportability Tools:** instala o MSI que contém ferramentas de suporte da Citrix.

  Opção de linha de comando: `/includeadditional "Citrix Supportability Tools"` para habilitar a instalação de componentes, `/exclude "Citrix Supportability Tools"` para prevenir a instalação de componentes

- **Citrix Profile Management:** este componente gerencia as configurações de personalização do usuário em perfis de usuário. Para obter detalhes, consulte Profile Management.

  Excluir Citrix Profile Management da instalação afeta o monitoramento e a solução de problemas de VDAs no Citrix Cloud.

  - Nas páginas **User details** e **EndPoint** da guia **Monitor**, o painel **Personalization** e o painel **Logon Duration** falham.
  - Nas páginas **Dashboard** e **Trends**, o painel **Average Logon Duration** exibe dados somente para máquinas que têm o Profile Management instalado.

  Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Citrix Profile Management Service. A ativação do Citrix Profile Management Service não é necessária.

  Opção de linha de comando: `/includeadditional "Citrix Profile Management "` para habilitar a instalação de componentes, `/exclude "Citrix Profile Management "` para prevenir a instalação de componentes

- **Citrix Profile Management WMI Plug-in:** este plug-in fornece informações de runtime do Profile Management em objetos WMI (Instrumentação de Gerenciamento do Windows) (por exemplo, provedor de perfil, tipo de perfil, tamanho e uso do disco). Objetos WMI fornecem informações da sessão ao Director.

  Opção de linha de comando: `/includeadditional "Citrix Profile Management WMI Plugin"` para habilitar a instalação de componentes, `/exclude "Citrix Profile Management WMI Plugin"` para prevenir a instalação de componentes

- **VDA Upgrade Agent:** (Aplica-se apenas a implantações do Citrix DaaS.) Permite que o VDA participe do recurso VDA Upgrade. Você pode usar esse recurso para atualizar os VDAs de um catálogo a partir do console de gerenciamento, imediatamente ou em um horário agendado. Se esse agente não estiver instalado, você poderá atualizar um VDA executando o instalador do VDA na máquina.

  Opções de linha de comando: `/includeadditional "Citrix VDA Upgrade Agent "` para ativar a instalação de componentes, `/exclude "Citrix VDA Upgrade Agent"` para impedir a instalação de componentes

- **Citrix Files for Windows:** este componente permite que os usuários se conectem à conta do Citrix Files. Assim, eles podem interagir com o Citrix Files por meio de uma unidade mapeada no sistema de arquivos Windows, sem exigir uma sincronização completa de seu conteúdo.

  Opções de linha de comando: `/includeadditional "Citrix Files for Windows"` para ativar a instalação de componentes, `/exclude "Citrix Files for Windows"` para impedir a instalação de componentes

- **Citrix Files for Outlook:** este componente permite ignorar restrições de tamanho de arquivo e adicionar segurança aos anexos ou e-mails enviando-os através do Citrix Files. Você pode fornecer uma solicitação de upload seguro de arquivos diretamente no seu e-mail. Para obter mais informações, consulte Citrix Files for Outlook.

  Opções de linha de comando: `/includeadditional "Citrix Files for Outlook"` para ativar a instalação de componentes, `/exclude "Citrix Files for Outlook"` para impedir a instalação de componentes

- **Otimização de armazenamento de Machine Creation Services (MCS):** Instala o driver Citrix MCS IO. Para obter mais informações, consulte Armazenamento compartilhado por hipervisores e Configurar cache para dados temporários.

  Opções de linha de comando: `/includeadditional "Citrix MCS IODriver"` para ativar a instalação de componentes, `/exclude "Citrix MCS IODriver"` para impedir a instalação de componentes

- **Rendezvous Proxy Configuration:** instale este componente se você planeja usar o protocolo Rendezvous com o Citrix Gateway Service em seu ambiente e tem um proxy não transparente em sua rede para as conexões de saída. Somente proxies HTTP são aceitos.

  Se você instalar esse componente, especifique o endereço do proxy ou caminho do arquivo PAC na página **Rendezvous Proxy Configuration**. Para obter detalhes do recurso, consulte Protocolo Rendezvous.

  Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para habilitar a instalação de componentes, `/exclude "Citrix Rendezvous V2"` para prevenir a instalação de componentes

- **Citrix Backup and Restore:** se a instalação ou atualização do VDA falhar, esse componente poderá voltar a máquina para um backup que foi feito antes da instalação ou atualização.

  Opção de linha de comando: `/includeadditional "Citrix Backup and Restore"` para habilitar a instalação de componentes, `/exclude "Citrix Backup and Restore"` para prevenir a instalação de componentes.

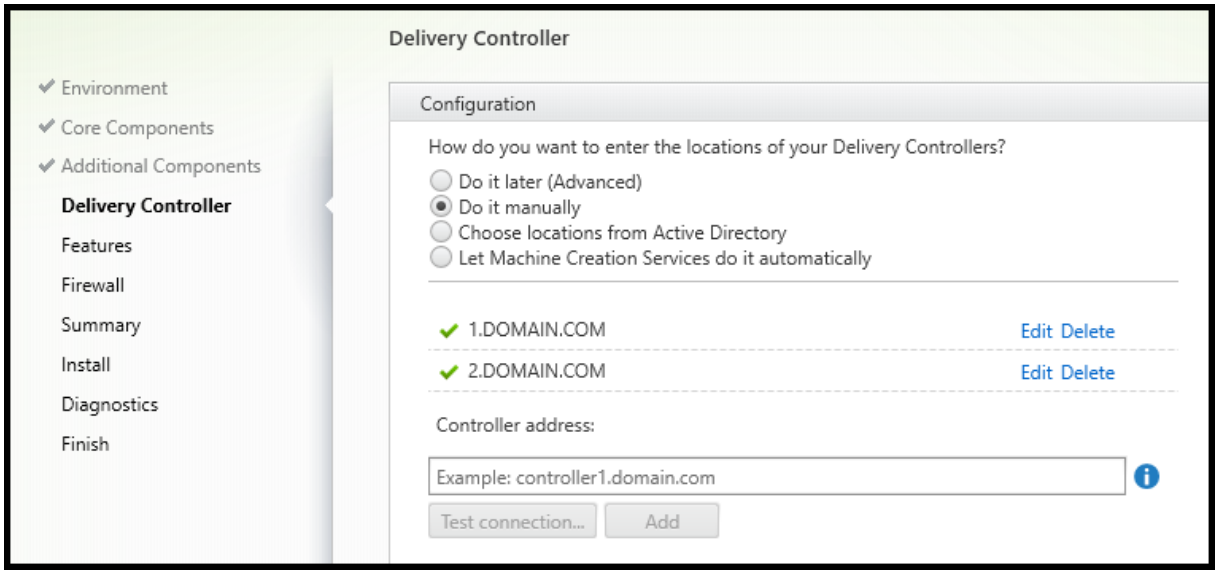
- **Citrix HyperV Filter Driver:** esse componente deve ser ativado usando a caixa de seleção somente se você atualizar de uma versão mais antiga do VDA (versão inferior a 2308). O compo-

nente mantém as configurações de NIC da imagem mestre nas VMs provisionadas. As configurações são mantidas mesmo após a atualização do Windows.

Opção de linha de comando: `/includeadditional "Citrix HyperV Filter Driver"` para habilitar a instalação de componentes, `/exclude "Citrix HyperV Filter Driver"` para prevenir a instalação de componentes.

> **Nota:**
>
> Esse componente é instalado automaticamente se você fizer uma nova instalação do VDA versão 2308 ou posterior em uma máquina com Hyper-V implantado (incluindo Azure e SCVMM) por meio das instalações da imagem mestre do MCS.

Etapa 5. Endereços do Cloud Connector



Na página **Delivery Controller**, selecione **Do it manually**. Insira o nome DNS de um Cloud Connector instalado e selecione **Add**. Se você instalou Cloud Connectors adicionais localização do recurso, adicione seus nomes DNS.

Selecione **Next**.

Considerações:

- O endereço pode conter apenas caracteres alfanuméricos.
- O registro bem-sucedido do VDA exige que as portas de firewall usadas para se comunicar com o Cloud Connector estejam abertas. Essa ação é ativada por padrão na página **Firewall** do assistente.

Opção de linha de comando: `/controllers`

Etapa 6. Rendezvous Proxy Configuration

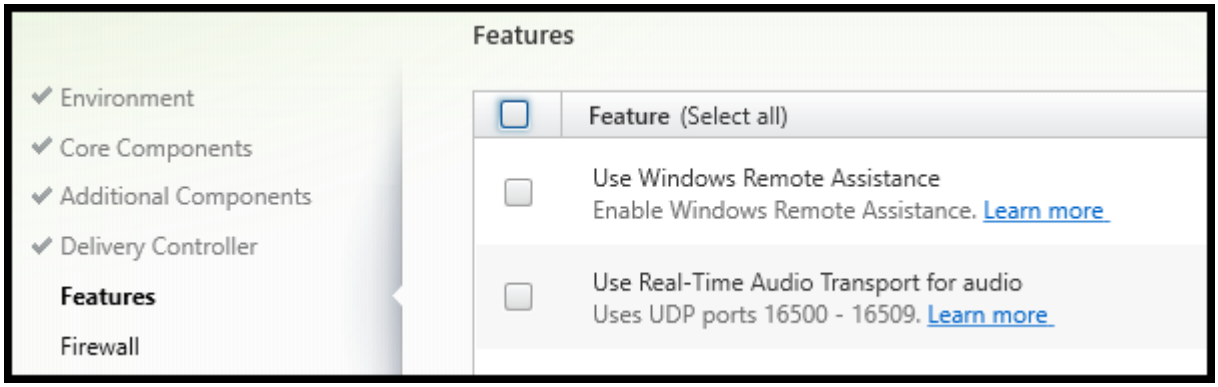
A página **Rendezvous Proxy Configuration** é exibida apenas se você marcar a caixa de seleção **Rendezvous Proxy Configuration** na página **Additional Components**.

1. Selecione se você especificará a origem do proxy por endereço proxy ou caminho do arquivo PAC.
2. Especifique o endereço proxy ou o caminho do arquivo PAC.
   - Formato de endereço proxy: `http://<url-or-ip>:<port>`
   - Formato de arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

O firewall da porta proxy deve estar aberto para que o teste de conexão seja realizado. Se não for possível estabelecer uma conexão com o proxy, você pode decidir se deseja continuar com a instalação do VDA.

Opção de linha de comando: `/proxyconfig`

Etapa 7. Ativar ou desativar recursos



Na página **Features**, use as caixas de seleção para ativar ou desativar os recursos que deseja usar.

- **Use Windows Remote Assistance:** quando este recurso está ativado, a Assistência Remota do Windows é usada com o recurso de sombreamento do usuário do componente do Director no Citrix Cloud. A Assistência Remota do Windows abre as portas dinâmicas no firewall. (Padrão = desativado)

  Opção de linha de comando: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio:** ative este recurso se Voice-over-IP for amplamente utilizado em sua rede. O recurso reduz a latência e melhora a resiliência de áudio em redes com perdas. Ele permite que os dados de áudio sejam transmitidos usando o transporte RTP sobre UDP. (Padrão = desativado)

  Opção de linha de comando: `/enable_real_time_transport`

- **Use screen sharing:** Quando ativado, as portas usadas pelo compartilhamento de tela são abertas no firewall do Windows. (Padrão = desativado)

  Opção de linha de comando: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud:** essa configuração ajuda a Citrix a identificar corretamente os locais de recursos para implantações de VDA no local e de serviço (Citrix Cloud) para fins de telemetria. Esse recurso não tem impacto na utilização do lado do cliente. Ative essa configuração se a sua implantação usar Citrix DaaS. (Padrão = desativado)

  Opção de linha de comando: `/xendesktopcloud`

Selecione **Next**.

Se esta página contiver um recurso chamado **MCS I/O**, não o use. O recurso MCS IO é configurado na página **Additional Components**.

Etapa 8. Portas de firewall

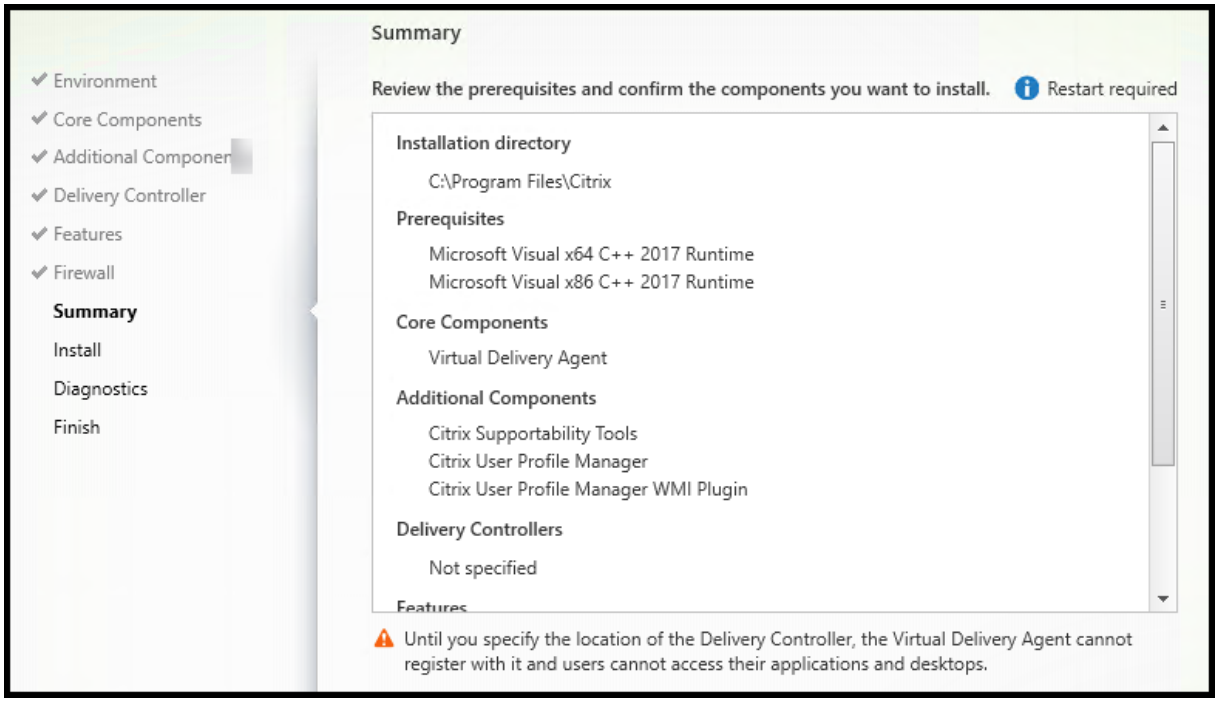
A página **Firewall** indica quais portas o VDA e os Cloud Connectors usam para se comunicar entre eles. Por padrão, essas portas são abertas automaticamente se o Serviço do Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Essa configuração padrão é adequada para a maioria das implantações.

Para obter informações sobre portas, consulte Network ports.

Selecione **Next**.

Opção de linha de comando: `/enable_hdx_ports`

Etapa 9. Verifique os pré-requisitos e confirme a instalação

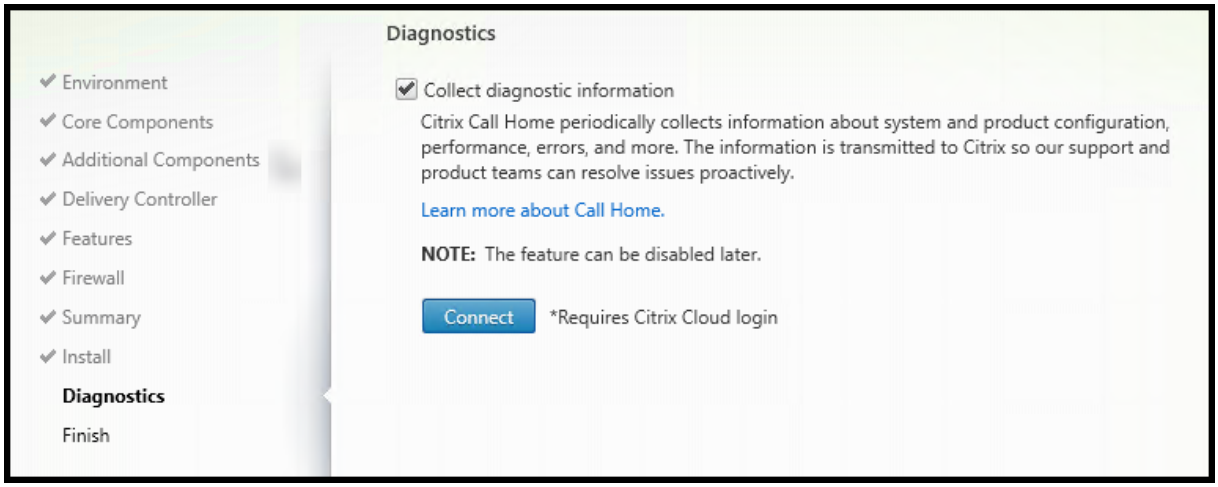


A página **Summary** lista o que será instalado. Você pode retornar às páginas anteriores do assistente e alterar as seleções, se necessário.

(Somente VDAs de sessão única) Marque a caixa de seleção **Enable automatic restore if update fails** para habilitar o recurso de restauração em caso de falha. Para obter detalhes, consulte Restaurar em caso de falha de instalação ou atualização.

Quando estiver pronto, selecione **Install**.

Etapa 10. Diagnóstico

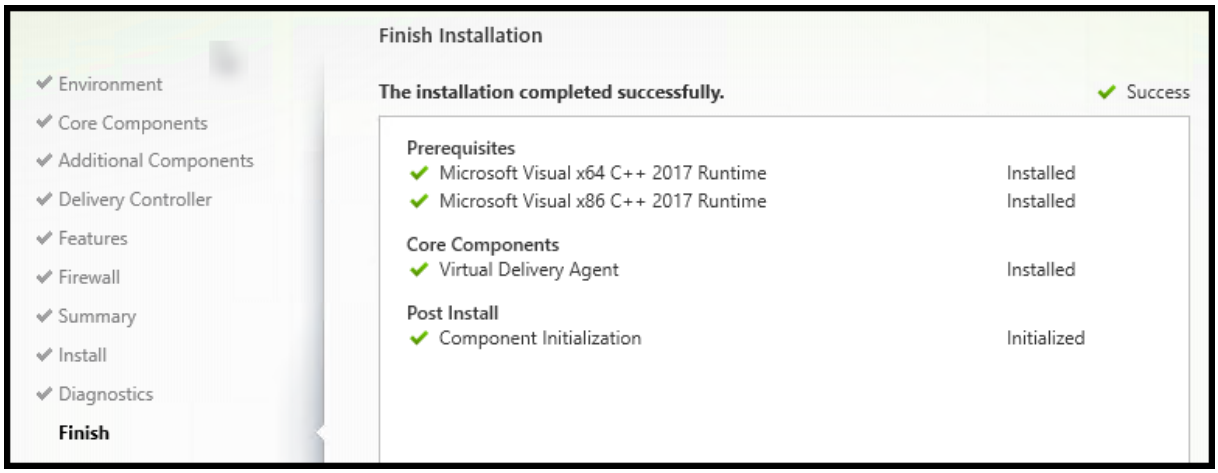


Na página **Diagnostics**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), selecione **Connect**. Quando solicitado, insira as credenciais da sua conta da Citrix.

Depois que suas credenciais forem validadas (ou se você optar por não participar), selecione **Next**.

Para obter mais informações, consulte Call Home.

Etapa 11. Conclua a instalação



A página **Finish** mostra marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com êxito.

Selecione **Finish**. Por padrão, a máquina é reinicializada automaticamente. Embora você possa desativar a reinicialização automática, o VDA não pode ser usado até que a máquina seja reinicializada.

Se você estiver instalando um VDA em máquinas individuais (em vez de uma imagem), repita as etapas acima para instalar um VDA em outras máquinas, conforme necessário.

Solução de problemas

Na exibição **Manage > Full Configuration** de um grupo de entrega, a entrada **Installed VDA version** no painel de detalhes pode não refletir a versão instalada nas máquinas. A exibição 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.

Depois de instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Veja 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 **Customize Virtual Delivery Agent Settings**.

Quando o instalador for iniciado, altere as configurações disponíveis.

Personalizar a porta para a comunicação com os Cloud Connectors

Você pode personalizar a porta que os VDAs usam para se comunicarem com os Cloud Connectors de acordo com os seus requisitos de segurança específicos. Esse recurso é útil se sua equipe de segurança não permitir que a porta padrão (porta 80) seja aberta ou se a porta padrão já estiver em uso.

Para personalizar a porta, conclua as seguintes etapas:

1. Adicione o número da porta do Controller nos Citrix Cloud Connectors.
2. Adicione o número da porta do VDA nos VDAs.

Adicionar o número da porta do Controller nos Citrix Cloud Connectors

Vá para o Citrix Cloud Connector e execute os dois comandos do 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`

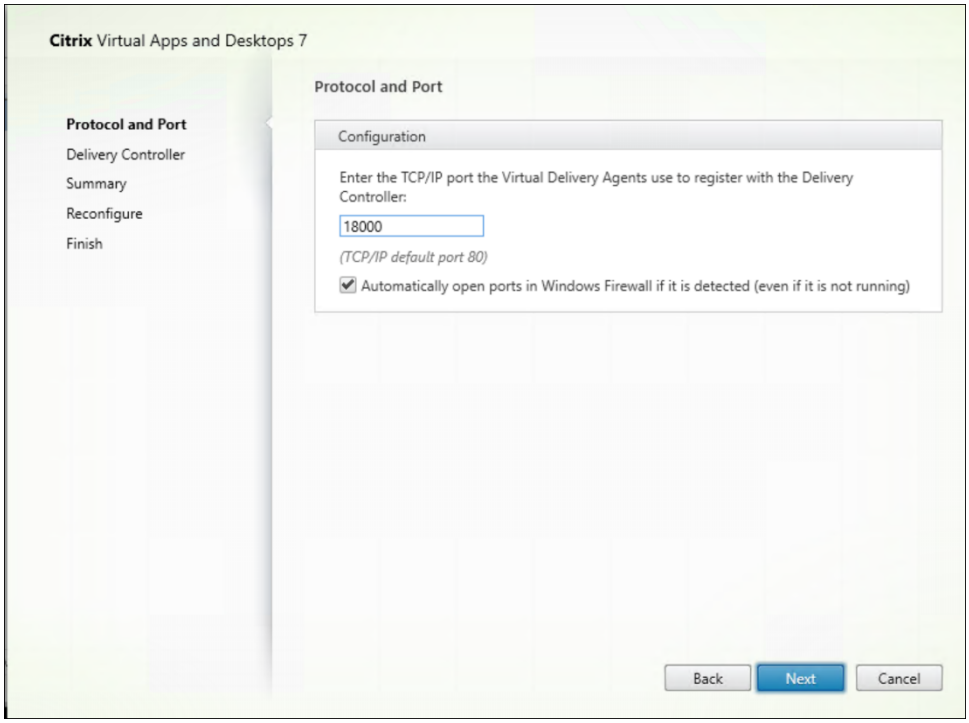
Ao personalizar a porta, considere o seguinte:

- Você deve usar o mesmo número de porta nos dois comandos.
- Você deve executar os dois 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.

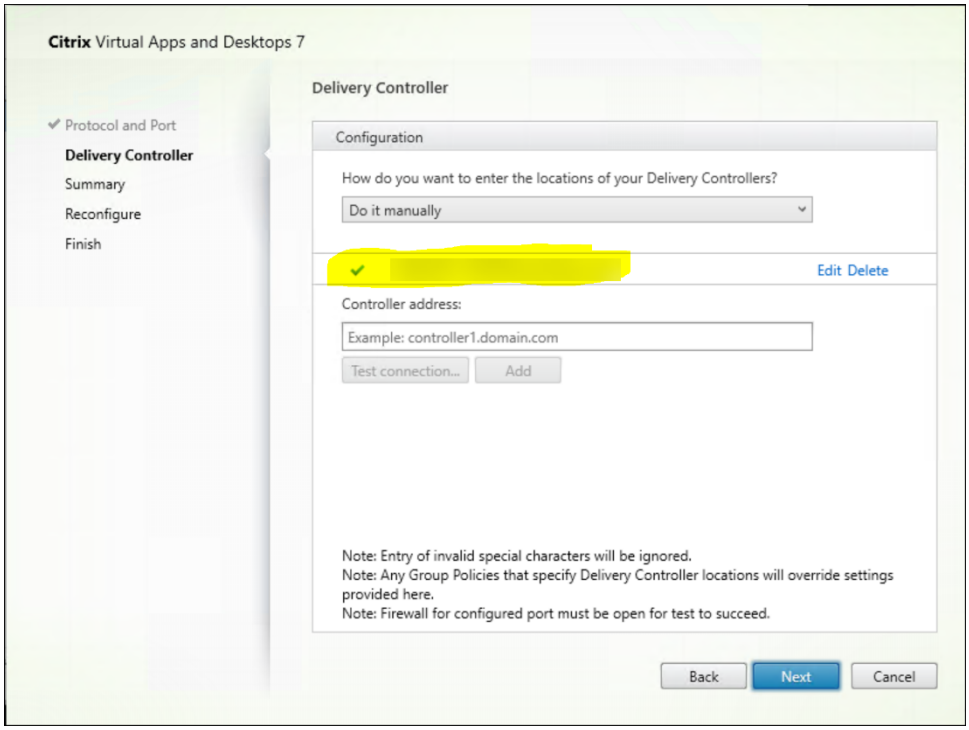
Adicionar o número da porta VDA em VDAs

Instale o VDA com as configurações padrão e configure 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 êxito.

> **Nota:**
>
> Você pode ver a seguinte mensagem de erro ao testar uma conexão do Controller: No running instance of a Controller found on < o endereço do Controller que você forneceu >. Se o endereço estiver correto, você pode ignorar a mensagem.

Solução de problemas

Para verificar se as portas personalizadas estão configuradas corretamente, acesse o Cloud Connector e execute as seguintes etapas da 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 comando a seguir 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 os 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 de seus componentes com o Cloud Health Check.

O que fazer a seguir

Criar catálogos de máquinas.

Para revisar todo o processo de configuração, consulte Planejar e criar uma implantação.

Instalar VDAs usando a linha de comando

June 6, 2023

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, consulte Instalar VDAs para saber mais sobre as 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 em que você está instalando o VDA, conecte-se ao Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. No canto superior direito, clique em **Downloads** e selecione **Download VDA**. Você é redirecionado para a página de download do VDA. Encontre o instalador do VDA desejado e clique em **Download File**.
4. Após a conclusão do download, execute o nome. Use as opções descritas neste artigo.
   - Para o Virtual Delivery Agent de SO multissessão, execute `VDAServerSetup.exe`
   - Para o Virtual Delivery Agent de SO de sessão única, execute `VDAWorkstationSetup.exe`
   - Para o Core Services Virtual Delivery Agent de SO de sessão única, execute `VDAWorkstationCoreSe .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. Do contrário, falhará.) Depois, 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 deixada de lado, somente o VDA será instalado (o aplicativo Citrix Workspace não).

  Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador não pode instalar o aplicativo Citrix Workspace.

- **/controllers** "*controlador* [*controlador*]…"

  FQDNs separados por espaço de Citrix Cloud Connectors com os quais o VDA pode se comunicar, entre aspas retas normais. Não especifique ambas as opções `/site_guid` e `/controllers`.

- **/disableexperiencemetrics**

  Impede o carregamento 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 recursos habilitados (exceto a Assistência Remota do Windows), se o Serviço do Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente. Para obter informações sobre portas, consulte Network ports.

  Para abrir as portas UDP do transporte adaptativo HDX, especifique a opção `/enable_hdx_udp_ports`, além da opção `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Abre portas UDP no firewall do Windows que o transporte adaptativo HDX requer, se o Serviço do Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente. Para obter informações sobre portas, consulte Network ports.

  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**

Ativa ou desativa o uso de UDP para pacotes de áudio (RealTime Audio Transport para áudio). Ativar esse recurso pode melhorar o desempenho do áudio. Inclua a opção `/enable_hdx_ports` se quiser que as portas UDP sejam abertas automaticamente quando o Serviço do Firewall do Windows for detectado.

- **/enable_remote_assistance**

  Habilita o recurso de sombreamento na Assistência Remota do Windows para uso com as funções no **Monitor**. Se você especificar esta opção, a Assistência Remota do Windows abre as portas dinâmicas no firewall.

- **/enablerestore** ou **/enablerestorecleanup**

  (Válido somente para VDAs de sessão única) Permite o retorno automático ao ponto de restauração, se a instalação ou atualização do VDA falhar.

  Se a instalação/atualização for concluída com sucesso:

  - `/enablerestorecleanup` instrui o instalador a remover o ponto de restauração.
  - `/enablerestore` instrui o instalador a manter o ponto de restauração, mesmo que ele não tenha sido usado.

  Para obter detalhes, consulte Restaurar em caso de falha de instalação ou atualização.

- **/enable_ss_ports**

  Abre 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 habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente.

- **/exclude** "*componente*"[,"*componente*"]

  Impede a instalação de um ou mais componentes opcionais separados por vírgula, cada qual entre aspas retas normais. Por exemplo, instalar ou atualizar um VDA em uma imagem gerenciada pelo MCS exige o componente Machine Identity Service. Os valores válidos são:

  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - 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 resolução de problemas de VDAs por meio da

guia **Monitor**. Nas páginas **User details** e **EndPoint**, o painel Personalization e o painel Logon Duration falham. Nas páginas **Dashboard** e **Trends**, o painel Average Logon Duration exibe dados somente para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução Profile Management de terceiros, a Citrix recomenda que você instale e execute o Citrix Profile Management Service. A ativação do Citrix Profile Management Service não é necessária.

Se você planeja usar o MCS para provisionar VMs, não exclua o Machine Identity Service.

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, o componente não é instalado.

Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente muitos destes itens.

- **/h** ou **/help**

  Exibe a ajuda do comando.

- **/includeadditional** "*componente*"[,"*componente*"] …

  Inclui a instalação de um ou mais componentes opcionais separados por vírgula, cada qual entre aspas retas normais. Os nomes dos componentes diferenciam maiúsculas de minúsculas.

  Esta opção é útil quando você estiver criando uma implantação do Remote PC Access e quiser instalar componentes que não estão incluídos por padrão. Os valores válidos são:

  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - Camada de personalização de usuário
  - Ferramenta de registro de VDA Citrix Web Socket

  Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, o componente não é 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*

  Localização 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.

- **/masterimage**

  Válido somente ao instalar um VDA em uma VM. Configura o VDA como uma imagem. Esta opção é equivalente a `/mastermcsimage`.

  Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup.exe`.

- **/mastermcsimage**

  Especifica que a máquina será usada como uma imagem com Machine Creation Services. Esta opção é equivalente a `/masterimage`.

- **/masterpvsimage**

  Especifica que a máquina será usada como uma imagem com o Citrix Provisioning ou com 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 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 será malsucedida. A maioria das edições compatíveis do Windows vem com o Media Foundation já instalado, exceto as edições N.

- **/nodesktopexperience**

  Válido somente ao instalar um VDA com SO multissessão. Impede a ativação do recurso Enhanced Desktop Experience. Esse recurso também é controlado com a configuração de política Enhanced Desktop Experience Citrix.

- **/noreboot**

  Impede uma reinicialização após a instalação. O VDA não pode ser usado até que seja reinicializado.

- **/noresume**

  Por padrão, quando uma reinicialização de máquina é necessária durante uma instalação, o instalador continua automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso é útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/portnumber** *porta*

Válido somente quando a opção `/reconfig` é especificada. Número da porta a ativar para comunicações entre o VDA e o Controller. A porta configurada anteriormente é desabilitada, a menos que seja a porta 80.

- **/proxyconfig** "*endereço ou caminho do arquivo PAC*"

  Válido somente se o comando contiver `/includeadditional "Citrix Rendezvous V2"`. O endereço ou o caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para obter detalhes do recurso, consulte Protocolo Rendezvous.

  - Formato de endereço proxy: `http://<url-or-ip>:<port>`
  - Formato de 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.

- **/reconfigure**

  Personaliza as configurações de VDA definidas anteriormente quando utilizado 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 é iniciada.

- **/remotepc**

  Válido somente para implantações de Remote PC Access (SO de sessão única) ou conexões agenciadas (SO multissessão).

  Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente a instalação destes componentes.

- **/remove_appdisk_ack**

  Autoriza o instalador de VDA a desinstalar o plug-in AppDisks VDA se ele estiver instalado.

- **/remove_pvd_ack**

  Autoriza o instalador de VDA a desinstalar o Personal vDisk se ele estiver instalado.

- **/remove**

  Remove os componentes especificados com a opção `/components`.

- **/removeall**

  Remove o VDA. Ele não remove o aplicativo Citrix Workspace (se instalado).

- **/sendexperiencemetrics**

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.

- **/servervdi**

  Instala um VDA com SO de sessão única em um servidor Windows compatível. Omita esta opção quando instalar um VDA com SO multissessão em um servidor Windows. Antes de usar essa opção, consulte VDI do servidor.

- **/site_guid** *guid*

  Identificador Globalmente Exclusivo da Unidade Organizacional (UO) do Active Directory do site. Associa uma área de trabalho virtual a um site quando você estiver usando o Active Directory para descoberta (a atualização automática é o método de descoberta recomendado e o padrão). O GUID do site é uma propriedade do site exibida em **Manage > Full Configuration**. Não especifique ambas as opções `/site_guid` e `/controllers`.

- **/tempdir** *diretório*

  Diretório para manter os arquivos temporários durante a instalação. Padrão = c:\Windows\Temp.

  Esta opção não está disponível na interface gráfica.

- **/virtualmachine**

  Válido somente 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 fazem com que elas apareçam como máquinas físicas.

  Esta opção não está disponível na interface gráfica.

- **/xendesktopcloud**

  Indica que o VDA está instalado em uma implantação do Citrix DaaS (Citrix Cloud).

Exemplos: instalar um VDA

- **Instalar um VDA em um SO multissesão.** O comando a seguir instala um VDA em um SO multissessão.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  O VDA será usado como uma imagem.

- **Instalar um VDA de SO multissessão ou VDA de SO de sessão única.** O comando a seguir instala um VDA de SO multissessão ou 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 de Delivery Controller por uma vírgula. Observe que `XXXX` representa a versão do VDA.

- **Instale um Core Services VDA em um SO de sessão única.** O comando a seguir instala um Core Services VDA em um SO de sessão única para uso em um Remote PC Access ou implantação de VDA.

```
VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
domain.com"/enable_hdx_ports /noreboot
```

O aplicativo Citrix Workspace e outros serviços não principais não são instalados. O endereço de um Cloud Connector é especificado e as portas no Serviço do 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` (necessário quando personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

O que fazer a seguir

- Criar catálogos de máquinas
- Para revisar todo o processo de configuração, consulte Planejar e criar uma implantação.

Criar e gerenciar conexões

December 6, 2023

Introdução

A configuração de uma conexão inclui a seleção do tipo de conexão entre os hipervisores suportados e os serviços da nuvem e o armazenamento e a rede selecionados nos *recursos* para essa conexão.

Você deve ser um administrador completo para executar tarefas de gerenciamento de conexão e recursos.

Onde encontrar informações sobre tipos de conexão

Os requisitos do sistema listam as versões de hipervisor e serviço de nuvem compatíveis e incluem links para artigos específicos do host.

Armazenamento em host

Um produto de armazenamento é suportado se ele puder ser gerenciado por um hipervisor compatível. O suporte Citrix auxilia esses fornecedores de produtos de armazenamento na solução de problemas e documenta esses problemas no Knowledge Center, conforme necessário.

Ao provisionar máquinas, os dados são classificados por tipo:

- Dados do sistema operacional (SO), que incluem imagens.
- Dados temporários, que incluem todos os dados não persistentes gravados em máquinas provisionadas pelo MCS, arquivos de paginação do Windows, dados de perfil de usuário e quaisquer dados sincronizados com o Content Collaboration (anteriormente ShareFile). Esses dados são descartados cada vez que uma máquina é reinicializada.

Fornecer armazenamento separado para cada tipo de dados pode reduzir a carga e melhorar o desempenho de IOPS em cada dispositivo de armazenamento, fazendo melhor uso dos recursos disponíveis do host. Ele também permite que o armazenamento apropriado seja usado para os diferentes tipos de dados. Persistência e resiliência são mais importantes para alguns dados do que para outros.

- O armazenamento pode ser compartilhado (localizado centralmente, separado de qualquer host, usado por todos os hosts) ou local para um hipervisor. Por exemplo, o armazenamento compartilhado central pode ser um ou mais volumes de armazenamento em cluster do Windows Server 2012 (com ou sem armazenamento conectado) ou um dispositivo de um fornecedor de armazenamento. O armazenamento central também pode fornecer suas próprias otimizações, como caminhos de controle de armazenamento de hipervisor e acesso direto por meio de plug-ins de parceiros.
- Armazenar dados temporários localmente evita a necessidade de atravessar a rede para acessar o armazenamento compartilhado e também reduz a carga (IOPS) no dispositivo de armazenamento compartilhado. O armazenamento compartilhado pode ser mais caro,

portanto, armazenar dados localmente pode reduzir as despesas. Esses benefícios devem 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 centralmente, fornecendo backup e gerenciamento centralizados. Esse armazenamento contém os discos de SO.

Ao selecionar esse método, você pode escolher se deseja usar o armazenamento local (em servidores no mesmo pool do hipervisor) 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 do SO principal. Esse disco é limpo após cada reinicialização de máquina. O disco é acessado através de um cache de memória de gravação. Lembre-se de que, se você usa o armazenamento local para dados temporários, o VDA provisionado estará vinculado ao host de um hipervisor específico. Se o host falhar, a VM não pode ser iniciada.

Exceção: se você usa volumes de armazenamento em cluster (CSV), o Microsoft System Center Virtual Machine Manager não permite 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 tamanho de memória e disco de cache de cada VM ao criar um catálogo de máquinas que usa essa conexão. Contudo, os valores padrão são adaptados ao tipo de conexão e são suficientes para a maioria dos casos.

O hipervisor também pode fornecer tecnologias de otimização através do cache de leitura das imagens de disco localmente. Por exemplo, o Citrix Hypervisor oferece o IntelliCache. Isso também pode reduzir o tráfego de rede para o armazenamento central.

Armazenamento local para o hipervisor

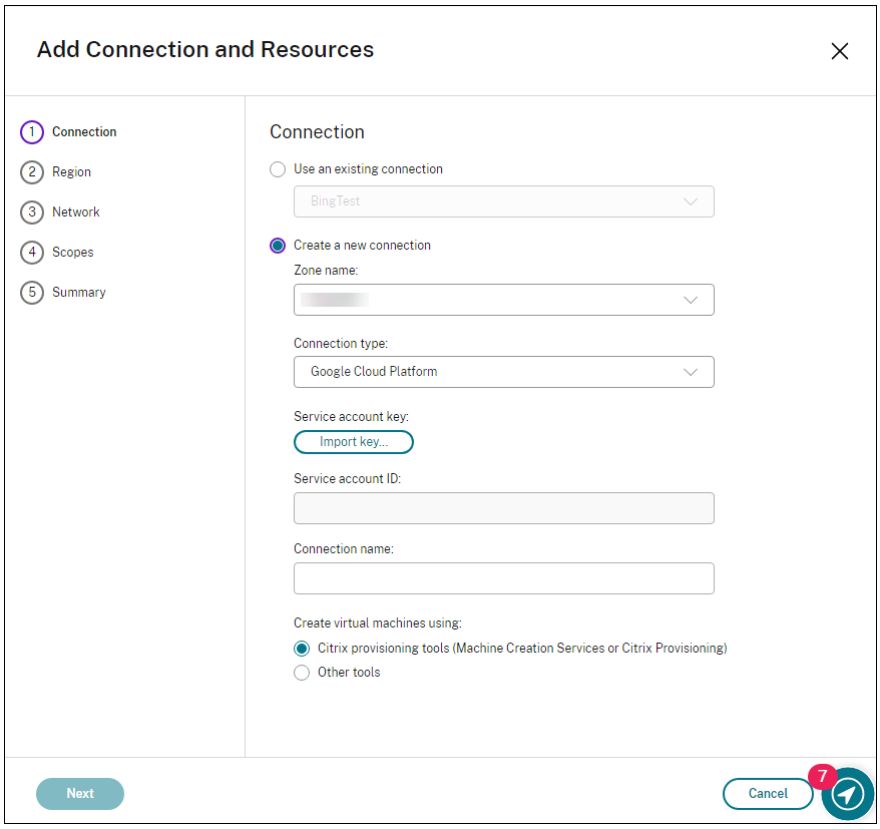
O armazenamento local para o método do hipervisor armazena dados localmente no hipervisor. Com esse método, imagens e outros dados do sistema operacional são transferidos para todos os hipervisores usados no site, tanto para criação inicial da máquina quanto para futuras atualizações de imagem. Isso resulta em tráfego significativo na rede de gerenciamento. A transferência das imagens também é demorada, e as imagens ficam disponíveis para cada host em momentos diferentes.

Criar uma conexão e recursos

> **Importante:**
>
> Os recursos do host (armazenamento e rede) no seu local de recursos devem estar disponíveis antes de criar uma conexão.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
4. Selecione **Add Connections and Resources** na barra de ações.
5. O assistente o orienta pelas páginas a seguir. O conteúdo específico da página depende do tipo de conexão selecionado. Depois de concluir cada página, selecione **Next** até chegar à página **Summary**.

Etapa 1. Conexão



Na página **Connection**:

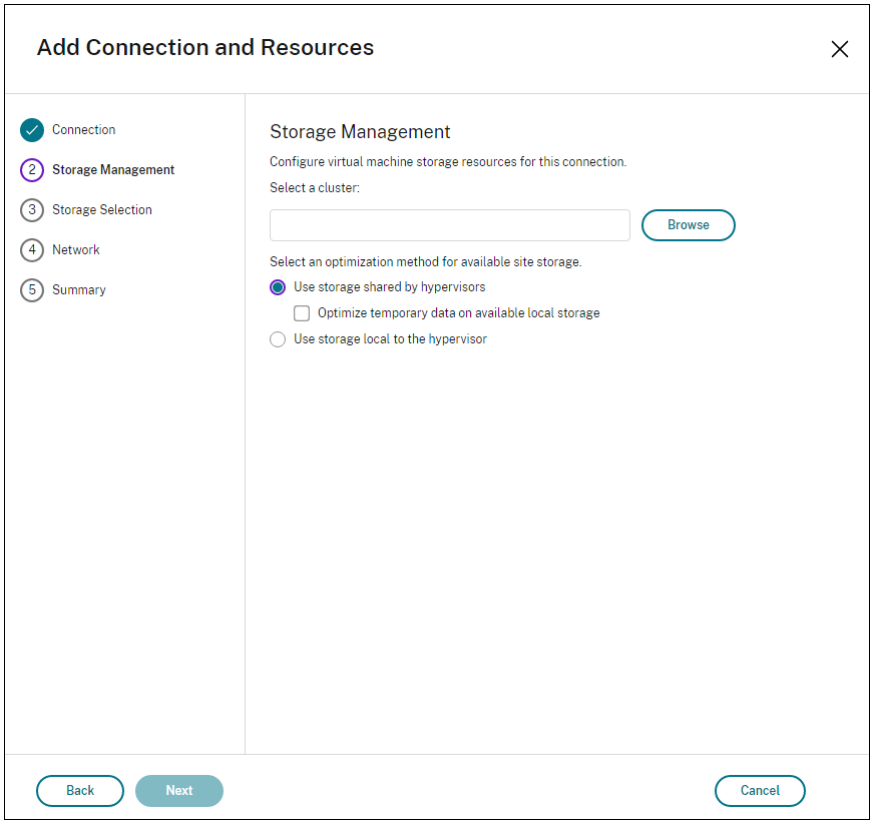
- Para criar uma nova conexão, selecione **Create a new Connection**. Para criar uma conexão com base na mesma configuração de host que uma conexão existente, selecione **Use an existing Connection** e escolha a conexão relevante.

- Selecione uma zona no campo **Zone name**. As opções são todos os locais de recursos que você configurou.
- Selecione um hipervisor ou serviço de nuvem no campo **Connection type**. As opções incluem todos os serviços em nuvem e hipervisores compatíveis com a Citrix:
  - Para um local de recursos sem Cloud Connectors acessíveis, somente hipervisores e serviços em nuvem que oferecem suporte a implantações sem conector estão disponíveis.
  - Para um local de recursos com Cloud Connectors acessíveis, somente hipervisores e serviços em nuvem que tenham seus plug-ins devidamente instalados nesses conectores estão disponíveis.

  Como alternativa, você pode usar o comando `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false ou true do PowerShell para obter a lista de hipervisores e serviços em nuvem disponíveis.
- Digite um nome para a conexão. Esse nome aparece na tela **Manage**.
- Escolha a ferramenta para criar máquinas virtuais: Machine Creation Services ou Citrix Provisioning.

As informações na página **Connection** diferem dependendo do host (tipo de conexão) que você está usando. Por exemplo, ao usar o Azure Resource Manager, você pode usar uma entidade de serviço existente ou criar uma nova. Para obter detalhes, consulte a página do ambiente de virtualização listada em Requisitos do sistema para seu tipo de conexão.

Etapa 2. Gerenciamento de armazenamento



Para obter informações sobre tipos e métodos de gerenciamento de armazenamento, consulte Armazenamento em host.

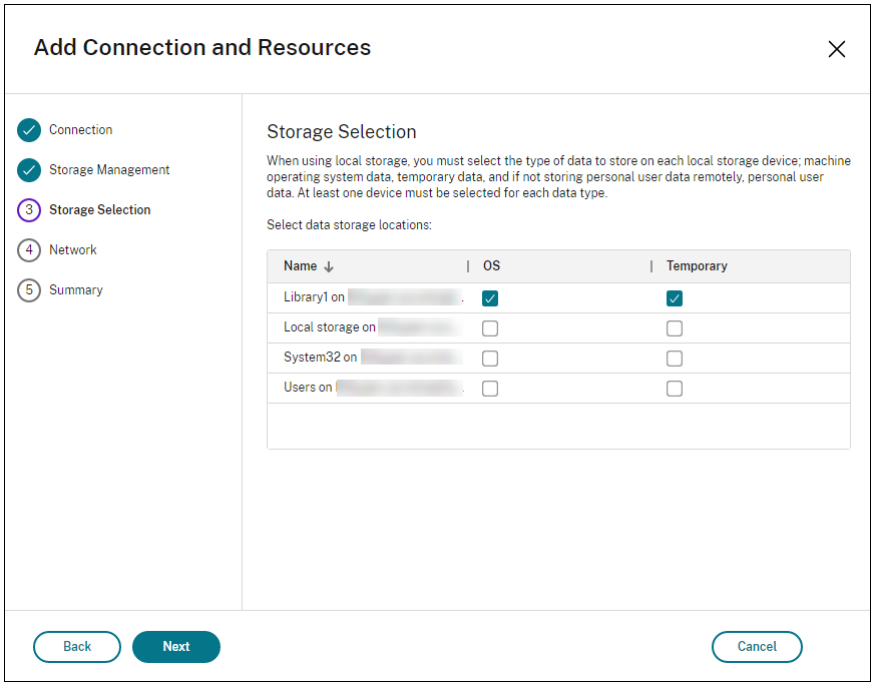
Se você estiver configurando uma conexão a um host Hyper-V ou VMware, navegue até o nome de cluster e selecione-o. Outros tipos de conexão não exigem um nome de cluster.

Selecione um método de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local para o hipervisor.

- Se você escolher armazenamento compartilhado por hipervisores, indique se deseja manter os dados temporários no armazenamento local disponível. (Você pode especificar tamanhos de armazenamento temporário não padrão nos catálogos de máquinas que usam essa conexão.) **Exceção:** ao usar os volumes de armazenamento em cluster (CSV, Clustered Storage Volumes), o Microsoft System Center Virtual Machine Manager não permite que discos de cache de dados temporários sejam criados no armazenamento local. Definir essa configuração de gerenciamento de armazenamento no console **Manage** falha.

Se você usa o armazenamento compartilhado em um pool do Citrix Hypervisor, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Ambientes de virtualização do Citrix Hypervisor.

Etapa 3. Seleção de armazenamento



Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento em host.

Selecione pelo menos um dispositivo de armazenamento de host para cada tipo de dados disponível. O método de gerenciamento de armazenamento selecionado 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 seguir para a próxima página do assistente.

A parte inferior da página **Storage Selection** contém mais opções de configuração se você escolheu o armazenamento compartilhado por hipervisores e habilitou **Optimize temporary data on available local storage**. 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, um dispositivo, como informa a linha "1 storage device selected"). Quando você passa o mouse sobre essa entrada, o nome dos dispositivos selecionados aparece (a menos que nenhum dispositivo esteja configurado).

1. Selecione **Select** para alterar os dispositivos de armazenamento que devem ser usados.
2. Na caixa de diálogo **Select Storage**, marque ou desmarque as caixas de seleção de dispositivos de armazenamento e selecione **OK**.

Etapa 4. Região

(Aparece apenas para alguns tipos de host.) A seleção de região indica onde as VMs serão implantadas. O ideal seria escolher uma região perto de onde os usuários acessarão seus aplicativos.

Etapa 5. Rede

Digite um nome para os recursos. Esse nome aparece no console Manage para identificar a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs usarão.

Alguns tipos de conexão (como o 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, volte para as páginas anteriores do assistente. Ao concluir a revisão, selecione **Finish**.

Lembre-se: se você armazenar dados temporários localmente, poderá configurar valores não padrão para armazenamento temporário de dados ao criar o catálogo que contém máquinas que usam essa conexão.

> **Nota:**
>
> O escopo não é mostrado para administradores com acesso completo. Para obter mais informações, consulte Administradores, funções e escopos.

Editar configurações de conexão

Não use este procedimento para renomear uma conexão ou para criar uma conexão. Essas são operações diferentes. 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.

Não é possível alterar as configurações de GPU de uma conexão, pois os catálogos que acessam esse recurso devem usar uma imagem específica da GPU apropriada. Em vez disso, crie uma nova conexão.

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **Edit Connection** na barra de ações.
3. Siga as instruções para as configurações disponíveis quando editar uma conexão.

4. Quando terminar, selecione **Apply** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Página **Connection Properties**:

- Para alterar o endereço de conexão e as credenciais, selecione **Edit settings…** e insira as novas informações.
- Para especificar os servidores de alta disponibilidade para uma conexão do Citrix Hypervisor, selecione **Edit servers…** e selecione os servidores. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o Citrix Hypervisor se a imagem 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. Para obter mais informações, consulte Criar uma conexão ao Citrix Hypervisor.

Página **Advanced**:

As configurações de limite de aceleração permitem especificar um número máximo de ações de energia permitidas em uma conexão. Essas configurações podem ajudar quando as configurações de gerenciamento de energia permitem que muitas ou poucas máquinas sejam iniciadas ao mesmo tempo. Cada tipo de conexão contém valores padrão específicos que são apropriados para a maioria dos casos. Normalmente, eles não precisam ser alterados.

- As configurações **Simultaneous actions (all types)** e **Simultaneous Personal vDisk inventory updates** especificam dois valores: o número absoluto máximo que pode ocorrer simultaneamente nesta conexão e a porcentagem máxima de todas as máquinas que usam essa conexão. Você deve especificar os valores absoluto e percentual. O limite real aplicado é o menor dos valores.

  Por exemplo, em uma implantação com 34 máquinas, se **Simultaneous actions (all types)** for definido como um valor absoluto de 10 e um valor percentual de 10, o limite real aplicado será 3 (ou seja, 10% de 34 arredondados para o número inteiro mais próximo, que é menor que o valor absoluto de 10 máquinas).
- **Maximum new actions per minute** é um número absoluto. Não há valor percentual.

Página **Shared Tenants**:

Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura dessa conexão. Como resultado, ao criar ou atualizar catálogos, você pode selecionar imagens compartilhadas desses locatários e assinaturas.

- Insira o **ID do aplicativo** e o **segredo do aplicativo** do aplicativo associado a essa conexão. Com essas informações, você pode se autenticar no Azure. Recomendamos que você troque as chaves regularmente para garantir a segurança.
- Especifique locatários compartilhados e assinaturas. Você pode adicionar até oito locatários compartilhados. Para cada locatário, você pode adicionar até oito assinaturas.
- Clique em **Save** e **Apply** quando terminar.

Insira as informações no campo **Connection options** somente sob a orientação de um representante do Suporte Citrix.

Editar redes

Você pode alterar as redes de uma conexão. Faça o seguinte:

1. Vá para **Manage > Full Configuration > Hosting**.
2. Selecione os recursos de destino na conexão e, em seguida, selecione **Edit Network** na barra de ações.
3. Selecione uma ou mais redes para as máquinas virtuais usarem.
4. Clique em **Save** para salvar suas alterações e sair.

Ativar ou desativar o modo de manutenção para uma conexão

Ligar o modo de manutenção para uma conexão impede que qualquer nova ação de energia afete as máquinas armazenadas 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 entra em vigor quando eles fazem logoff.

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão. Para ativar o modo de manutenção, selecione **Turn On Maintenance Mode** na barra de ações. Para desativar o modo de manutenção, selecione **Turn Off Maintenance Mode**.

Você também pode ativar ou desativar o modo de manutenção para máquinas individuais. Você pode ativar ou desativar o modo de manutenção para as 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

> perda de dados. Certifique-se de que seja feito o backup dos dados de usuário nas máquinas afetadas ou que eles não sejam mais necessários.

Antes de excluir uma conexão, certifique-se de que:

- Todos os usuários estão desconectados das máquinas armazenadas na conexão.
- Nenhuma sessão de usuário desconectada está sendo executada.
- O modo de manutenção está ativado para máquinas em pool e dedicadas.
- Todas as máquinas nos catálogos de máquinas usadas pela conexão estão desligadas.

Um catálogo de máquinas torna-se inutilizável quando você exclui uma conexão à qual o catálogo faz referência. Se essa conexão for referenciada por um catálogo, você pode excluir o catálogo. Antes de excluir um catálogo, verifique se ele não é usado por outras conexões.

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **Delete Connection** na barra de ações.
3. Se a conexão tiver máquinas armazenadas nela, você será perguntado se as máquinas devem ser excluídas ou não. Se tiverem que ser excluídas, especifique o que fazer com as contas de computador do Active Directory associadas.

Renomear ou testar uma conexão

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e depois selecione **Rename Connection** ou **Test Connection** na barra de ações.

Exibir detalhes da máquina em uma conexão

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **View Machines** na barra de ações.

O painel superior lista as máquinas acessadas através da conexão. Selecione uma máquina para exibir 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 **Unfold** e depois selecione nas listas de propriedades e operadores.

Gerenciar máquinas em uma conexão

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione uma conexão e selecione **View Machines** na barra de ações.
3. Selecione uma das seguintes opções na barra de ações. Algumas ações não estarão disponíveis, dependendo do estado da máquina e do tipo de host da conexão.

   - **Start:** inicia a máquina se estiver desligada ou suspensa.
   - **Suspend:** pausa a máquina sem desligá-la e atualiza a lista de máquinas.
   - **Shut down:** solicita que o sistema operacional seja desligado.
   - **Force shut down:** força o desligamento da máquina e atualiza a lista de máquinas.
   - **Restart:** solicita que o sistema operacional seja desligado e, em seguida, inicializa a máquina novamente. Se o sistema operacional não conseguir, a área de trabalho permanecerá em seu estado atual.
   - **Enable maintenance mode:** interrompe temporariamente as conexões com uma máquina. Os usuários não podem se conectar a uma máquina nesse estado. Se os usuários estiverem conectados, o modo de manutenção entra em vigor quando eles fazem logoff. (Você também pode ativar ou desativar o modo de manutenção para todas as máquinas acessadas por meio de uma conexão, conforme descrito anteriormente.)
   - **Remove from Delivery Group:** remover uma máquina de um grupo de entrega não a exclui do catálogo de máquinas que o grupo de entrega usa. Você pode remover uma máquina somente quando nenhum usuário está conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver removendo a máquina.
   - **Delete:** quando você exclui uma máquina, os usuários não têm mais acesso a ela, e a máquina é excluída do catálogo de máquinas. Antes de excluir uma máquina, certifique-se de que seja feito o backup de todos os dados de usuário ou que eles não sejam mais necessários. Você pode excluir uma máquina somente quando nenhum usuário está 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 for desligada dentro de 10 minutos, ela será encerrada. Se o Windows tentar instalar atualizações durante o desligamento, existe o risco de a máquina ser encerrada antes que as atualizações sejam concluídas.

Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar os dados pessoais (PvD), temporários e de sistema operacional das VMs que usam uma conexão. Você também pode especificar quais servidores usar para armazenamento de cada tipo de dados.

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **Edit Storage** na barra de ações.
3. No painel esquerdo, selecione o tipo de dados: de sistema operacional ou temporário.
4. Marque ou desmarque as caixas de seleção de 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:

- **In use**: o armazenamento está sendo usado para criar máquinas.
- **Superseded**: o armazenamento está sendo usado apenas para máquinas existentes. Nenhuma nova máquina é adicionada a este armazenamento.
- **Not in use**: o armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo atualmente selecionado como **In use**, seu status será alterado para **Superseded**. As máquinas existentes continuarão a usar esse dispositivo de armazenamento (e podem gravar dados nele). Portanto, esse local pode ficar cheio mesmo depois de deixar de ser usado para criar máquinas.

Excluir, renomear ou testar recursos

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione o recurso e, em seguida, selecione a entrada apropriada na barra de ações: **Delete Resources**, **Rename Resources** ou **Test Resources**.

Detectar recursos órfãos do Azure

Recursos órfãos são recursos não utilizados presentes no sistema e que podem gerar despesas desnecessárias.

Esse recurso permite que você detecte os recursos órfãos do Azure nos hosts do seu site na nuvem.

Siga as etapas no Citrix DaaS:

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione uma conexão e, em seguida, selecione **Detect Orphaned Resources** na barra de ações. A caixa de diálogo **Detect Orphaned Resources** exibe o relatório de recursos órfãos.
3. Para exibir o relatório de recursos órfãos, selecione **View Report**.

Como alternativa, você pode detectar recursos órfãos do Azure usando o PowerShell. Para obter mais informações, consulte Recuperar uma lista de recursos órfãos.

Para entender os motivos por trás dos recursos órfãos e saber como prosseguir, consulte Efficiently manage Orphaned Azure resources with Citrix.

Timers de conexão

Você pode usar configurações de política Citrix para definir três timers de conexão:

- **Maximum connection timer:** determina a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e uma área de trabalho virtual. Use as configurações de política **Session connection timer** e **Session connection timer interval**.
- **Connection idle timer:** determina quanto tempo uma conexão ininterrupta do dispositivo do usuário a uma área de trabalho virtual é mantida se não houver nenhuma entrada pelo usuário. Use as configurações de política **Session idle timer** e **Session idle timer interval**.
- **Disconnect timer**: determina quanto tempo uma área de trabalho virtual desconectada e bloqueada pode permanecer bloqueada antes que seja feito logoff da sessão. Use as configurações de política **Disconnected session timer** e **Disconnected session timer interval**.

Quando você atualizar qualquer uma dessas configurações, assegure que elas sejam consistentes em toda a sua implantação.

Consulte a documentação de configurações de política para obter mais informações.

Recuperar uma lista de recursos órfãos

Você pode obter uma lista de recursos órfãos criados pelo MCS, mas que não são mais monitorados pelo MCS. Para obter a lista, você pode usar os comandos do PowerShell. Você pode filtrar usando conexões.

> **Nota:**
>
> - Atualmente, esse recurso se aplica somente aos ambientes do Azure.
> - O comando do PowerShell é rejeitado se houver um provisionamento ou atualização de imagem em andamento.
> - Um recurso gerenciado pelo cliente marcado com todas as tags Citrix é detectado como um recurso órfão. No entanto, se você adicionar outra tag CitrixDetectIgnore com valor true para esse recurso, o recurso será ignorado ao detectar recursos órfãos.

Limitações:

- Somente um usuário com a função interna Full admin ou um usuário administrador com a função Cloud admin pode executar o comando PowerShell e obter a lista de recursos órfãos.
- 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 em caso de possível carga de trabalho pesada.
- A lista de grupos de recursos órfãos não está disponível no momento.

Para exibir a lista de recursos órfãos:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute os seguintes comandos:

```
$pluginId = 'AzureRmFactory'
$connections = Get-ChildItem xdhyp:\connections | where {
  $_.PluginId -eq $pluginId  }

get-provorphanedresource -HypervisorConnectionUid $connections.
    HypervisorConnectionUid
<!--NeedCopy-->
```

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:

```
$connections = Get-ChildItem xdhyp:\connections | where {
  $_.CustomProperties -match '<subscriptionId>'  }

get-provorphanedresource -HypervisorConnectionUid $connections.
    HypervisorConnectionUid
<!--NeedCopy-->
```

O que fazer a seguir

- Para obter informações sobre a conexão com tipos específicos de host, consulte:
  - Conexão com a AWS
  - Conexão com o Citrix Hypervisor
  - Conexão com ambientes de nuvem do Google
  - Conexão com o Microsoft Azure
  - Conexão com o Microsoft System Center Virtual Machine Manager
  - Conexão com a Nutanix
  - Conexão com soluções de nuvem e parceiros da Nutanix
  - Conexão com o VMware
  - Conexão com soluções de nuvem e parceiros do VMware

Se você estiver no processo de implantação inicial, crie um catálogo de máquinas.

Conexão com a AWS

December 20, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem da AWS.

> **Nota:**
>
> Antes de criar uma conexão com a AWS, você precisa primeiro concluir a configuração da sua conta da AWS como um local de recursos. Consulte Ambientes de nuvem da AWS.

Criar uma conexão

Quando você cria uma conexão a partir da interface Full Configuration:

- Você deve fornecer os valores da chave de API e da chave secreta. Você pode exportar o arquivo de chaves que contém esses valores da AWS e depois importá-los. Você também deve fornecer a região, a zona de disponibilidade, o nome da VPC, os endereços de sub-rede, o nome do domínio, o nome dos grupos de segurança e as credenciais.
- O arquivo de credenciais para a conta raiz da AWS (recuperado do console da AWS) não está formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão da AWS. Portanto, o gerenciamento do Citrix Virtual Apps and Desktops não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Verifique se você está usando os arquivos de credenciais do AWS Identity Access Management (IAM).

> **Nota:**
>
> Depois de criar uma conexão, as tentativas de atualizar a chave de API e a chave secreta podem falhar. Para resolver o problema, verifique as restrições do seu servidor proxy ou do firewall e confirme que o seguinte endereço pode ser contatado: `https://*.amazonaws.com`.

Valores padrão de conexão do host

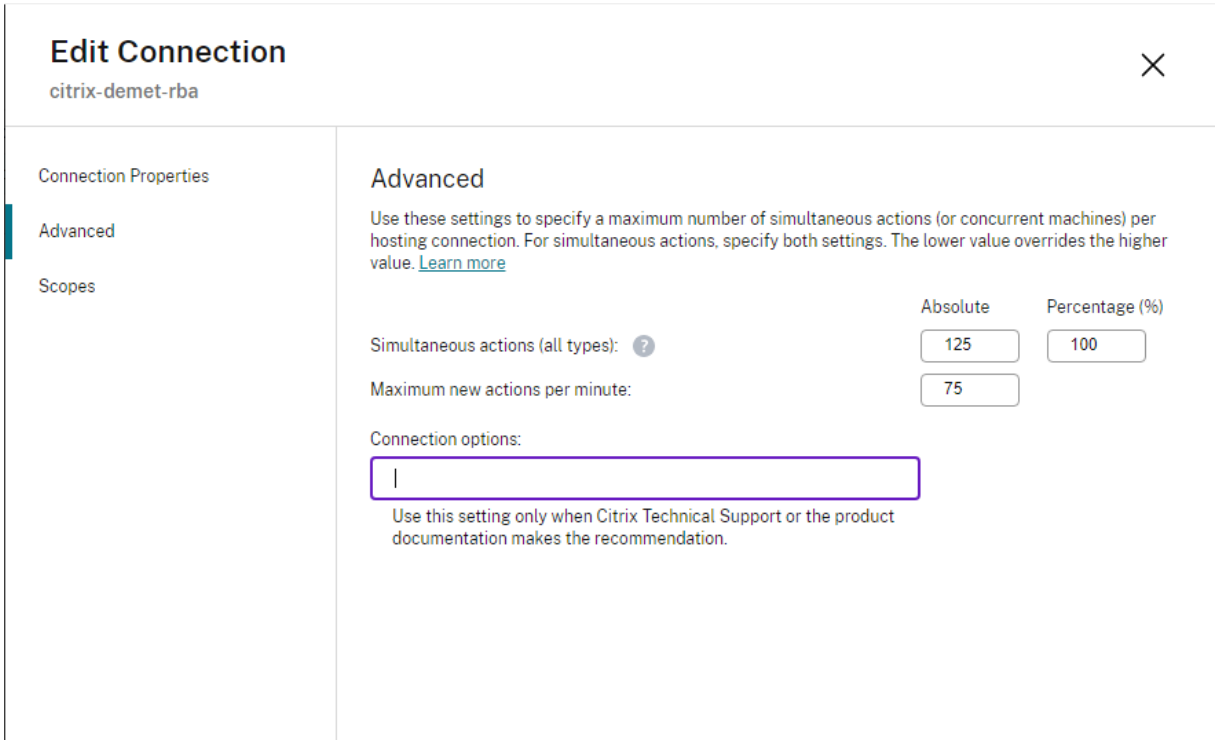
Quando você cria conexões de host na interface Full Configuration de um ambiente de nuvem da AWS, os seguintes valores padrão são exibidos:

Opção	Absoluto	Porcentagem
Ações simultâneas (todos os tipos)	125	100

Opção	Absoluto	Porcentagem
Máximo de novas ações por minuto	125	
Máximo de operações simultâneas de provisionamento	100	

Por padrão, o MCS oferece suporte a 100 operações de provisionamento simultâneas.

Você pode configurar esses valores acessando a seção **Advanced** na tela **Edit Connection** no Citrix Studio.



Por padrão, o MCS oferece suporte a 100 operações simultâneas no máximo. Como alternativa, você pode usar o SDK remoto do PowerShell para definir o número máximo de operações simultâneas ideal para o seu ambiente.

Use a propriedade personalizada do PowerShell, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações simultâneas de provisionamento da AWS.

Antes da configuração:

- Verifique se você instalou o PowerShell SDK for Cloud.
- Confirme que o valor padrão de `MaximumConcurrentProvisioningOperations` é 100.

Execute as seguintes etapas para personalizar o valor `MaximumConcurrentProvisioningOperations`:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Digite `cd xdhyp:\Connections\`.
4. Digite `dir` para listar as conexões.
5. Altere ou inicialize a cadeia de caracteres Custom Properties:
   - Se a cadeia de caracteres Custom Properties tiver um valor, copie o valor de Custom Properties para o Bloco de Notas. Em seguida, altere a propriedade `MaximumConcurrentProvisionin` para o valor de sua preferência. Você pode inserir um valor que varia de 1 a 1000. Por exemplo, `<Property xsi:type="IntProperty"Name="MaximumConcurrentProvis "Value="xyz"/>`.
   - Se a cadeia de caracteres Custom Properties estiver vazia/nula, você deve inicializar a cadeia de caracteres inserindo a sintaxe adequada para o esquema e para a propriedade `MaximumConcurrentProvisioningOperations`.
6. Na janela do **PowerShell**, cole o valor Custom Properties modificado do Bloco de Notas e atribua uma variável à cadeia Custom Properties. Se você inicializou Custom Properties, adicione as linhas abaixo seguindo 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>'.
   ```

   Essa cadeia de caracteres define a propriedade `MaximumConcurrentProvisioningOperations` como 100. Na cadeia de caracteres Custom Properties, você deve definir a propriedade `MaximumConcurrentProvisioningOperations` como um valor que se alinhe às suas necessidades.
7. Digite `Get-XDAuthentication`, o que solicita suas credenciais.
8. Execute `$cred = Get-Credential`, o 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 da AWS.
9. Execute `set-item -PSPath 'XDHyp:\Connections<connection-name>'-CustomProperties $customProperties -username $cred.username -`

`Securepassword $cred.password`. Você deve definir *<connection-name>* com o nome da conexão.

10. Digite `dir` para verificar a cadeia de caracteres CustomProperties atualizada.

URL do ponto de extremidade de serviço

URL do ponto de extremidade do serviço de zona padrão

Quando você usa MCS, uma nova conexão da 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 sobre as zonas suportadas usando a chamada de API do EC2 da AWS: DescribeRegions. A consulta é feita usando uma URL genérica do ponto de extremidade de serviço do EC2: `https://ec2.amazonaws.com/`. Use o MCS para selecionar a zona para a conexão na lista de zonas suportadas. A URL do ponto de extremidade de serviço preferencial da AWS é selecionada automaticamente para a zona. No entanto, depois de criar a URL do ponto de extremidade de serviço, você não pode mais definir ou modificar a URL.

URL do ponto de extremidade de serviço não padrão

Pode haver situações em que não seja necessário ter a URL do ponto de extremidade 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 ponto de extremidade de serviço não padrão. Por exemplo, para criar uma conexão usando a URL do ponto de extremidade de serviço `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configure o Cloud Connector hospedado na AWS e confirme que ele tem 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
<!--NeedCopy-->
```

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 -ZoneUidZoneUid-
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 **Full Configuration > Hosting** para verificar se a conexão do EC2 foi criada.
5. Adicione um local de recursos usando a nova conexão.

Definição de permissões do IAM

Use as informações nesta seção para definir as permissões do IAM para o Citrix DaaS na AWS. O serviço IAM da Amazon permite contas com vários usuários, que podem ser organizados em grupos. Os usuários podem ter permissões diferentes para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões do IAM, consulte 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 do IAM** na lista suspensa.
2. Selecione **Create a New Group of Users**.
3. Digite um nome para o novo grupo de usuários e selecione **Continue**.
4. Na página **Permissions**, selecione **Custom Policy** e **Select**.
5. Digite um nome para a **Permissions policy**.
6. Na seção **Policy Document**, insira as permissões relevantes.

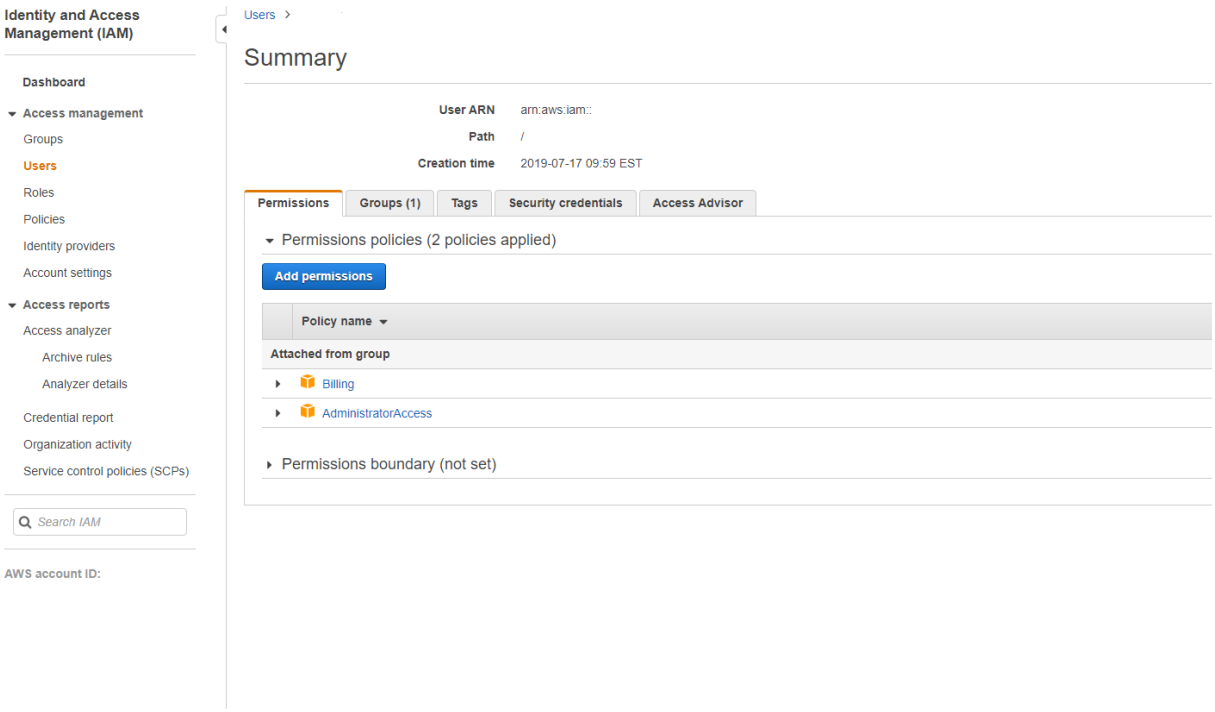
Depois de inserir as informações da política, selecione **Continue** para concluir o grupo de usuários. Os usuários do grupo recebem permissões para executar somente as ações necessárias para o Citrix DaaS.

> **Importante:**
>
> Use o texto de política fornecido no exemplo acima para listar as ações que um Citrix DaaS usa para executar ações em uma conta da 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.

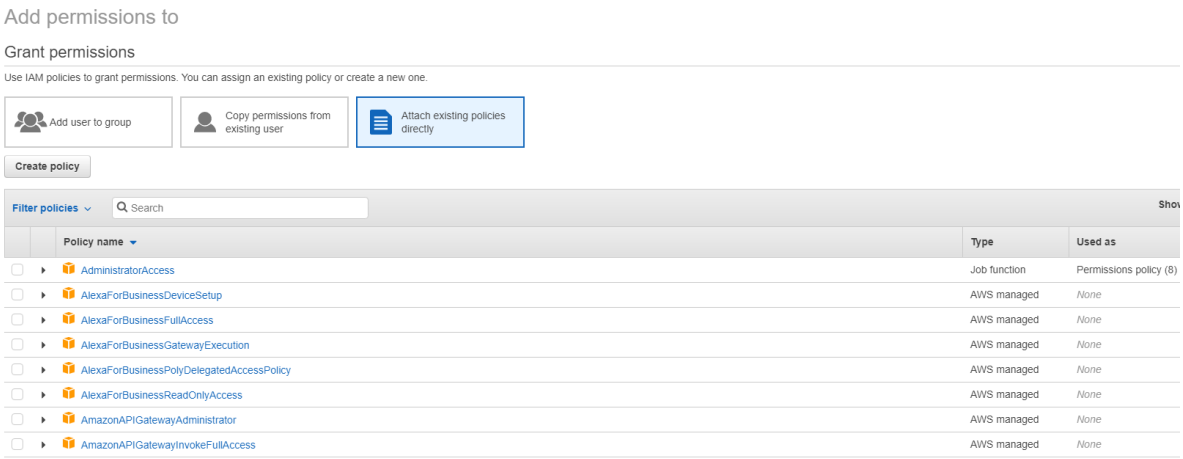
Adicionar permissões do IAM

Defina as permissões na seção **IAM** do AWS Management Console:

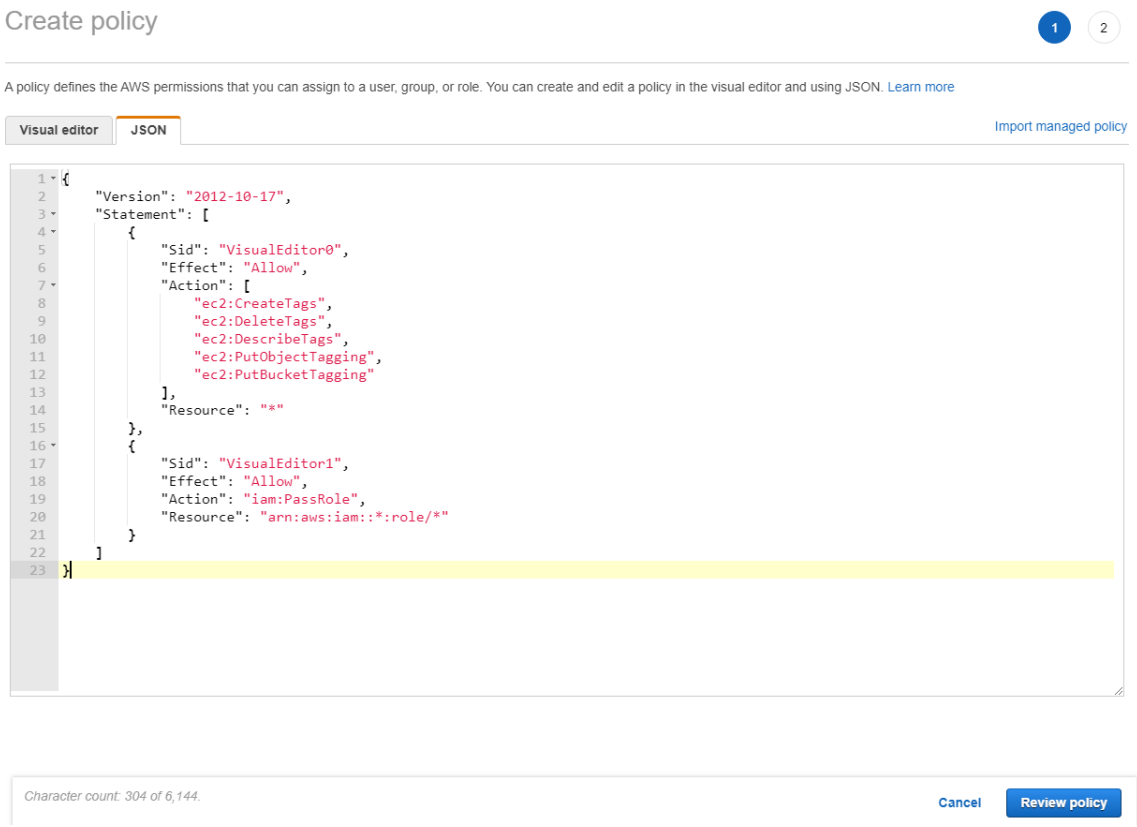
1. No painel **Summary**, selecione a guia **Permissions**.
2. Selecione **Add permissions.**



Na tela **Add Permissions to**, conceda permissões:



Use o seguinte como exemplo na guia **JSON**:



> **Dica:**
>
> O exemplo de JSON observado talvez não inclua todas as permissões para o seu ambiente. Consulte How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS para obter mais informações.

Sobre as permissões da AWS

Esta seção contém a lista completa de permissões da AWS. Use o conjunto completo de permissões, conforme indicado na seção, para que a funcionalidade funcione corretamente.

> **Nota:**
>
> A permissão *iam:PassRole* é necessária somente para **role_based_auth**.

Criar uma conexão de host

Uma nova conexão de host é adicionada usando as informações obtidas na AWS.

```
1  {
2
3      "Version": "2012-10-17",
```



```
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Gerenciamento de energia de VMs

As instâncias de máquina estão ligadas ou desligadas.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```


Criar, atualizar ou excluir VMs

Um catálogo de máquinas é criado, atualizado ou excluído com VMs provisionadas como instâncias da AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "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:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeElasticGpus",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "\*"
         }
```



```
49  ,
50          {
51
52              "Action": [
53                  "ec2:AuthorizeSecurityGroupEgress",
54                  "ec2:AuthorizeSecurityGroupIngress",
55                  "ec2:CreateSecurityGroup",
56                  "ec2:DeleteSecurityGroup",
57                  "ec2:RevokeSecurityGroupEgress",
58                  "ec2:RevokeSecurityGroupIngress"
59              ],
60              "Effect": "Allow",
61              "Resource": "\*"
62           }
63  ,
64          {
65
66              "Action": [
67                  "s3:CreateBucket",
68                  "s3:DeleteBucket",
69                  "s3:PutBucketAcl",
70                  "s3:PutBucketTagging",
71                  "s3:PutObject",
72                  "s3:GetObject",
73                  "s3:DeleteObject",
74                  "s3:PutObjectTagging"
75              ],
76              "Effect": "Allow",
77              "Resource": "arn:aws:s3:::citrix*"
78           }
79  ,
80          {
81
82              "Action": [
83                  "ebs:StartSnapshot",
84                  "ebs:GetSnapshotBlock",
85                  "ebs:PutSnapshotBlock",
86                  "ebs:CompleteSnapshot",
87                  "ebs:ListSnapshotBlocks",
88                  "ebs:ListChangedBlocks",
89                  "ec2:CreateSnapshot"
90              ],
91              "Effect": "Allow",
92              "Resource": "*"
93           }
94
95      ]
96  }
97
98  <!--NeedCopy-->
```


> **Nota:**
>
> - A seção do EC2 relacionada a SecurityGroups só será necessária se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Feito isso, essas permissões não serão necessárias.

Upload e download direto do disco O upload direto do disco elimina o requisito do volume worker para o provisionamento do catálogo de máquinas e, em vez disso, usa APIs públicas fornecidas pela AWS. Essa funcionalidade reduz o custo associado a contas extras de armazenamento e a complexidade para manter as operações do volume worker.

> **Nota:**
>
> O suporte para o volume worker foi preterido.

As seguintes permissões devem ser adicionadas à política:

- ebs:StartSnapshot
- ebs:GetSnapshotBlock
- ebs:PutSnapshotBlock
- ebs:CompleteSnapshot
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ec2:CreateSnapshot
- ec2:DescribeLaunchTemplates

> **Importante:**
>
> - Você pode adicionar uma nova VM aos catálogos de máquinas existentes sem nenhuma operação do volume worker, como volume worker AMI e volume worker VM.
> - Se você excluir um catálogo existente que usava o volume worker antes, todos os artefatos, incluindo os relacionados ao volume worker, serão excluídos.

Criptografia do EBS dos 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 do IAM.

```
1 {
2
3     "Version": "2012-10-17",
4     "Statement": [
```



```
5           {
6
7               "Effect": "Allow",
8               "Action": [
9                    "kms:CreateGrant",
10                   "kms:Decrypt",
11                   "kms:DescribeKey",
12                   "kms:GenerateDataKeyWithoutPlainText",
13                   "kms:GenerateDataKey",
14                   "kms:ReEncryptTo",
15                   "kms:ReEncryptFrom"
16              ],
17              "Resource": "*"
18           }
19
20      ]
21   }
22
23  <!--NeedCopy-->
```

> **Nota:**
>
> As permissões podem ser limitadas a chaves específicas, incluindo um bloco Resource e Condition a critério do usuário. Por exemplo, **Permissões do KMS com condição**:

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": [
9                   "kms:CreateGrant",
10                  "kms:Decrypt",
11                  "kms:DescribeKey",
12                  "kms:GenerateDataKeyWithoutPlainText",
13                  "kms:GenerateDataKey",
14                  "kms:ReEncryptTo",
15                  "kms:ReEncryptFrom"
16             ],
17             "Resource": [
18                 "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                      -456d-a12b-a123b4cd56ef"
19             ],
20             "Condition": {
21
22                 "Bool": {
23
24                     "kms:GrantIsForAWSResource": true
25                  }
26
27              }
```



```
28
29          }
30
31      ]
32  }
33
34 <!--NeedCopy-->
```

A declaração de política de chaves a seguir é a política de chaves padrão completa para chaves do KMS que é necessária para permitir que a conta use políticas do IAM para delegar permissão para todas as ações (kms: *) na chave do KMS.

```
1  {
2
3  "Sid": "Enable IAM policies",
4  "Effect": "Allow",
5  "Principal": {
6
7  "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10 "Action": "kms:",
11 "Resource": ""
12  }
13
14 <!--NeedCopy-->
```

Para obter mais informações, consulte a documentação oficial do AWS Key Management Service.

Autenticação baseada na função do IAM

As seguintes permissões são adicionadas para oferecer suporte à autenticação baseada em função.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5         {
6
7             "Effect": "Allow",
8             "Action": "iam:PassRole",
9             "Resource": "arn:aws:iam::\*:role/\*"
10          }
11
12     ]
13  }
14
15 <!--NeedCopy-->
```


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 o gerenciamento de energia usando essa política.

A política pode ser aplicada aos usuários conforme explicado nas seções Definição de 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 do IAM desejada na instância EC2 do Cloud Connector ao configurar o Cloud Connector. 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 a autenticação baseada em função.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "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:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
```



```
35                  "ec2:DescribeSnapshots",
36                  "ec2:DescribeSubnets",
37                  "ec2:DescribeTags",
38                  "ec2:DescribeSpotInstanceRequests",
39                  "ec2:DescribeInstanceCreditSpecifications",
40                  "ec2:DescribeInstanceAttribute",
41                  "ec2:DescribeElasticGpus",
42                  "ec2:GetLaunchTemplateData",
43                  "ec2:DescribeVolumes",
44                  "ec2:DescribeVpcs",
45                  "ec2:DetachVolume",
46                  "ec2:DisassociateIamInstanceProfile",
47                  "ec2:RebootInstances",
48                  "ec2:RunInstances",
49                  "ec2:StartInstances",
50                  "ec2:StopInstances",
51                  "ec2:TerminateInstances"
52              ],
53              "Effect": "Allow",
54              "Resource": "\*"
55          }
56  ,
57          {
58
59              "Action": [
60                  "ec2:AuthorizeSecurityGroupEgress",
61                  "ec2:AuthorizeSecurityGroupIngress",
62                  "ec2:CreateSecurityGroup",
63                  "ec2:DeleteSecurityGroup",
64                  "ec2:RevokeSecurityGroupEgress",
65                  "ec2:RevokeSecurityGroupIngress"
66              ],
67              "Effect": "Allow",
68              "Resource": "\*"
69          }
70  ,
71          {
72
73              "Action": [
74                  "s3:CreateBucket",
75                  "s3:DeleteBucket",
76                  "s3:DeleteObject",
77                  "s3:GetObject",
78                  "s3:PutBucketAcl",
79                  "s3:PutObject",
80                  "s3:PutBucketTagging",
81                  "s3:PutObjectTagging"
82              ],
83              "Effect": "Allow",
84              "Resource": "arn:aws:s3:::citrix*"
85          }
86  ,
87          {
```



```
88
89              "Action": [
90                  "ebs:StartSnapshot",
91                  "ebs:GetSnapshotBlock",
92                  "ebs:PutSnapshotBlock",
93                  "ebs:CompleteSnapshot",
94                  "ebs:ListSnapshotBlocks",
95                  "ebs:ListChangedBlocks",
96                  "ec2:CreateSnapshot"
97              ],
98              "Effect": "Allow",
99              "Resource": "\*"
100          }
101  ,
102         {
103
104             "Effect": "Allow",
105             "Action": [
106                  "kms:CreateGrant",
107                  "kms:Decrypt",
108                  "kms:DescribeKey",
109                  "kms:GenerateDataKeyWithoutPlainText",
110                  "kms:GenerateDataKey",
111                  "kms:ReEncryptTo",
112                  "kms:ReEncryptFrom"
113             ],
114             "Resource": "\*"
115          }
116  ,
117         {
118
119             "Effect": "Allow",
120             "Action": "iam:PassRole",
121             "Resource": "arn:aws:iam::\*:role/\*"
122          }
123
124     ]
125  }
126
127 <!--NeedCopy-->
```

Nota:

- A seção do EC2 relacionada a SecurityGroups só será necessária se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Feito isso, essas permissões não serão necessárias.
- A seção KMS só é necessária ao usar a criptografia de volume do EBS.
- A seção de permissão iam:PassRole é necessária somente para **role_based_auth**.
- Permissões específicas de 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 permissões ec2:CreateNetworkInterface e ec2:DeleteNetworkInterface somente se você estiver usando o método do volume worker.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas da AWS, consulte Criar um catálogo da AWS.

Mais informações

- Conexões e recursos
- Ambientes de nuvem da AWS

Conexão com o Citrix Hypervisor

January 3, 2023

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

Conexão com ambientes de nuvem do Google

November 21, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Google.

> **Nota:**
>
> Antes de criar uma conexão com os ambientes de nuvem do Google, você precisa primeiro concluir a configuração da sua conta de nuvem do Google como um local de recursos. Consulte Ambientes do Google Cloud.

Adicionar uma conexão

Na interface Full Configuration, siga as orientações em Criar uma conexão e recursos. A descrição a seguir orienta você para configurar uma conexão de hospedagem:

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione **Add Connection and Resources** na barra de ações.
3. Na página **Connection**, selecione **Create a new Connection** e **Citrix provisioning tools**, depois selecione **Next**.
    - **Zone name**. Selecione a zona (equivalente a um local de recursos) em que você deseja que os recursos do host residam. As zonas são criadas automaticamente quando você cria um local de recursos e adiciona um Cloud Connector a ele. Para obter mais informações, consulte Zonas.
    - **Connection type**. Selecione **Google Cloud** no menu.
    - **Service account key**. Importe a chave contida no arquivo de credenciais do Google (.json). Para isso, localize o seu arquivo de credenciais, abra o arquivo com o Bloco de Notas (ou

qualquer editor de texto) e copie o conteúdo. Depois disso, retorne à página **Connection**, selecione **Import key**, cole o conteúdo e selecione **Save**.

- **Service account ID**. O campo é preenchido automaticamente com a informação da chave importada.
- **Connection name**. Digite um nome para a conexão.
- **Route traffic through Citrix Cloud Connectors**. Para rotear as solicitações de API através de um Citrix Cloud Connector disponível, marque essa caixa de seleção. Você também pode marcar a caixa de seleção **Enable Google Cloud Build to use private pools** para obter uma camada adicional de segurança.

  Como alternativa, você pode ativar esse recurso usando o PowerShell. Para obter mais informações, consulte Criar um ambiente seguro para o tráfego gerenciado do GCP.

> **Nota:**
>
> Essa opção está disponível somente quando há Citrix Cloud Connectors ativos em sua implantação. Atualmente, esse recurso não é suportado por Connector Appliances.

4. Na página **Region**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Next**.
5. Na página **Network**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Next**. O nome do recurso ajuda a identificar a combinação de região e rede. As redes virtuais com o sufixo *(Shared)* anexado ao nome representam VPCs compartilhadas. Se você configurar uma função do IAM no nível da sub-rede para uma VPC compartilhada, somente sub-redes específicas da VPC compartilhada aparecem na lista de sub-redes.

   > **Nota:**
   >
   > - O nome do recurso pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )'`).

6. Na página **Summary**, confirme as informações e selecione **Finish** para sair da janela **Add Connection and Resources**.

Depois de criar a conexão e os recursos, a conexão e os recursos que você criou 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 na conexão. Para fazer isso, selecione o recurso na conexão e, em seguida, selecione a opção aplicável na barra de ações.

URLs do ponto de extremidade 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`

Projetos do Google Cloud

Existem basicamente dois tipos de projetos do Google Cloud:

- Projeto de provisionamento: nesse caso, a conta de administrador atual é proprietária das máquinas provisionadas no projeto. Esse projeto também é conhecido como projeto local.
- Projeto de VPC compartilhada: projeto no qual máquinas criadas no projeto de provisionamento usam a VPC do projeto de VPC compartilhada. A conta de administrador usada para provisionar o projeto tem permissões limitadas nesse projeto –especificamente, somente permissões para usar a VPC.

Criar um ambiente seguro para o tráfego gerenciado do GCP

Você só pode permitir o acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aumenta a segurança para manipular dados confidenciais. Para isso:

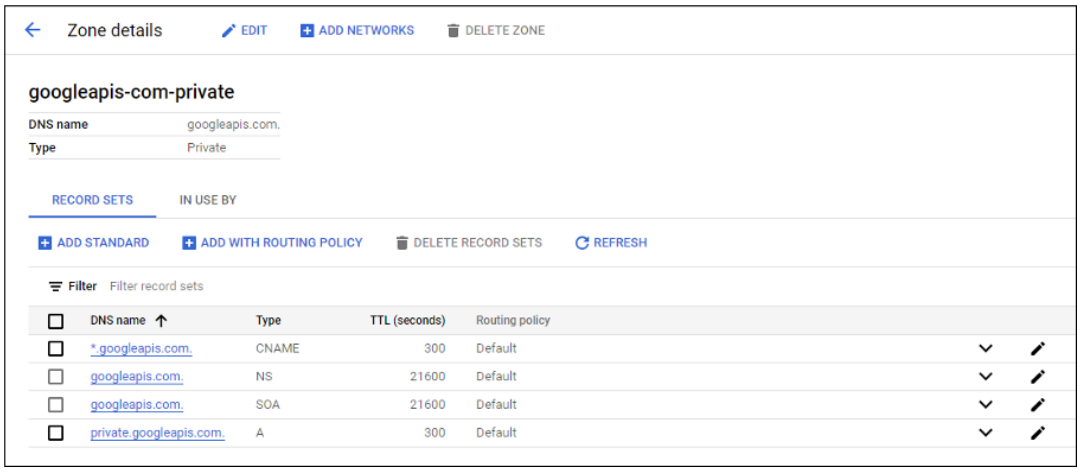
1. Instale os Cloud Connectors na VPC onde você deseja aplicar os controles do serviço VPC. Consulte VPC Service Controls para obter mais informações.
2. Adicione `ProxyHypervisorTrafficThroughConnector` em `CustomProperties` no caso de uma implantação do Citrix Cloud. Se você estiver usando um pool de workers privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter informações sobre o pool de workers privado, consulte Visão geral dos pools privados.

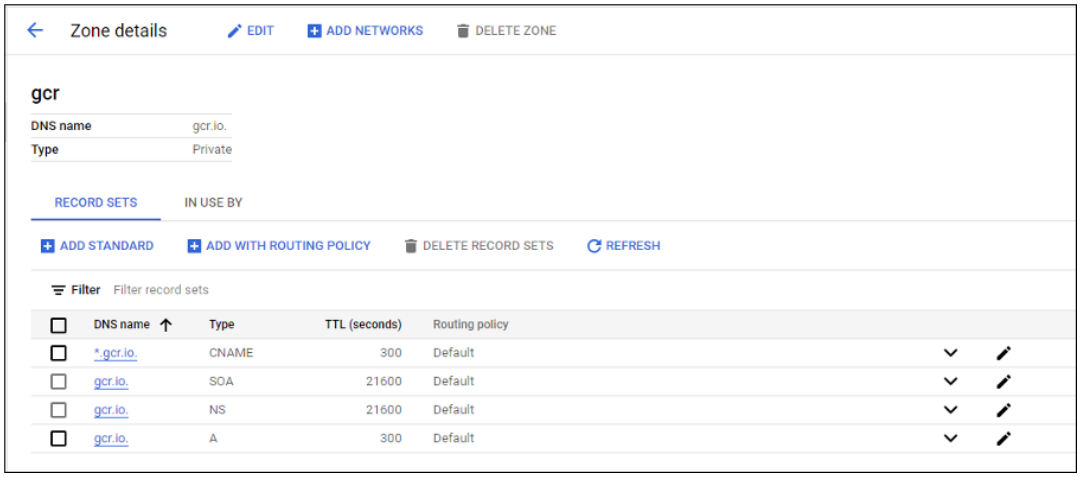
> **Nota:**
>
> Atualmente, esse recurso não é suportado pelo Connector Appliance.

Requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP

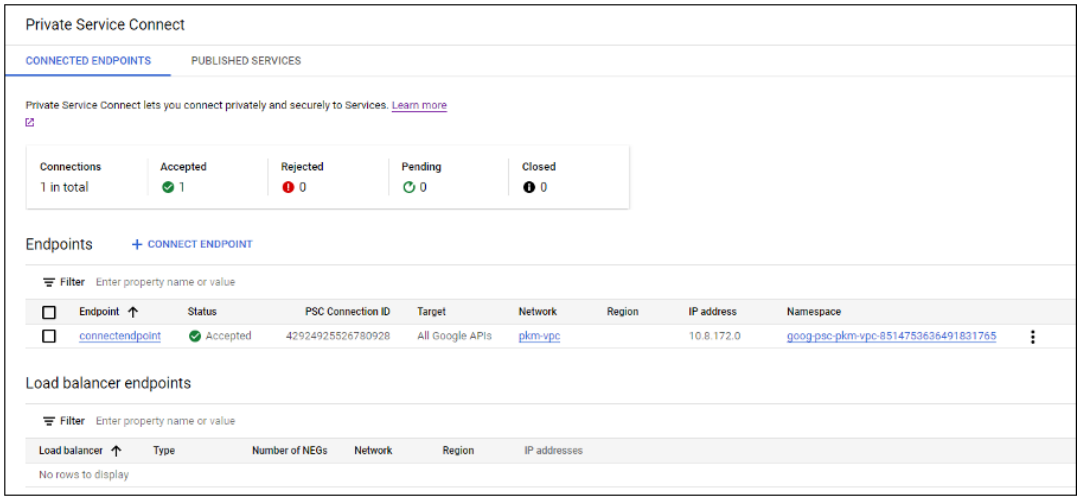
Os requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP são:

- Certifique-se de que a conexão de hospedagem esteja no modo de manutenção ao atualizar as propriedades personalizadas.
- Para usar pools de workers privados, as seguintes alterações são necessárias:
  - Para a conta de serviço do Citrix Cloud, adicione as seguintes funções do IAM:
    - Cloud Build Service Account
    - Compute Instance Admin
    - Service Account User
    - Service Account Token Creator
    - Cloud Build WorkerPool Owner
  - 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 do DNS.

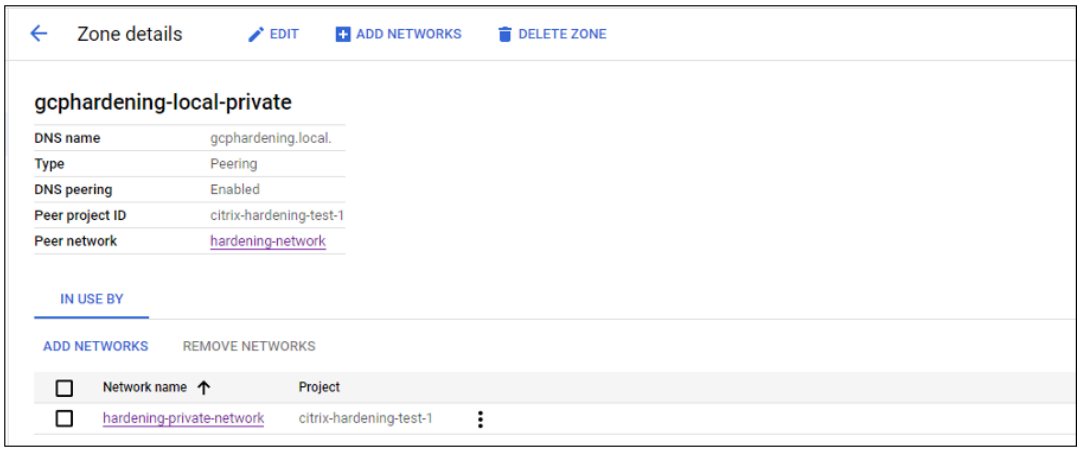




  - Configure a conversão de endereços de rede (NAT) privada ou use a conexão de serviço privada. Para obter mais informações, consulte Acessar APIs do Google por endpoints.



- Se estiver usando uma VPC emparelhada, crie uma zona de peering no Cloud DNS para a VPC emparelhada. Para obter mais informações, consulte Criar uma zona de peering.



- Nos controles de serviço da VPC, configure regras de saída Egress para que as APIs e as VMs possam se comunicar com a Internet. As regras de entrada Ingress são opcionais. Por exemplo:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Habilitar o proxy

Para ativar o proxy, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell a partir do host do Delivery Controller ou use o Remote PowerShell SDK. Para obter mais informações sobre o Remote PowerShell SDK, 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 na nuvem (usando pools públicos): anexe a configuração da propriedade `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` a `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>
     <!--NeedCopy-->
     ```

     Permita a regra de entrada na 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
     <!--NeedCopy-->
     ```

     Para obter informações sobre o perímetro do serviço da VPC, consulte Detalhes e configuração do perímetro de serviço.
   - No caso de um pool de workers privado em uma implantação na nuvem, anexe a configuração da propriedade `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` e `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>` a `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>
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Sobre as permissões do GCP

Esta seção tem a lista completa das permissões do GCP. Use o conjunto completo de permissões, conforme indicado na seção, para que a funcionalidade funcione corretamente.

Criar 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
```



```
8  resourcemanager.projects.get
9  <!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Cloud Datastore User

- Permissões adicionais necessárias para a VPC compartilhada para a conta de serviço do Citrix Cloud no projeto de VPC compartilhada:

```
1  compute.networks.list
2  compute.subnetworks.list
3  resourcemanager.projects.get
4  <!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User

Gerenciamento de energia de VMs

Permissões mínimas necessárias para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
1  compute.instanceTemplates.list
2  compute.instances.list
3  compute.instances.get
4  compute.instances.reset
5  compute.instances.resume
6  compute.instances.start
7  compute.instances.stop
8  compute.instances.suspend
9  compute.networks.list
10 compute.projects.get
11 compute.regions.list
12 compute.subnetworks.list
13 compute.zones.list
14 resourcemanager.projects.get
15 <!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Cloud Datastore User

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.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
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Storage Admin
- Cloud Build Editor
- Service Account User
- Cloud Datastore User

- Permissões adicionais necessárias para a 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
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Cloud Datastore User

- Permissões mínimas exigidas para a conta de serviço Cloud Build no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
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
```



```
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Cloud Build Service Account
- Compute Instance Admin
- Service Account User

- Permissões mínimas exigidas para a conta do serviço 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
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Permissões adicionais necessárias para a VPC compartilhada para a conta de serviço do Cloud Build no projeto de Provisioning exigido pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- 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
<!--NeedCopy-->
```


As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute KMS Viewer

Permissões gerais

A seguir estão as permissões para a conta do Citrix Cloud Service no projeto Provisioning para todos os recursos suportados no MCS. Essas permissões oferecem 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.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
<!--NeedCopy-->
```

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do Google Cloud Platform (GCP), consulte Criar um catálogo

do Google Cloud Platform.

Mais informações

- Conexões e recursos
- Ambientes do Google Cloud.

Conexão com o HPE Moonshot (prévia)

December 6, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos do HPE Moonshot.

> **Nota:**
>
> Antes de criar uma conexão com o HPE Moonshot, você precisa primeiro concluir a configuração da sua conta do HPE. Consulte Ambientes de virtualização do HPE Moonshot.

Criar uma conexão

Você pode criar uma conexão com o HPE Moonshot usando:

- Interface Full Configuration
- Comandos do PowerShell

Criar uma conexão usando a interface Full Configuration

1. Na página **Add Connection and Resources**, selecione **HPE Moonshot** como o tipo de conexão.
2. Digite o endereço de conexão do seu Moonshot iLO Chassis Manager. Você pode usar um endereço IP, nome do host ou FQDN para o endereço.
3. Insira as credenciais administrativas do chassi e um nome de conexão amigável.

A configuração da conexão é interrompida quando ocorre uma das situações:

- O DaaS recebe um certificado assinado pela CA pública com erros: aparece uma mensagem de erro. 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 pela CA privada. Uma página de aviso é exibida. Compare a impressão digital recebida com a do servidor quanto à validade do certificado. Se for válido, selecione **Trust certificate** e clique em **OK** para continuar com a criação da conexão. O DaaS então confiará no certificado e armazenará a impressão digital para validação futura.

Criar uma conexão usando comandos do PowerShell

Ao criar uma conexão usando um comando do 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
<!--NeedCopy-->
```

> **Nota:**
>
> O parâmetro `sslthumbprint` é necessário somente para certificados assinados por CA privada.

Validação de certificado e impressão digital

Para criar uma conexão bem-sucedida com o **HPE Moonshot**, o certificado não deve conter erros e a impressão digital deve ter um valor correto. A seguir estão os casos de uso relacionados à validação do certificado e da impressão digital:

- O certificado assinado pela CA pública tem erros. A conexão não é criada com sucesso. Veja os detalhes do erro e resolva o problema.
- Certificado assinado pela CA pública sem erros. A conexão é criada com sucesso e o valor `SslThumbprints` é **Null**.
- Certificado assinado pela CA privada sem erros e um valor `sslthumbprint`. A conexão é criada com sucesso com um valor `SslThumbprints` correto.
- Certificado assinado pela CA privada com um valor de impressão digital incorreto. A conexão não é criada com sucesso.

- Certificado assinado pela CA privada sem erros. 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

Esta seção detalha como você pode gerenciar conexões:

- Corrigir problemas de certificado usando a interface Full Configuration
- Atualizar o valor da impressão digital 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 nos nós HPE Moonshot associados. Você verá um ícone de erro ao lado da conexão na lista **Host connections**. Consulte a tabela a seguir para problemas e soluções específicos.

Problema	Solução
Ocorre um erro de certificado no certificado assinado pela CA pública	Clique na conexão e selecione a guia **Troubleshoot**. Veja os detalhes do erro e resolva o problema.
O certificado recebido é assinado pela 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 **Edit Connection**. 1. Na página **Connection Properties**, clique em **Edit settings**. 1. Digite a senha para se conectar ao chassi HPE Moonshot e clique em **Save**. 1. Na página **Warning** exibida, compare a impressão digital recebida com a do servidor para verificar a validade do certificado.

Problema	Solução
	1. Se forem iguais, selecione **Trust certificate** e clique em **OK**.

Atualizar o valor da impressão digital

Depois de criar a conexão, você pode atualizar o valor da impressão digital de uma conexão usando o comando `Set-Item` do PowerShell. Por exemplo, execute os seguintes comandos:

1. Obtenha os detalhes da conexão. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

2. Atualize o valor da impressão digital. Por exemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. Verifique o valor atualizado da impressão digital. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> **Nota:**
>
> A atualização falhará se você fornecer um valor de impressão digital incorreto no comando `Set-Item`.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do HPE Moonshot, consulte Criar um catálogo de máquinas do HPE Moonshot.

Mais informações

- Conexões e recursos
- Ambientes de virtualização do HPE Moonshot

Conexão com o Microsoft Azure

November 9, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Azure Resource Manager.

> **Nota:**
>
> Antes de criar uma conexão com o Microsoft Azure, você precisa concluir a configuração da sua conta do Azure como um local de recursos. Consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Criar entidades de serviço e conexões

Antes de criar conexões, você deve configurar as entidades de serviço que as conexões usam para acessar os recursos do Azure. Você pode criar uma conexão de duas maneiras:

- Criar uma entidade de serviço e uma conexão juntas usando Full Configuration
- Criar uma conexão usando uma entidade de serviço criada anteriormente

Esta seção mostra como realizar essas tarefas:

- Criar uma entidade de serviço e uma conexão usando Full Configuration
- 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, fique atento às seguintes considerações:

- A Citrix recomenda usar as entidades de serviço com a função *Colaborador*. No entanto, consulte a seção Minimum permissions para obter a lista de permissões mínimas.
- Ao criar a primeira conexão, o Azure solicita que você conceda as permissões necessárias. Em conexões futuras, ainda será necessário que você se autentique, mas o Azure se lembra do seu consentimento anterior e não exibe o prompt novamente.
- As contas usadas para autenticação devem ser coadministradores da assinatura.
- A conta usada para autenticação deve ser um membro do diretório da assinatura. É preciso distinguir dois tipos de conta: ‘Trabalho ou escola’e ‘conta pessoal da Microsoft’. Veja CTX219211 para obter mais detalhes

- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, pode haver complicações se o usuário tiver recebido anteriormente acesso de convidado a um dos recursos do diretório. Nesse caso, eles podem ter uma entrada de espaço reservado no diretório que não lhes concede as permissões necessárias e é retornado um erro.

  Retifique isso removendo os recursos do diretório e adicionando-os de volta explicitamente. No entanto, use essa opção com cuidado, pois ela tem efeitos não intencionais em outros recursos que essa conta pode acessar.
- Há um problema conhecido em que determinadas contas são detectadas como convidados do diretório quando na verdade são membros. Configurações como essa geralmente ocorrem com contas de diretório estabelecidas mais antigas. Solução alternativa: adicione uma conta ao diretório, que recebe o valor de associação adequado.
- Os grupos de recursos são simplesmente contêineres de recursos e podem conter recursos de regiões diferentes da sua própria região. Isso pode ser confuso se você espera que os recursos exibidos na região de um grupo de recursos estejam disponíveis.
- Sua rede e sub-rede devem ser grandes o suficiente para hospedar o número de máquinas necessárias. Isso requer alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientações sobre a capacidade do espaço de endereço.

Criar uma entidade de serviço e uma conexão usando Full Configuration

> **Importante:**
>
> Esse recurso ainda não está disponível para assinaturas do Azure China.

Em Full Configuration, você pode criar uma entidade de serviço e uma conexão em um único fluxo de trabalho. As entidades de serviço dão às conexões o acesso aos recursos do Azure. Quando você se autentica no Azure para criar uma entidade de serviço, um aplicativo é registrado no Azure. Uma chave secreta (chamada *segredo do cliente* ou *segredo do aplicativo*) é criada para o aplicativo registrado. O aplicativo registrado (nesse caso, uma *conexão*) usa o segredo do cliente para se autenticar no Azure AD.

Antes de começar, verifique se você atende aos seguintes pré-requisitos:

- Você tem uma conta de usuário no locatário do Azure Active Directory da sua assinatura.
- A conta de usuário do Azure AD também é coadministradora da assinatura do Azure que você deseja usar para provisionar recursos.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativos para autenticação. As permissões podem ser revogadas após a criação da conexão com o host. Para obter mais informações sobre funções, consulte Funções internas do Azure AD.

Use o assistente **Add Connection and Resources.** para criar uma entidade de serviço e uma conexão juntas:

1. Na página **Connection**, selecione **Create a new connection**, o tipo de conexão **Microsoft Azure** e seu ambiente do Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Next**.
3. Na página **Connection Details**, crie uma entidade de serviço e defina o nome da conexão da seguinte forma:

   a) Para conceder a permissão de conexão para eliminar automaticamente dispositivos obsoletos ingressados no Azure AD, selecione **Enable Azure AD joined device management**. Recomendamos que você selecione essa opção se quiser criar máquinas ingressados no Azure AD por meio dessa conexão. Para obter mais informações, consulte Habilitar o gerenciamento de dispositivos ingressados no Azure AD.

   b) Insira seu ID de assinatura do Azure e um nome para a sua conexão. Depois de inserir o ID da assinatura, o botão **Create new** será ativado.

   > **Nota:**
   >
   > O nome da conexão pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\/;:#.*?=<>|[]{ } "'()'`.

   a) Selecione **Create new** e insira o nome de usuário e a senha da conta do Azure Active Directory.

   b) Selecione **Sign in**.

   c) Selecione **Accept** para dar ao Citrix DaaS as permissões listadas. O Azure cria uma entidade de serviço que permite ao Citrix DaaS gerenciar recursos do Azure em nome do usuário especificado.

   d) Depois de selecionar **Accept**, você é levado de volta à página **Connection Details**.

   > **Nota:**
   >
   > Depois de autenticar com êxito no Azure, os botões **Create new** e **Use existing** desaparecem. O texto **Connection successful** aparece, com uma marca de seleção verde, indicando a conexão bem-sucedida com sua assinatura do Azure.

   e) Para rotear solicitações de API para o Azure por meio dos Citrix Cloud Connectors, marque a caixa de seleção **Route traffic through Citrix Cloud Connectors**.

   Como alternativa, você pode ativar esse recurso usando o PowerShell. Para obter mais informações, consulte Criar um ambiente seguro para o tráfego gerenciado do Azure.

> **Nota:**
>
> Essa opção está disponível somente quando há Citrix Cloud Connectors ativos em sua implantação. Atualmente, esse recurso não é suportado por Connector Appliances.

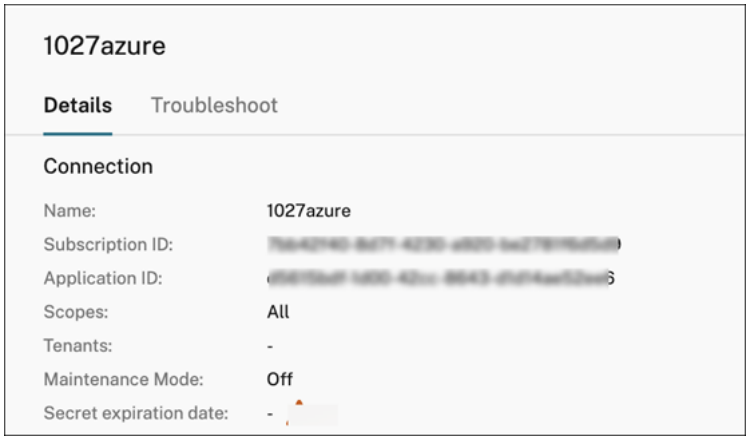
f) Selecione **Next**.

> **Nota:**
>
> Você não pode prosseguir para a próxima página até que você se autentique com êxito no Azure e faça a concessão das permissões necessárias.

4. Configure os recursos para a conexão da seguinte forma:
   - Na página **Region**, selecione uma região.
   - Na página **Network**, 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 fornecerá 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 **Summary**, exiba um resumo das configurações e selecione **Finish** para concluir a configuração.

Exibir o ID do aplicativo Depois de criar uma conexão, você pode ver o ID do aplicativo que a conexão usa para acessar os recursos do Azure.

Na lista **Add Connection and Resources**, selecione a conexão para exibir os detalhes. A guia **Details** mostra a ID do aplicativo.



Criar uma entidade de serviço usando o PowerShell

Para criar uma entidade de serviço usando o PowerShell, conecte-se à sua assinatura do Azure Resource Manager e use os cmdlets do PowerShell fornecidos nas seções a seguir.

Verifique se você tem esses 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 no Azure AD.
- **ApplicationName:** Nome do aplicativo a ser criado no Azure AD.

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 na qual 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
   ```

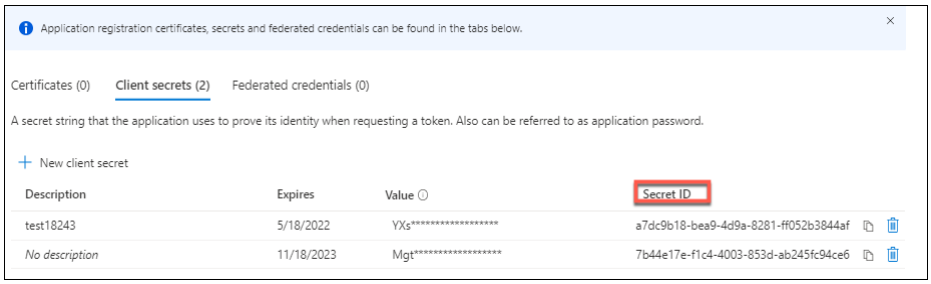

6. Na janela de saída do console do PowerShell, observe o ApplicationId. Você fornece esse ID ao criar a conexão do host.

Obter o segredo do aplicativo no Azure

Para criar uma conexão usando uma entidade de serviço existente, primeiro você deve 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** na interface Full Configuration ou usando o PowerShell.
2. Faça login no portal do Azure.
3. No Azure, selecione **Azure Active Directory**.
4. Em **App registrations** no Azure AD, selecione o seu aplicativo.
5. Acesse **Certificates & secrets**.
6. Clique em **Client secrets**.



Criar uma conexão usando uma entidade de serviço existente

Se você já tem uma entidade de serviço, pode usá-la para criar uma conexão usando Full Configuration.

Verifique se você tem esses 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 **Add Connection and Resources**:

1. Na página **Connection**, selecione **Create a new connection**, o tipo de conexão **Microsoft Azure** e seu ambiente do Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Next**.
3. Na página **Connection Details**, 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 **Use existing**. Na janela **Existing Service Principal Details**, insira as seguintes configurações para a entidade de serviço existente. Depois de inserir os detalhes, o botão **Save** é ativado. Selecione **Save**. Você não pode progredir além desta página até fornecer detalhes válidos.

   - **Subscription ID**. Insira seu ID de assinatura do Azure. Para obter sua ID de assinatura, entre no portal do Azure e navegue até **Subscriptions > Overview**.
   - **ID do Active Directory** (ID do locatário). Insira a ID do Diretório (locatário) do aplicativo que você registrou no Azure AD.
   - **Application ID**. Insira a ID do aplicativo (cliente) do aplicativo que você registrou no Azure AD.
   - **Application secret**. Insira uma chave secreta (segredo do cliente). O aplicativo registrado usa a chave para autenticar no Azure AD. Recomendamos que você altere as chaves regularmente por motivos de segurança. Lembre-se de salvar a chave porque você não poderá recuperá-la mais tarde.
   - **Secret expiration date**. Insira a data após a qual o segredo do aplicativo expira. Você recebe um alerta no console antes que a chave secreta expire. No entanto, se a chave secreta expirar, você receberá erros.

     > **Nota:**
     >
     > Por motivos de segurança, o período de expiração não pode ser superior a dois anos a partir de agora.

   - **Authentication URL**. Esse campo é preenchido automaticamente e não é editável.
   - **Management URL**. Esse campo é preenchido automaticamente e não é editável.
   - **Storage suffix**. Esse campo é preenchido automaticamente e não é editável.

     O acesso aos seguintes pontos de extremidade é necessário para criar um catálogo MCS no Azure. O acesso a esses pontos de extremidade 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/. Essa é uma URL de solicitação das APIs do provedor do Azure Resource Manager. O ponto de extremidade 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./. O (*) é um caractere curinga para o sufixo de armazenamento. Por exemplo, https://demo.table.core.windows.net/.

5. Depois de selecionar **Save**, você é levado de volta à página **Connection Details**. Selecione **Next** para prosseguir para a próxima página.
6. Configure os recursos para a conexão da seguinte forma:
   - Na página **Region**, selecione uma região.
   - Na página **Network**, 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 fornecerá 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 **Summary**, exiba um resumo das configurações e selecione **Finish** para concluir a configuração.

Gerenciar entidades de serviço e conexões

Esta seção detalha como você pode gerenciar as entidades de serviço e conexões:

- Definir as configurações de limitação do Azure
- Habilitar o gerenciamento de dispositivos ingressados no Azure AD
- Habilitar o compartilhamento de imagens no Azure
- Adicionar locatários compartilhados a uma conexão usando Full Configuration
- Implementar o compartilhamento de imagens usando o PowerShell
- Criar um ambiente seguro para o tráfego gerenciado do Azure
- Gerenciar o segredo do aplicativo e data de expiração do segredo

Definir as configurações de limitação do Azure

O Azure Resource Manager controla as solicitações de assinaturas e locatários, roteando o tráfego com base em limites definidos, adaptados às necessidades específicas do provedor. Consulte Throttling Resource Manager requests 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 com muitas máquinas pode ter problemas de desempenho relacionados a operações de energia.

> **Dica:**
>
> Para obter mais informações, consulte Improving Azure performance with Machine Creation Services.

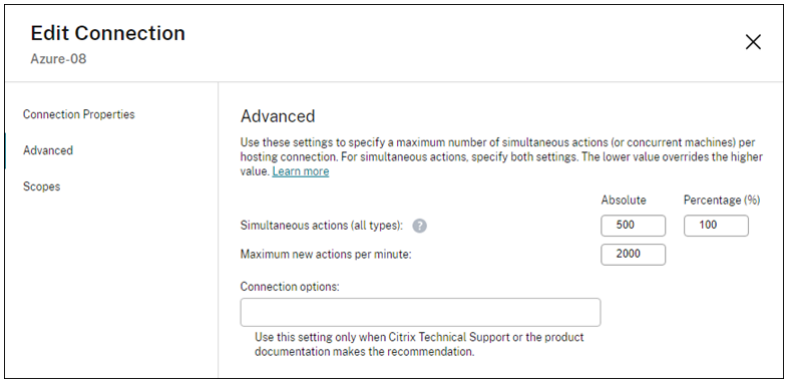
Para ajudar a mitigar esses problemas, o Citrix DaaS permite que você remova a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

Recomendamos as seguintes configurações ideais ao ativar ou desativar VMs em assinaturas grandes, por exemplo, aquelas que contêm 1.000 VMs:

- Operações simultâneas absolutas: 500
- Máximo de novas operações por minuto: 2000
- Simultaneidade máxima de operações: 500

Use a interface Full Configuration para configurar as operações do Azure para uma determinada conexão de host:

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione uma conexão relacionada ao Azure para editá-la.
3. No assistente **Editar conexão**, selecione **Avançado**.
4. Na página **Advanced**, 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.



Por padrão, o MCS oferece suporte a 500 operações simultâneas no máximo. Como alternativa, você pode usar o SDK remoto do PowerShell para definir o número máximo de operações simultâneas.

Use a propriedade **PowerShell**, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações simultâneas de provisionamento do Azure. Ao usar essa propriedade, leve em consideração:

- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` por meio do comando do PowerShell `Set-item`.

Habilitar o gerenciamento de dispositivos ingressados no Azure AD

Dispositivos ingressados no Azure AD obsoletas no Azure podem impedir que novas máquinas ingressem no Azure AD, fazendo com que funcionem incorretamente. Para evitar possíveis problemas, você pode conceder permissão de conexões para gerenciar os dispositivos ingressados no Azure AD. Com essa permissão, as conexões podem eliminar automaticamente os dispositivos obsoletos ingressados no Azure AD.

> **Nota:**
>
> Os dispositivos ingressados no Azure AD não podem ser excluídos do Azure AD quando você exclui máquinas ou catálogos de máquinas.

1. Em **Manage > Full Configuration**, selecione Hosting no painel esquerdo.
2. Selecione a conexão e selecione **Edit Connection** na barra de ações.
3. Selecione **Connection Properties** no painel esquerdo.
4. Na página **Connection Properties** exibida, siga estas etapas:
   a) Selecione **Enable Azure AD joined device management**.
   b) Clique em **Salvar**.
   c) Na janela de login do Azure exibida, insira sua senha de assinatura e clique em **Sign in**.

      Depois que o login for concluído, você será levado de volta à lista de conexões e recursos de hospedagem. Clique na conexão na lista e, em seguida, clique na guia **Details** no painel inferior. Você pode ver que o campo **Azure AD joined device management** mostra **Enabled**.

Ao habilitar o gerenciamento de dispositivos ingressados no Azure AD com Full Configuration, você deve se autenticar no Azure AD, independentemente do método de criação de conexão de host escolhido (criar uma nova ou usar a existente). A função **Cloud Device Administrator** interna do Azure AD é atribuída à entidade de serviço. Para adotar as permissões mínimas de dispositivos ingressados no Azure AD para gerenciamento, você pode remover manualmente a atribuição da função **Cloud Device Administrator** da entidade de serviço e criar uma função personalizada do Azure AD que inclua apenas as permissões mínimas e atribuí-la à entidade de serviço.

> **Nota:**
>
> - As permissões mínimas para o gerenciamento de dispositivos ingressados no Azure AD são as permissões do Azure AD e não as permissões do Azure Resource Manager. Elas não podem ser explicitamente atribuídas a uma entidade de serviço. Você deve criar uma função personalizada no Azure AD que inclua essas permissões e atribuí-la à entidade de serviço. Consulte Criar e atribuir uma função personalizada no Azure Active Directory para obter detalhes.
> - Para criar uma função personalizada no Azure AD, você precisa da licença P1 ou P2 do Azure AD Premium.

Habilitar o compartilhamento de imagens no Azure

Ao criar ou atualizar catálogos de máquinas, você pode selecionar imagens compartilhadas de diferentes locatários do Azure e assinaturas (compartilhadas através da Galeria de Computação do Azure). Para habilitar o compartilhamento de imagens dentro ou entre locatários, você deve aplicar as configurações necessárias no Azure:

- Compartilhar imagens com um locatário (entre assinaturas)
- Compartilhar imagens entre locatários

Compartilhar imagens com um locatário (entre assinaturas) Para selecionar uma imagem na Galeria de Computação do Azure que pertença a uma assinatura diferente, a imagem deve ser compartilhada com a entidade de serviço (SPN) dessa assinatura.

Por exemplo, se houver uma entidade de serviço (SPN 1) configurada no Studio como:

Entidade de serviço: SPN 1

Assinatura: subscription 1

Locatário: tenant 1

A imagem está em uma assinatura diferente, configurada no Studio como:

Assinatura: subscription 2

Locatário: tenant 1

Se você quiser compartilhar a imagem em subscription 2 com subscription 1 (SPN 1), vá para subscription 2 e compartilhe o grupo de recursos com SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em função (RBAC) do Azure. O Azure RBAC é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o Azure RBAC, consulte o documento da Microsoft

O que é o RBAC do Azure (controle de acesso baseado em função do Azure)?. Para conceder acesso, você atribui funções às entidades de serviço no escopo do grupo de recursos com a função de Colaborador. Para atribuir funções do Azure, você deve ter 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 a Galeria de Computação do Azure, crie um registro de aplicativo.

Por exemplo, se houver dois locatários (locatário 1 e locatário 2) e você quiser compartilhar sua galeria de imagens com Tenant 1:

1. Crie um registro de aplicativo para Tenant 1. Para obter mais informações, consulte Criar o registro do aplicativo.
2. Dê ao Tenant 2 acesso ao aplicativo solicitando um login usando um navegador. Substitua `Tenant2 ID` pelo ID do locatário Tenant 1. Substitua `Application (client)ID` pelo ID do aplicativo do registro de aplicativo que você criou. Quando terminar de fazer as substituições, cole a URL em um navegador e siga as instruções de login para entrar no Tenant 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
   <!--NeedCopy-->
   ```

   Para obter mais informações, consulte Dar acesso ao locatário 2.
3. Dê ao aplicativo acesso ao grupo de recursos em Tenant 2. Faça login como Tenant 2 e dê ao registro do aplicativo acesso ao grupo de recursos que tem a imagem da galeria. Para obter mais informações, consulte Autenticar solicitações entre locatários.

Adicionar locatários compartilhados a uma conexão usando Full Configuration

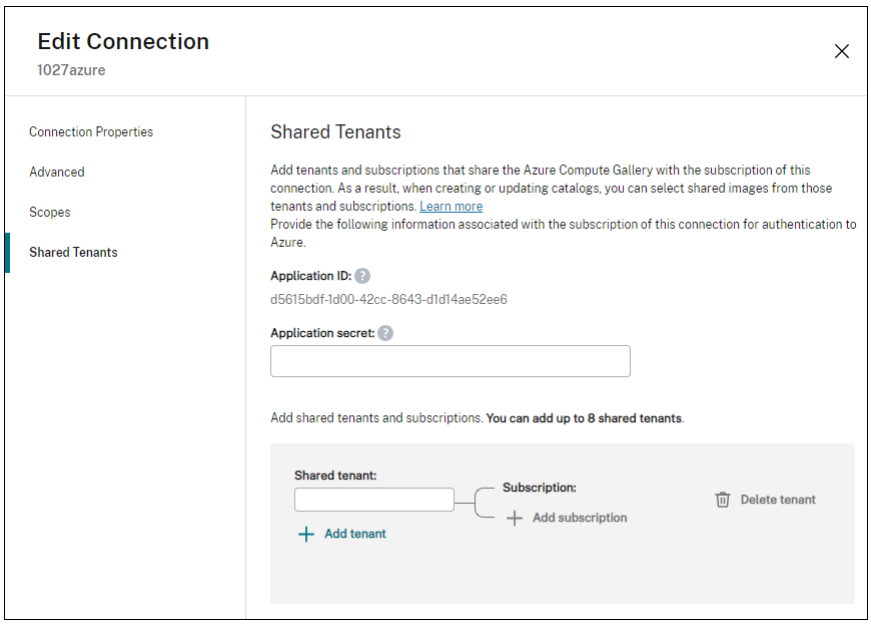
Ao criar ou atualizar catálogos de máquinas na interface Full Configuration, você pode selecionar imagens compartilhadas de diferentes locatários do Azure e assinaturas (compartilhadas através da Galeria de Computação do Azure). O recurso exige que você forneça informações compartilhadas de locatário e assinatura para as conexões de host associadas.

> **Nota:**
>
> Verifique se você definiu as configurações necessárias no Azure para permitir o compartilhamento de imagens entre locatários. Para obter mais informações, consulte Compartilhar

> imagens entre locatários.

Siga estas etapas para a conexão:

1. Em **Manage > Full Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **Edit Connection** na barra de ações.



3. Em **Shared Tenants**, faça o seguinte:
   a) Forneça o ID do aplicativo e o segredo do aplicativo associado à assinatura da conexão. O DaaS usa essas informações para se autenticar no Azure AD.
   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 **Apply** 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 orienta você nos processos de compartilhamento de imagens usando o PowerShell:

- Selecionar uma imagem de uma assinatura diferente
- Atualizar propriedades personalizadas da conexão de hospedagem com IDs de locatários 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 pertença 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, a 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"
<!--NeedCopy-->
```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados da assinatura compartilhada.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription"
<!--NeedCopy-->
```

4. Selecione um grupo de recursos e liste todas as galerias do grupo de recursos.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Selecione uma galeria e liste todas as definições de imagem da galeria.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Selecione uma definição de imagem e liste todas as versões da definição de imagem.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\sigtestdef.imagedefinition"
<!--NeedCopy-->
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Atualizar propriedades personalizadas da conexão de hospedagem com IDs de locatários compartilhados Use `Set-Item` para atualizar as propriedades personalizadas da conexão de hospedagem com IDs de locatário e IDs de assinatura compartilhados. 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"] }
 ]
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

> **Nota:**
>
> Você pode adicionar mais de um locatário. Cada locatário pode ter mais de uma assinatura.

Selecionar uma imagem de um locatário diferente Você pode selecionar uma imagem na Galeria de Computação do Azure que pertença a um locatário do Azure diferente 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. Liste todas as assinaturas compartilhadas.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
<!--NeedCopy-->
```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados da assinatura compartilhada.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Selecione um grupo de recursos e liste todas as galerias do grupo de recursos.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Selecione uma galeria e liste todas as definições de imagem da galeria.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Selecione uma definição de imagem e liste todas as versões da definição de imagem.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Criar um ambiente seguro para o tráfego gerenciado do Azure

O MCS permite que o tráfego de rede (chamadas de API do Citrix Cloud para o hipervisor do Azure) seja roteado através de Cloud Connectors no 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 as políticas do Azure para ter acesso ao disco privado aos discos gerenciados do Azure.

Se você configurar a política do Azure para criar Acessos ao disco automaticamente para cada novo disco para usar pontos de extremidade privados, você não poderá carregar ou baixar mais de cinco discos ou instantâneos ao mesmo tempo com o mesmo objeto de acesso ao disco 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 ao disco automaticamente para cada novo disco para usar pontos de extremidade privados, o limite de cinco operações simultâneas não será imposto.

> **Nota:**
>
> Atualmente, esse recurso não é suportado pelo Connector Appliance.

Limitações Devido à limitação do Azure, esse recurso atualmente não é suportado quando os discos gerenciados têm criptografia no lado do servidor com chaves gerenciadas pelo cliente. Para outras limitações relacionadas, consulte Restringir o acesso de importação/exportação a discos gerenciados usando o Link Privado do Azure.

Para obter mais informações sobre criptografia no lado do servidor, consulte Criptografia do servidor do Azure.

Habilitar o proxy Para ativar o proxy, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell usando o SDK do Remote PowerShell. Para obter mais informações, consulte https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Execute os seguintes comandos:
   a) `Add-PSSnapin citrix*`.
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copie `CustomProperties` da conexão para um bloco de notas e anexe a configuração da propriedade `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThrou "Value="True"/>` a `CustomProperties` para ativar 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>
<!--NeedCopy-->
```

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>'
<!--NeedCopy-->
```

5. Execute `$cred = Get-Credential`. Se solicitado, forneça as credenciais de conexão. As credenciais são ID e segredo do Aplicativo Azure.

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 ausente, substitua todas as aspas duplas (“) pelo sinal de crase seguido por 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>
<!--NeedCopy-->
```

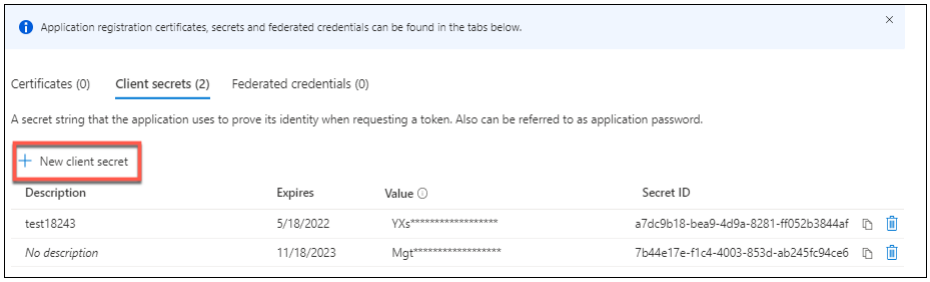
7. Execute `dir` para verificar as configurações `CustomProperties` atualizadas.

Gerenciar o segredo do aplicativo e data de expiração do segredo

Certifique-se de alterar o segredo do aplicativo para uma conexão antes que o segredo expire. Você recebe um alerta na interface Full Configuration antes que a chave secreta expire.

Criar um segredo de aplicativo no Azure Você pode criar um segredo de aplicativo para uma conexão por meio do portal do Azure.

1. Selecione **Azure Active Directory**.
2. Em **App registrations** no Azure AD, selecione o seu aplicativo.
3. Acesse **Certificates & secrets**.
4. Clique em **Client secrets > New client secret**.



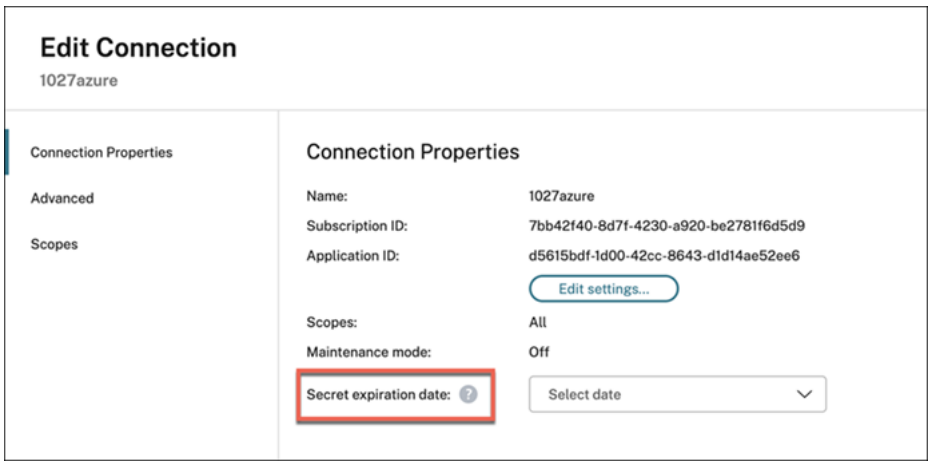
5. Forneça uma descrição do segredo e especifique uma duração. Quando terminar, selecione **Add**.

> **Nota:**
>
> Lembre-se de salvar o segredo do cliente porque você não pode recuperá-lo mais tarde.

6. Copie o valor do segredo do cliente e a data de expiração.
7. Na interface Full Configuration, edite a conexão correspondente e substitua o conteúdo no campo **Application secret** e **Secret expiration date** pelos valores copiados.

Alterar a data de expiração do segredo Você pode usar a interface Full Configuration para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

1. No assistente **Add Connection and Resources**, clique com o botão direito do mouse em uma conexão e clique em **Edit Connection**.
2. Na página **Connection Properties**, clique em **Secret expiration date** para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.



Permissões necessárias do Azure

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 somente permissões mínimas forem concedidas. Esta seção lista as permissões mínimas por ação.

Criar 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",
<!--NeedCopy-->
```

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",
<!--NeedCopy-->
```

Criar, atualizar ou excluir VMs Crie um catálogo de máquinas e, em seguida, 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 localizados na mesma região da conexão de hospedagem.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"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.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",
```



```
<!--NeedCopy-->
```

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 localizada na mesma região da conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

- Se a imagem mestre for uma ImageVersion da Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas):

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Se a imagem mestre for um disco gerenciado, um 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",
<!--NeedCopy-->
```

- Se você usar o grupo de recursos gerenciados pela Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Se você colocar a imagem mestre na Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas):

```
"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",
<!--NeedCopy-->
```

- Se você usar o suporte a host dedicado do Azure:


```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Se você usar a criptografia do lado do servidor (SSE) com chaves gerenciadas pelo cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- 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",
<!--NeedCopy-->
```

- Se você usar a especificação de modelo do Azure como um perfil de máquina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Criação, atualização e exclusão de máquinas com disco não gerenciado A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é VHD e usa o grupo de recursos conforme fornecido pelo administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"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"
<!--NeedCopy-->
```


Gerenciar dispositivos ingressados no Azure AD A seguir encontra-se a lista de permissões mínimas necessárias para gerenciar os dispositivos ingressados no Azure AD:

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

Permissões gerais

A função de colaborador tem acesso total para gerenciar todos os recursos. Esse conjunto de permissões não impede que você obtenha novos recursos.

O conjunto de permissões a seguir fornece 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.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",
```



```
37 "Microsoft.Network/networkSecurityGroups/write",
38 "Microsoft.Network/virtualNetworks/subnets/read",
39 "Microsoft.Network/virtualNetworks/read",
40 "Microsoft.Network/virtualNetworks/subnets/join/action",
41 "Microsoft.Resources/deployments/operationstatuses/read",
42 "Microsoft.Resources/deployments/read",
43 "Microsoft.Resources/deployments/validate/action",
44 "Microsoft.Resources/deployments/write",
45 "Microsoft.Resources/deployments/delete",
46 "Microsoft.Resources/subscriptions/resourceGroups/read",
47 "Microsoft.Resources/subscriptions/resourceGroups/write",
48 "Microsoft.Resources/subscriptions/resourceGroups/delete",
49 "Microsoft.Storage/storageAccounts/delete",
50 "Microsoft.Storage/storageAccounts/listKeys/action",
51 "Microsoft.Storage/storageAccounts/read",
52 "Microsoft.Storage/storageAccounts/write",
53 "Microsoft.Resources/templateSpecs/read",
54 "Microsoft.Resources/templateSpecs/versions/read",
55 <!--NeedCopy-->
```

Permissão do Azure AD Se você criar catálogos de máquinas ingressados no Azure AD, o MCS será responsável por gerenciar os dispositivos do Azure AD quando você habilitar o gerenciamento de dispositivos ingressados no Azure AD. A função **Cloud Device Administrator** integrada do Azure AD oferece a melhor compatibilidade daqui para frente, embora inclua mais permissões do que o necessário com o conjunto de recursos atual.

O que fazer a seguir

- 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

- Conexões e recursos
- Ambientes de nuvem do Microsoft Azure Resource Manager

Conexão com o Microsoft System Center Virtual Machine Manager

December 21, 2022

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem 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 da sua conta do VMM como um local de recursos. Consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Criar uma conexão

Se você usou o MCS para provisionar VMs, no assistente de criação de conexão faça o seguinte:

- Digite o endereço como um nome de domínio totalmente qualificado do servidor host.
- Insira as credenciais da conta de administrador que você configurou anteriormente. Essa conta deve ter permissão para criar novas VMs.
- Na caixa de diálogo Host Details, selecione o cluster ou o host autônomo para usar ao criar VMs.

  > **Importante**
  >
  > Procure um cluster ou host autônomo mesmo se você estiver usando uma única implantação de host Hyper-V.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para criar catálogos de máquinas com MCS no compartilhamento de arquivos SMB 3, consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager.

Mais informações

- Conexões e recursos
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Conexão com a Nutanix

December 21, 2022

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos da Nutanix.

> **Nota:**
>
> Antes de criar uma conexão com a Nutanix, você precisa primeiro concluir a configuração da sua conta da Nutanix como um local de recursos. Consulte Ambientes de virtualização da Nutanix.

Criar uma conexão com Nutanix

As informações a seguir são um complemento às orientações em Criar e gerenciar conexões. Para estabelecer uma conexão com o Nutanix, siga as orientações gerais neste artigo, cuidando dos detalhes específicos ao Nutanix.

No assistente **Add Connection and Resources**, selecione o tipo de conexão **Nutanix** na página **Connection** e especifique o endereço e as credenciais, além de um nome para a conexão. Na página **Network**, selecione uma rede para a unidade de hospedagem.

Os seguintes tipos de conexão estão disponíveis para seleção: **Nutanix AHV**, **Nutamix AHV XI** e **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique o endereço e as credenciais do cluster do Prism Element (PE).
- Para **Nutanix AHV PC**, especifique o endereço e as credenciais do hipervisor.
- Para **Nutanix AHV XI**, especifique seu endereço e nome de usuário e importe seus arquivos de credenciais públicas e privadas do Nutanix XI (`.pem`). (Chaves públicas e privadas são geradas na nuvem Nutanix XI pelos administradores do Nutanix XI.)
  - Para importar a chave, localize seu arquivo de credencial, abra-o com o Bloco de Notas (ou qualquer editor de texto) e copie o conteúdo. Depois disso, retorne à página **Connection**, selecione **Import key**, cole o conteúdo e selecione **Save**.

  Cuidado: não altere o conteúdo da credencial ou o formato.

> **Dica:**
>
> Se você implantar máquinas usando o Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas da Nutanix, consulte Criar um catálogo da Nutanix.

Mais informações

- Conexões e recursos

- Ambientes de virtualização da Nutanix
- Soluções de nuvem e parceiros da Nutanix

Conexão com soluções de nuvem e parceiros da Nutanix

June 6, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos das soluções de nuvem e parceiros da Nutanix.

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) oferece suporte à seguinte solução de nuvem e parceiros da Nutanix:

- Nutanix Cloud Clusters na AWS

> **Nota:**
>
> Antes de criar uma conexão com a solução de nuvem e de parceiros da Nutanix, você precisa primeiro concluir a configuração de sua respectiva conta como um local de recursos. Consulte Soluções de nuvem e parceiros da Nutanix.

Conecte-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. RDP na VM bastion, vá para o 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 da Nutanix

Depois de se conectar ao **Nutanix Prism**, crie VMs no cluster da 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 criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas dessa sub-rede para direcionar todo o tráfego local para o gateway NAT acima.

4. RDP na VM bastion, 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. 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:**
>
> Verifique se as informações de horário e fuso horário nas VMs estão configuradas corretamente. Isso aplica-se especialmente ao AD.

Criar conexão de host

1. Inicie o Citrix Studio.
2. Selecione o nó de hospedagem e clique em **Add Connection and Resources**.
3. Na tela **Conexão**, selecione **Criar uma nova conexão**e, no **Endereço de conexão**, insira `https://xxx.xxx.xxx.xxx:9440`.
4. Siga a interface do usuário para concluir o assistente.

> **Nota:**
>
> Todas as VMs conectoras 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.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas da Nutanix, consulte Criar um catálogo da Nutanix.

Mais informações

- Conexões e recursos

- Ambientes de virtualização da Nutanix
- Soluções de nuvem e parceiros da Nutanix

Conexão com o VMware

December 6, 2023

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização do VMware.

> **Nota:**
>
> Antes de criar uma conexão com o VMware, você precisa primeiro concluir a configuração da sua conta do VMware como um local de recursos. Consulte Ambientes de virtualização do VMware.

Permissões necessárias

Crie uma conta de usuário VMware e uma ou mais funções do VMware com um conjunto ou todas as permissões listadas neste artigo. Baseie a criação das funções no nível específico de granularidade exigido das permissões do usuário para solicitar as várias operações do Citrix Virtual Apps ou Citrix Virtual Desktops a qualquer momento. Para conceder ao usuário permissões específicas a qualquer momento, associe-as à respectiva função, no nível do data center, a um nível mínimo.

As tabelas a seguir mostram os mapeamentos entre as operações do Citrix Virtual Apps and Desktops e as permissões mínimas necessárias do VMware.

Adicionar conexões e recursos

SDK	Interface de usuário
System.Anonymous, System.Read e System.View	Adicionada automaticamente. Pode usar a função somente leitura interna.

Gerenciamento de energia

SDK	Interface de usuário
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

Provisionar máquinas (Machine Creation Services)

Para provisionar máquinas usando o MCS, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

SDK	Interface de usuário
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Atualização e reversão da imagem

SDK	Interface de usuário
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new

SDK	Interface de usuário
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Excluir máquinas provisionadas

SDK	Interface de usuário
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Perfil de armazenamento (vSAN)

Para exibir, criar ou excluir políticas de armazenamento durante a criação de catálogos em um armazenamento de dados vSAN, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
storage.Profile-driven storage update	PROFILE-DRIVEN STORAGE > Profile-driven storage update
storage.Profile-driven storage view	PROFILE-DRIVEN STORAGE > Profile-driven storage view

Marcas e atributos personalizados

As marcas e os atributos personalizados permitem que você anexe metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e a filtragem desses objetos. Para criar, editar, atribuir e excluir marcas ou categorias, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
Tagging.Create	vSphere Tagging > Create vSphere Tag
Tagging.Create	vSphere Tagging > Create vSphere Tag Category
Tagging.Edit	vSphere Tagging > Edit vSphere Tag
Tagging.Edit	vSphere Tagging > Edit vSphere Tag Category
Tagging.Delete	vSphere Tagging > Delete vSphere Tag
Tagging.Delete	vSphere Tagging > Delete vSphere Tag Category
Tagging.Assign	vSphere Tagging > Assign ou Unassign vSphere Tag
Tagging.Assign	vSphere Tagging > Assign ou Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Nota:**
>
> Quando o MCS cria um catálogo de máquinas, ele marca as VMs de destino com marcas de nomes especiais. Essas marcas diferenciam a imagem mestre das VMs criadas pelo MCS e evitam o uso de VMs criadas pelo MCS para preparação de imagens. Você pode identificar a diferença pelo valor do atributo `XdProvisioned` no vCenter. O atributo é definido como **True** se o MCS criar VMs.

Operações criptográficas

Os privilégios de operações criptográficas controlam quem pode realizar qual tipo de operação criptográfica e 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 de usuário
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographic operations.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographic operations.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographic operations.Read KMS information	Privileges > All Privileges > Cryptographic operations > Read KMS information

Provisionar máquinas (Citrix Provisioning)

Todas as permissões de **Provisionar máquinas (Machine Creation Services)** e o seguinte.

SDK	Interface de usuário
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
vApp.Export	vApp > Export

> **Nota:**
>
> - As permissões para clonar e implantar um modelo são necessárias para provisionar VMs usando o Assistente de Instalação do Citrix Virtual Apps and Desktops e o Assistente de Exportação de Dispositivos por meio do console Citrix Provisioning.
> - `vApp.Export` é necessário para criar catálogos de máquinas MCS usando o perfil da máquina.

Protegendo conexões com o ambiente VMware

O uso de conexões `HTTPS`/`SSL` com o vCenter requer que a conexão seja confiável pelo Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops).

Existem duas opções:

- Cada cloud connector confia no certificado do vCenter, e os serviços no conector reutilizam essa confiança. Essa confiança pode ser proveniente de:
  - Certificado vCenter, emitido pela Autoridade de Certificação e confiável pelo Windows, resultando em confiança estabelecida entre o Windows e o vCenter.
  - Certificado vCenter instalado no Windows, resultando em confiança estabelecida entre o Windows e o vCenter.
- Como alternativa, o banco de dados do Citrix Virtual Apps and Desktops tem a impressão digital SSL instalada. Essa impressão digital é usada pelo Citrix DaaS em cada conector de nuvem para confiar nas conexões com o vCenter.

> **Nota:**
>
> O certificado vCenter e a impressão digital SSL da VMware não são necessários para o VMware Cloud e suas soluções de parceiros.

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 conseguir usar um certificado digital emitido por uma autoridade de certificação e a política de segurança da sua organização permitir, você poderá usar o certificado autoassinado instalado pela VMware. Adicione o certificado VMware vCenter a cada Cloud Connector.

1. Adicione o nome de domínio totalmente qualificado (FQDN) do computador que executa o vCenter Server ao arquivo hosts nesse servidor, localizado em %SystemRoot%/WINDOWS/system32/Drivers/

Essa etapa só é necessária 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 vCenter server:

   a) Copie o arquivo rui.crt do servidor vCenter para um local acessível nos seus Cloud Connectors.
   b) No Cloud Connector, navegue 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, será necessário 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 estabeleça uma conexão da 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 do certificado.
   d) Examine o certificado e clique na guia Detalhes.
   e) Selecione **Copiar para arquivo e exportar no formato .CER**, fornecendo um nome quando solicitado.
   f) Salve o certificado exportado.
   g) Navegue até o local do certificado exportado e abra o arquivo .CER.

   Importe-o diretamente do Internet Explorer executado como administrador:

   a) Abra seu navegador da Web e estabeleça uma conexão da 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 do certificado.
   d) Examine o certificado.

3. Importe o certificado para o repositório de certificados em cada Cloud Connector.

   a) Clique em **Instalar certificado**, selecione **Máquina local** e clique em **Avançar**.
   b) Selecione **Colocar todos os certificados no repositório a seguir** e clique em **Procurar**. Em uma versão posterior suportada: selecione **Pessoas confiáveis** e clique em **OK**. Clique em **Avançar** e, em seguida, clique **Concluir**.

> **Importante:**
>
> Se você alterar o nome do servidor vSphere após a instalação, será necessário gerar um novo certificado autoassinado no servidor antes de importar o novo certificado.

Impressão digital SSL do VMware

O recurso de impressão digital SSL da VMware soluciona um erro relatado com frequência ao criar uma conexão de host com um hipervisor VMware vSphere. Anteriormente, os administradores precisavam criar manualmente uma relação de confiança entre os controladores de entrega gerenciados pela Citrix no site e o certificado do hipervisor antes de criar uma conexão. O recurso de impressão digital SSL da VMware remove esse requisito 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 Virtual Apps ou Citrix Virtual Desktops, mesmo que não pelos controladores.

Ao criar uma conexão de host do vSphere, uma caixa de diálogo permite visualizar o certificado da máquina à qual você está se conectando. Você pode então escolher se deve confiar nele.

A impressão digital SSL do VMware pode ser atualizada posteriormente usando o PowerShell SDK `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`.

> **Dica:**
>
> A impressão digital do certificado deve ser escrita em letras maiúsculas.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do VMware, consulte Criar um catálogo do VMware.

Mais informações

- Conexões e recursos
- Ambientes de virtualização do VMware
- Soluções de nuvem e parceiros da VMware

Conexão com soluções de nuvem e parceiros do VMware

December 21, 2022

Depois de configurar o cluster do Azure VMware Solution (AVS), o Google Cloud VMware Engine e a nuvem do VMware na AWS, crie as conexões. Consulte Conexão com ambientes de virtualização do VMware para criar conexões.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do VMware, consulte Criar um catálogo do VMware.

Mais informações

- Conexões e recursos
- Ambientes de virtualização do VMware.
- Soluções de nuvem e parceiros da VMware

Criar catálogos de máquinas

November 21, 2023

> **Nota:**
>
> Este artigo descreve como criar catálogos usando a interface Full Configuration. 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. Todas as máquinas em um catálogo têm o mesmo tipo de sistema operacional: SO multissessão ou SO de sessão única e máquinas Windows ou Linux.

A interface **Manage > Full Configuration** orienta você 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 criado 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 usar o MCS para provisionar VMs, você fornece uma imagem mestre (ou instantâneo de uma imagem) para criar VMs idênticas no catálogo. Antes de criar o catálogo, você primeiro usa o hipervisor ou as ferramentas de serviço de nuvem para criar e configurar a imagem. Esse processo inclui a instalação de um Virtual Delivery Agent (VDA) na imagem. Em seguida, você cria o catálogo de máquinas na interface **Manage > Full Configuration**. 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 deverá criar um ou mais catálogos de máquinas para importar essas VM para o catálogo.

Ao usar o MCS para criar o primeiro catálogo, você especifica a unidade de hospedagem que 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 as informações sobre essa unidade de hospedagem ou sua conexão de host principal ou criar mais conexões e unidades de hospedagem.

Se um Cloud Connector não estiver funcionando corretamente, as operações de provisionamento do MCS (como atualizações de catálogo) demoram muito mais do que o normal e o desempenho da interface de gerenciamento diminui significativamente.

Verificação de licença RDS

A criação de um catálogo de máquinas contendo máquinas do SO com várias sessões do Windows inclui uma verificação automática de licenças válidas do Microsoft RDS. 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 do RDS não pode ser executada.
- Se uma máquina for encontrada e um erro for detectado, **Manage > Full Configuration** exibirá uma mensagem de aviso para o catálogo que contém o problema detectado. Para remover um aviso de licença do RDS de um catálogo (para que ele não apareça mais na exibição), selecione o catálogo. Selecione **Remove RDS license warning**. Quando solicitado, confirme a ação.

Registro de VDA

Um VDA deve ser registrado com um Cloud Connector para ser considerado ao iniciar sessões intermediadas. Os VDAs não registrados podem resultar na subutilização de recursos disponíveis. Há várias razões para que um VDA não possa ser registrado, muitas das quais você pode resolver. São fornecidas informações sobre solução de problemas no assistente de criação de catálogo e depois de adicionar um catálogo a um grupo de entrega.

No assistente de criação de catálogos, depois de adicionar máquinas existentes usando o assistente, a lista de nomes de contas de computador indica se cada máquina é adequada para adicionar ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre a máquina.

Se a mensagem identificar uma máquina problemática, você pode remover essa máquina (usando o botão **Remove**) ou adicionar a máquina. Por exemplo, se uma mensagem indicar que as informações sobre uma máquina não puderam ser obtidas (talvez porque ela nunca foi registrada), você pode optar por adicionar a máquina.

Para obter mais informações sobre a solução de problemas de registro VDA, consulte CTX136668.

Resumo da criação de um catálogo MCS

Apresentamos a seguir uma breve visão geral das ações padrão do MCS depois que você fornece informações no assistente de criação de catálogo.

- Se você selecionou uma imagem mestre (em vez de um instantâneo), o MCS criará um instantâneo.
- O MCS cria uma cópia completa do instantâneo e coloca a cópia em cada local de armazenamento definido na conexão do host.
- O MCS adiciona as máquinas ao Active Directory, que cria identidades exclusivas.
- O MCS cria o número de VMs especificadas no assistente, com dois discos definidos para cada VM. Além dos dois discos por VM, uma imagem mestre também é armazenada no mesmo local de armazenamento. Se você tiver vários locais de armazenamento definidos, cada um deles obterá os seguintes tipos de disco:
  - A cópia completa do instantâneo 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 exclusiva. Cada VM obtém um disco de identidade.
  - Um disco de diferença exclusivo para armazenar gravações feitas na VM. Esse disco é provisionado pelo thin (se suportado pelo armazenamento do host) e aumenta até o tamanho máximo da imagem mestre, se necessário. Cada VM obtém um disco de diferença. O disco de diferença mantém as alterações feitas durante as sessões. É permanente para áreas de trabalho dedicadas. Para áreas de trabalho em pool, ela é excluída e uma nova é criada após cada reinicialização.

Como alternativa, ao criar VMs para fornecer áreas de trabalho estáticas, você pode especificar (na página **Machines** do assistente de criação de catálogo) clones de VM thick (cópia completa). Os clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem o seu próprio arquivo.

Considerações sobre armazenamento MCS

Há muitos fatores a considerar ao decidir sobre soluções, configurações e capacidades de armazenamento para MCS. As informações a seguir fornecem considerações apropriadas sobre a capacidade

de armazenamento:

Considerações sobre a capacidade:

- Discos

  Os discos Delta ou Differencing (Diff) consomem a maior quantidade de espaço na maioria das implantações MCS por VM. Cada VM criada pelo MCS recebe no mínimo dois discos após a criação.

  - Disk0 = Diff Disk: contém o SO quando copiado da imagem base mestre.
  - Disk1 = Identity Disk: 16 MB - contém dados do Active Directory de cada VM.

  À medida que o produto evolui, pode ser preciso adicionar mais discos para satisfazer determinados casos de uso e consumo de recursos que você tenha. Por exemplo:

  - O MCS Storage Optimization cria um disco de estilo cache de gravação para cada VM.
  - O MCS adicionou a capacidade de usar clones completos, contrário ao cenário de disco Delta descrito na seção anterior.

  Os recursos do Hypervisor também podem entrar na equação. Por exemplo:

  - Citrix Hypervisor IntelliCache cria um disco de leitura no armazenamento local para cada Citrix Hypervisor. Essa opção economiza IOPS em comparação à imagem mestre, que pode ser mantida no local de armazenamento compartilhado.

- Sobrecarga do hipervisor

  Diferentes hipervisores usam arquivos específicos que criam sobrecarga para VMs. Os hipervisores também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir sobrecargas para:

  - Arquivos de log
  - Arquivos específicos do Hypervisor. Por exemplo:
    * VMware adiciona mais arquivos à pasta de **armazenamento da VM**. Consulte VMware Best Practices.
    * Calcule os seus requisitos totais de tamanho de máquinas virtuais. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de permuta e 100 MB para arquivos de log, o que consome 36,1 GB no total.
  - Snapshots for XenServer; Snapshots for VMware.

- Sobrecarga do processo

  Criar um catálogo, adicionar uma máquina e atualizar um catálogo têm implicações únicas no armazenamento. Por exemplo:

  - A criação de um catálogo inicial requer que uma cópia do disco base seja copiada para cada local de armazenamento.
    * Essa opção também requer que você crie uma VM de preparação temporariamente.
  - A adição de uma máquina a um catálogo não exige copiar o disco base para cada local de armazenamento. A criação do catálogo varia de acordo com os recursos selecionados.
  - Atualizar o catálogo para criar um disco básico extra em cada local de armazenamento. Atualizações de catálogo também apresentam um pico de armazenamento temporário, onde cada VM no catálogo possui 2 discos Diff por um determinado período de tempo.

Mais considerações:

- **Dimensionamento de RAM:** afeta o tamanho de determinados discos e arquivos do hipervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de instantâneos.
- **Provisionamento thin/thick:** o armazenamento NFS é preferido devido aos recursos de provisionamento dinâmico.

Otimização de armazenamento de Machine Creation Services (MCS)

O recurso de otimização de armazenamento do Machine Creation Services (MCS) também é conhecido como MCS I/O. Esse recurso só está disponível no Azure, GCP, Citrix Hypervisor, VMware 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 MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico, ao incluir suporte para um arquivo de despejo de memória do Windows gravado no disco de cache de gravação.
- O MCS I/O mantém a tecnologia de *cache em RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação multicamada mais adequada. Essa funcionalidade permite que um administrador equilibre entre o custo de cada camada, RAM e disco, e desempenho para atender à expectativa de carga de trabalho desejada.

Atualizar o método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. MCS I/O não suporta mais 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. Uma vez que a VM esteja ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.
3. O pagefile, ou arquivo de paginação, é redirecionado para o volume formatado, `MCSWCDisk`. Como resultado, o 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, acrescido do tamanho do arquivo de paginação. Isso geralmente é associado ao tamanho da RAM da VM.

Ativar atualizações de otimização de armazenamento MCS Para ativar a funcionalidade de otimização de armazenamento MCS I/O, atualize o Delivery Controller e o VDA para a versão mais recente do Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será exigida. O VDA e a atualização do Delivery Controller manipulam a atualização do MCS I/O.

Atribuir uma letra de unidade específica ao disco de cache de write-back MCS I/O

Você pode atribuir uma letra de unidade específica ao disco de cache de write-back MCS I/O. Essa implementação ajuda a evitar conflitos entre a letra da unidade de qualquer aplicativo que você usa e a letra da unidade do disco de cache de write-back MCS I/O. Para fazer isso, você pode usar os comandos do PowerShell. Os hipervisores compatíveis são Azure, GCP, VMware, SCVMM e Citrix Hypervisor.

> **Nota:**
>
> Esse recurso requer VDA versão 2305 ou posterior.

Limitações

- Aplicável somente ao sistema operacional Windows
- Letra da unidade de disco 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 quando você cria um novo catálogo de máquinas

Atribuir uma letra de unidade ao disco cache de write-back

Para atribuir uma letra de unidade ao disco de cache de write-back:

1. Abra uma 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_d3e2d6352xxxxxxxx2130aa145ec77.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>'
<!--NeedCopy-->
```

5. Conclua a criação do catálogo. Para obter informações, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Preparar uma imagem mestre no hipervisor ou no serviço de nuvem

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

É bom saber:

- Uma imagem mestre também é conhecida como imagem clonada, imagem final, VM base ou imagem base. Os fornecedores de host e os provedores de serviços de nuvem podem usar termos diferentes.
- Verifique se o hipervisor ou serviço de rede tem processadores, memória e armazenamento suficientes para acomodar o número de máquinas criadas.
- Configure a quantidade correta de espaço em disco rígido necessário para áreas de trabalho e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo de máquinas.
- Os catálogos de máquinas do Remote PC Access não usam imagens mestre.
- Considerações de ativação do Microsoft KMS ao usar o MCS: se a 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 precisa rearmar manualmente o Microsoft Windows ou o Microsoft Office.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para o seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou ferramentas VMware). Se você omitir esta etapa, aplicativos e áreas de trabalho podem não funcionar corretamente.
- Um VDA. A Citrix recomenda a instalação da versão mais recente para permitir o acesso aos recursos novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros, conforme necessárias, como softwares antivírus ou agentes de distribuição eletrônica de software. Defina os serviços com configurações apropriadas para os usuários e o tipo de máquina (por exemplo, atualização de recursos).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda a virtualização de aplicativos. A virtualização reduz os custos eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduz o tamanho dos discos rígidos de imagem mestre, o que economiza nos 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.
- Quando usar MCS, se você localiza o Microsoft Windows, instale os locais e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam os locais e os pacotes de idiomas instalados.

> **Importante:**
>
> Se você estiver usando o MCS, não execute o Sysprep em imagens mestras.

Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e instale o sistema operacional, além de todos os service packs e atualizações. Especifique o número de CPUs virtuais. Você também pode especificar o valor vCPU se criar o catálogo da máquinas usando o PowerShell. Você não pode especificar o número de vCPUs ao criar um catálogo em **Manage > Full Configuration**. Configure a quantidade de espaço em disco rígido necessário para áreas de trabalho e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo.
2. Assegure-se de que o disco rígido esteja conectado ao local do dispositivo 0. A maioria dos modelos de imagem mestre padrão configura esse local por padrão, mas alguns modelos personalizados podem não o fazer.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, associe a imagem mestre ao domínio onde aplicativos e áreas de trabalho são membros. Assegure-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas. Se você estiver usando o MCS, não é necessário associar a imagem mestre a um domínio. As máquinas provisionadas são ingressadas no domínio especificado no assistente de criação de catálogo.
5. A Citrix recomenda que você crie e nomeie um instantâneo da sua imagem mestre para que ela possa ser identificada 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 do licenciamento por volume

O MCS oferece suporte à ativação de licenciamento por volume para automatizar e gerenciar a ativação dos sistemas operacionais Windows e do Microsoft Office. Os três modelos que o MCS aceita 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 suportadas pela Citrix. Durante a preparação da imagem, o MCS faz a rearmação do Microsoft Windows e do Microsoft Office KMS. Você pode pular a rearmação executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre o Microsoft Windows KMS Rearm e o Microsoft Office KMS Rearm durante a preparação da imagem, consulte Machine Creation Services: Image Preparation Overview and Fault-Finding. 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-Provserviceconfiguration` têm a mesma configuração que a fornecida no comando.

Ativação baseada no Active Directory (ADBA)

O ADBA permite que você ative as 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 suportadas pela Citrix, exceto o Windows Server 2022. Para obter mais informações sobre a ativação baseada no Active Directory, consulte Ativar usando a Ativação baseada no Active Directory.

Chave de ativação múltipla (MAK)

A 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 com um número fixo de contas de ativação. Toda vez que um sistema Windows é ativado, a uma redução na contagem de ativações. Há duas formas de ativar o sistema:

- Ativação on-line: se o sistema Windows que você deseja ativar tiver acesso à Internet, o sistema ativará automaticamente o Windows ao instalar a chave do produto. Esse processo reduz as contas de ativação em 1 da MAK correspondente.
- Ativação offline: se o sistema Windows não conseguir se conectar à Internet para fazer a ativação on-line, o MCS receberá 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.

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 Deploy MAK Activation para ver as etapas para instalar a chave MAK em um sistema Windows.
- Se você não estiver usando a preparação de imagens:
  1. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
  2. Defina o valor como 1.

Contagens de ativação Para ver o número de ativações restantes para a chave MAK ou verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação de Volume (VAMT). Consulte Instalar a VAMT.

Ativar o sistema Windows usando MAK Para ativar o sistema Windows usando a MAK:

1. Instale a chave do produto na imagem mestre. Essa etapa consome uma conta de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagens:
   a) Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
   b) Defina o valor como 1.

   Esse método desativa a opção de ativação on-line.
4. Adicione VMs ao catálogo de máquinas.
5. Ligue as VMs.
6. Dependendo da ativação, se on-line ou offline, o sistema Windows é ativado.
   - Se a ativação estiver on-line, o sistema Windows será ativado após a instalação da chave do produto.
   - Se a ativação estiver offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. Em seguida, o MCS recupera um ID de confirmação e um ID instalado 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`: veja o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS a partir da imagem mestre mais recente.
- O comando `Get-ProvVM`. Veja os parâmetros `WindowsActivationType`, `WindowsActivationSta` , `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Você pode verificar o erro e conferir as etapas para resolver o problema.

Comece a criar o catálogo

Antes de criar um catálogo:

- Revise esta seção para saber mais sobre as escolhas que você faz e as informações que você fornece.
- 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, verifique se você instalou um VDA nessa imagem.

Para iniciar o assistente de criação de catálogo:

1. Faça login no Citrix Cloud. No menu superior esquerdo, selecione **My Services > DaaS**.
2. Selecione **Manage**.
3. Se este for o primeiro catálogo sendo criado, você será levado para a seleção correta (como "Set up the machines and create machine catalogs to run apps and desktops"). O assistente de criação de catálogo é aberto.
4. Se você já criou um catálogo e deseja criar outro, siga estas etapas:
   a) Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
   b) Para organizar catálogos usando pastas, crie pastas abaixo da pasta **Machine Catalogs** padrão. Para obter mais informações, consulte Criar uma pasta de catálogo.
   c) Selecione a pasta em que você deseja criar o catálogo e clique em **Create Machine Catalog**. O assistente de criação de catálogo é aberto.

O assistente o leva pelas páginas descritas nas seções a seguir. As páginas que você vê podem ser diferentes, dependendo das seleções feitas e da conexão (com um host) que você usa. Hosts / virtualization resources lista as fontes de informação para os tipos de host com suporte.

Sistema operacional

Cada catálogo contém máquinas de apenas um tipo.

- **Multi-session OS:** um catálogo de SO multissessão fornece áreas de trabalho compartilhadas hospedadas. As máquinas podem estar executando versões suportadas dos sistemas operacionais Windows ou Linux, mas o catálogo não pode conter os dois.
- **Single-session OS:** um catálogo de SO de sessão única fornece áreas de trabalho VDI que você pode atribuir a vários usuários diferentes.
- **Remote PC Access:** um catálogo de Remote PC Access fornece aos usuários acesso remoto a suas áreas de trabalho nas máquinas físicas no escritório. O Remote PC Access não requer uma VPN para fornecer segurança.

Gerenciamento de máquinas

Esta página não aparece quando você está um catálogo de Remote PC Access.

A página **Machine Management** indica como as máquinas são gerenciadas e qual ferramenta você usa para implantar as máquinas.

Escolha se as máquinas no catálogo serão gerenciadas por meio da interface de Full Configuration.

- As máquinas têm a energia gerenciada por meio da interface Full Configuration ou são provisionadas por meio de um ambiente de nuvem, por exemplo, VMs ou PCs blade. Essa opção estará disponível somente se você já tiver configurado uma conexão com um hipervisor ou serviço de nuvem.
- As máquinas não têm a energia gerenciada por meio da interface Full Configuration, por exemplo, máquinas físicas.

Se você indicou que as máquinas têm a energia gerenciada por meio da interface Full Configuration ou são provisionadas por meio de um ambiente de nuvem, escolha qual ferramenta usar para criar VMs.

- **Citrix Machine Creation Services (MCS):** usa uma imagem mestre para criar e gerenciar máquinas virtuais. Os catálogos de máquinas em ambientes de nuvem usam o MCS. O MCS não está disponível para máquinas físicas.
- **Other:** uma ferramenta que gerencia máquinas já 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.

Tipos de área de trabalho (experiência de área de trabalho)

Esta página é exibida quando você está criando um catálogo contendo máquinas de SO de sessão única ou multissessão.

- Para máquinas com SO de sessão única:

  Na página **Desktop Experience**, você pode determinar o que ocorre cada vez que os usuários fazem logon e logoff. Selecione uma das seguintes opções:

  - Users are assigned a new (random) desktop each time they log on.
  - Users are assigned the same (static) desktop each time they log on. Você também pode decidir se as alterações feitas pelos usuários serão salvas ou descartadas depois que eles se desconectarem.

- Para máquinas com SO multissessão:

  Os usuários recebem uma área de trabalho aleatória toda vez que fazem logon. Na página Desktop Experience, você pode determinar o que ocorre quando eles fazem logoff. Selecione uma das seguintes opções:

  - Changes that users make to the desktop will be saved (persistent).
  - Changes that users make to the desktop will be discarded (non-persistent).

> **Nota:**
>
> Para máquinas multissessão persistentes, as alterações feitas pelos usuários nas áreas de trabalho serão salvas e estarão acessíveis a todos os usuários autorizados.

Imagem mestre

Esta página aparece somente quando você está usando o MCS para provisionar VMs. Siga estas etapas para completar as configurações:

1. Selecione o instantâneo ou a VM criada anteriormente como imagem mestre. Você pode adicionar uma nota para a imagem selecionada, se necessário.

   > **Nota:**
   >
   > - Quando você estiver usando o MCS, não execute o Sysprep em imagens mestras.
   > - Se você especificar uma imagem mestre em vez de um instantâneo, a interface de gerenciamento criará um instantâneo, mas você não poderá nomeá-lo.
   > - Uma mensagem de erro será exibida se você selecionar um instantâneo ou VM que não seja compatível com a tecnologia de gerenciamento de máquina selecionada anteriormente no assistente.

> - Para atualizar imagens em um nó de imagem, selecione-o na árvore e clique na opção para **Atualizar** no canto superior direito. Se você não selecionar nenhum nó da imagem, clicar em **Atualizar** atualiza todas as imagens na árvore. Para desmarcar um nó selecionado na árvore, mantenha pressionada a tecla **CTRL** e clique no nó.

2. Para usar uma VM existente como perfil de máquina, selecione **Use a machine profile** e depois selecione a VM.

   > **Nota:**
   >
   > Atualmente, o uso de perfis de máquina é restrito às VMs do Azure, AWS e GCP.

3. Selecione o nível funcional mínimo do catálogo. Para permitir o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tem a versão mais recente do VDA instalada.

Ambientes de serviço e plataforma de nuvem

Quando você está usando um serviço de nuvem ou plataforma 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 **Storage and License Types**.

Para obter informações específicas do host, siga o link apropriado listado em Start creating the catalog.

Máquinas

Esta página não aparece quando você está criando catálogos de Remote PC Access.

O título desta página depende do que você selecionou na página **Machine Management**: **Machines**, **Virtual Machines** ou **Machines and Users**.

> **Nota:**
>
> 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 criar. Digite **0** (zero) se não quiser criar nenhuma. Posteriormente, para criar VMs para um catálogo vazio, você pode usar **Add machines**.
  - Escolha a quantidade de memória (em MB) que cada VM tem.
  - **Importante:** cada VM criada tem um disco rígido. O respectivo tamanho é definido na imagem mestre; você não pode alterar o tamanho do disco rígido no catálogo.

  - Se você indicou na página **Desktop Experience** que as alterações do usuário para 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 (localização do recurso), você poderá selecionar uma zona para o catálogo.
  - Se você estiver criando VMs de áreas de trabalho estáticas, selecione um modo de cópia de máquina virtual. Veja Modo de cópia da máquina virtual
  - Se você estiver criando VMs de área de trabalho aleatórias não persistentes, poderá ativar e configurar o cache de write-back de dados temporários em 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 **Desktop Experience**, poderá, opcionalmente, especificar o nome de usuário para usar com cada VM que adicionar.

  > **Dica:**
  >
  > Para adicionar usuários, você pode navegar até os usuários ou inserir manualmente uma lista de nomes de usuário separados por ponto e vírgula. 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 **Remove** para excluir nomes da lista enquanto ainda estiver na página do assistente.

- **Ao usar outras ferramentas (não o MCS):**

  Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada) ajudam a identificar máquinas que podem não estar qualificadas para serem adicionadas ao catálogo ou que não podem se registrar com um Cloud Connector.

Adicionar SIDs ao criar máquinas virtuais

Agora você pode adicionar o parâmetro `ADAccountSid` para identificar as máquinas de forma exclusiva ao criar novas máquinas virtuais.

Para 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
<!--NeedCopy-->
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta do AD que não está no pool de identidades do catálogo
- Uma conta do AD que não está no estado disponível

Modo de cópia da máquina virtual

O modo de cópia que você especificar na página **Machines** determina se o MCS cria clones thin (cópia rápida) ou thick (cópia completa) a partir da imagem mestre. (Padrão = clones thin)

- Use clones de cópia rápida para uma utilização de armazenamento mais eficiente e criação de máquinas mais rápida.
- Use clones de cópia completa para melhorar o suporte a migração e recuperação de dados, com IOPS potencialmente reduzido após a criação das máquinas.

Configurar cache para dados temporários

Ao usar o MCS para gerenciar máquinas aleatórias não persistentes em um catálogo, você pode ativar o cache de write-back das máquinas para melhorar o desempenho de E/S.

O cache de write-back é conhecido como MCSIO. Para obter mais informações, consulte este artigo de blog.

Pré-requisitos Para ativar o cache de write-back, o catálogo deve atender aos seguintes requisitos:

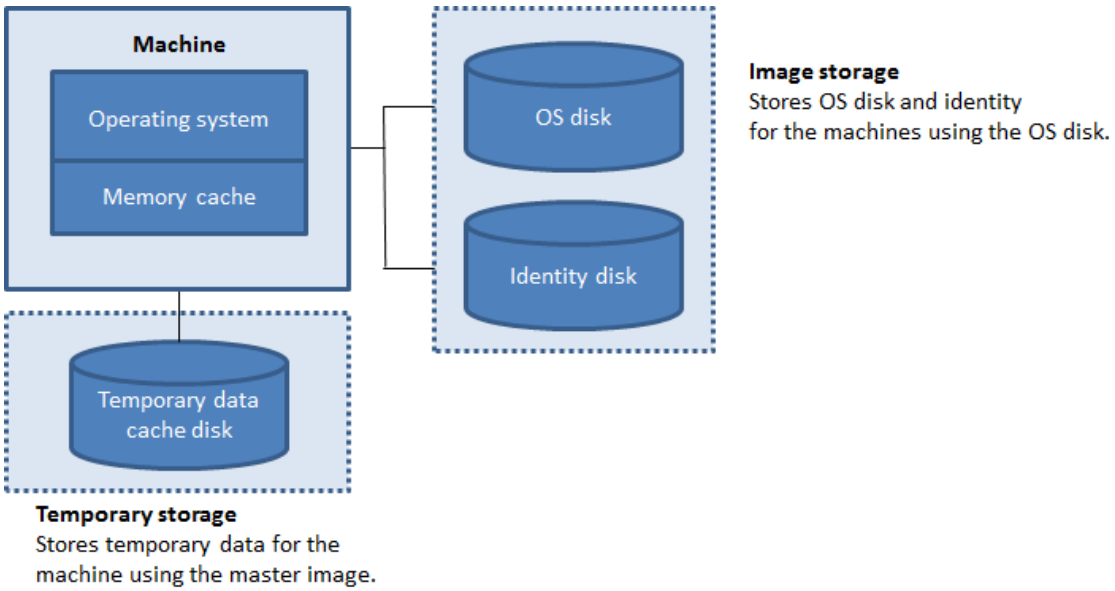
- Usar uma conexão que especifica o armazenamento de dados temporários. Para obter mais informações, consulte Conexões e recursos.
- Os VDAs devem ser pelo menos da versão 7.9 e estar instalados com um driver MCSIO atual.

  > **Nota:**
  >
  > Instalar esse driver é uma opção quando você instala ou atualiza um VDA. Por padrão, esse driver não é instalado.

- Para habilitar a atribuição de letras 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 no cache de *Memória* e no 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, leve em consideração o espaço necessário para:
  - Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
  - Dados de perfil do usuário.
  - Dados do ShareFile que são sincronizados com as sessões de usuários.
  - Dados que podem ser criados ou copiados por um usuário da sessão ou por qualquer aplicativo que os usuários possam instalar dentro da sessão.



- Se você ativar a caixa de seleção **Memory cache size (MB) (recommended)**, os dados temporários serão gravados inicialmente no cache de memória. Quando o cache de memória atinge seu limite configurado, os dados mais antigos são movidos para o disco de cache de dados temporários.
- O cache de memória faz parte da quantidade total de memória em cada máquina. Portanto, se você habilitar a caixa de seleção **Memory cache size (MB) (recommended)**, considere aumentar a quantidade total de memória em cada máquina.
- Se você mantiver a caixa de seleção **Memory cache size (MB) (recommended)** desmarcada, os dados temporários serão gravados diretamente no cache de disco, usando uma quantidade mínima de memória.
- Alterar o valor padrão em **Disk cache size (GB)** 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 ficará inutilizável.

Se você desmarcar a caixa de seleção **Disk cache size**, nenhum disco de cache será criado. Nesse caso, especifique um valor de **Memory allocated to cache** que seja grande o suficiente para conter todos os dados temporários. Isso só é possível se grandes quantidades de RAM estiverem disponíveis para alocação em cada VM.

Se você desmarcar as duas caixas de seleção, os dados temporários não serão armazenados em cache. Eles serão gravados no disco de diferença (localizado no armazenamento do sistema operacional) para cada VM. (Essa é a ação de provisionamento em versões anteriores a 7.9.)

Não ative o armazenamento em cache se você pretender usar esse catálogo para criar AppDisks.

Não é possível alterar os valores de cache em um catálogo de máquinas após ele ser criado.

Uso de arquivos CSV para adicionar máquinas em massa

Se você usar a interface de gerenciamento de **Full Configuration**, poderá adicionar máquinas em massa usando arquivos CSV. O recurso está disponível para todos os catálogos, exceto os catálogos criados por meio do MCS.

Um fluxo de trabalho geral para usar arquivos CSV para adicionar máquinas em massa é o seguinte:

1. Na página **Machines**, selecione **Add CSV File**. A janela **Add Machines in Bulk** é aberta.
2. Selecione **Download CSV Template**.
3. Preencha o arquivo de modelo.
4. Arraste ou navegue até o arquivo para carregá-lo.
5. Selecione **Validate** para realizar verificações de validação na importação.
6. Selecione **Import** para concluir.

Para obter informações sobre considerações sobre o arquivo 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 ser usado como um modelo ao adicionar máquinas em massa. Para exportar máquinas:

1. Na página **Machines**, selecione **Export to CSV file**. É baixado um arquivo CSV que contém uma lista das máquinas.

2. Abra o arquivo CSV para adicionar ou editar máquinas conforme o necessário. Para adicionar máquinas em massa usando o arquivo CSV salvo, consulte a seção anterior, Uso de arquivos CSV para adicionar máquinas em massa.

> **Nota:**
>
> - Esse recurso não está disponível para catálogos de acesso remoto ao PC.
> - A exportação e a importação de máquinas em arquivos CSV apenas têm suporte entre catálogos do mesmo tipo.

NIC (NICs)

Esta página não aparece quando você está criando catálogos de Remote PC Access.

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 a partir dessa página.

Contas de máquina

Esta página é exibida somente ao criar catálogos de Remote PC Access.

Especifique as contas de máquina do Active Directory ou Unidades Organizacionais (UOs) para adicionar que correspondam a usuários ou grupos de usuários. Não use barra (/) no nome de uma unidade organizacional.

Você pode escolher uma conexão de gerenciamento de energia configurada anteriormente ou selecionar não usar o gerenciamento de energia. Se quiser usar o gerenciamento de energia, mas uma conexão adequada ainda não tiver sido configurada, você pode criar essa conexão mais tarde e, então, 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 **Machine Accounts**, selecione **Add CSV File**. A janela **Add Machines in Bulk** é aberta.
2. Selecione **Download CSV Template**.
3. Preencha o arquivo de modelo.
4. Arraste ou navegue até o arquivo para carregá-lo.
5. Selecione **Validate** para realizar verificações de validação na importação.
6. Selecione **Import** para concluir.

Para obter informações sobre considerações sobre o arquivo CSV, consulte Considerações ao usar arquivos CSV para adicionar máquinas.

Identidades de máquina

Esta página aparece somente ao usar o MCS para criar VMs.

Cada máquina no catálogo deve ter uma identidade exclusiva. Essa página permite configurar identidades para máquinas no catálogo. As máquinas são ingressadas à identidade depois de serem provisionadas. Você não pode alterar o tipo de identidade depois de criar o catálogo.

Um fluxo de trabalho geral para definir as configurações nesta página é o seguinte:

1. Selecione uma identidade na lista.
2. Indique se deseja criar contas ou usar as existentes e a localização (domínio) dessas contas.

Você pode selecionar uma das seguintes opções:

- **On-premises Active Directory**. Máquinas pertencentes a uma organização e conectadas com uma conta do Active Directory que pertence a essa organização. Eles existem no local.

  > **Nota:**
  >
  > Por padrão, o domínio em que o recurso (conexão) reside é selecionado.

- **Azure Active Directory joined**. Máquinas pertencentes a uma organização e conectadas com uma conta do Azure Active Directory que pertence a essa organização. Elas existem apenas na nuvem. Para obter informações sobre os requisitos, limitações e considerações, consulte Ingressado no Azure Active Directory.

  > **Nota:**
  >
  > Essa opção exige que a imagem mestre atenda aos pré-requisitos do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join.

- **Hybrid Azure Active Directory joined**. 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 Ingressado no Azure Active Directory híbrido.

  > **Nota:**
  >
  > – Antes de poder usar a associação híbrida do Azure Active Directory, verifique se o seu ambiente do Azure atende aos pré-requisitos. Veja https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.

> – Essa opção exige que a imagem mestre atenda aos pré-requisitos do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid.

- **Non-domain-joined**. Máquinas que não ingressaram em nenhum domínio. Para obter informações sobre os requisitos e limitações, consulte Não ingressado em domínio.

> **Importante:**
>
> - Se você selecionar **On-premises Active Directory** ou **Hybrid Azure Active Directory joined** como o tipo de identidade, cada máquina no catálogo deverá 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 disponibilizá-lo, atualize o nível funcional mínimo.
> - Os tipos de identidade **Azure Active Directory joined** e **Hybrid Azure Active Directory joined** exigem a versão 2203 ou posterior do VDA como o nível funcional mínimo para o catálogo. Para disponibilizá-los, atualize o nível funcional mínimo.

Antes de criar contas, verifique se você tem permissão para criar contas de computador na unidade organizacional em que as máquinas residem. Cada máquina no catálogo deve ter um nome exclusivo. Especifique como você deseja criar a identidade das máquinas:

- Especifique a unidade organizacional e o esquema de nomenclatura da máquina. Para obter mais informações, consulte Machine account naming scheme. Quando você cria um catálogo, um pool de identidades é criado automaticamente para conter todas as identidades de máquinas que você definiu para o catálogo.
- Escolha um pool de identidades existente em seu ambiente.

> **Nota:**
>
> Os nomes das UO não podem conter barras (`/`).

Se você usar contas existentes, navegue até as contas ou clique em **Import** e especifique o arquivo .csv que contém o nome das contas. O conteúdo do arquivo importado deve usar o formato:

- [ADComputerAccount] ADcomputeraccountname.domain

É preciso haver contas suficientes para todas as máquinas que você está adicionando. A interface Full Configuration gerencia essas contas. Portanto, permita que o Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

Para catálogos que contêm 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 nomeação de conta de máquina

Cada máquina em um catálogo deve ter um nome exclusivo. Você deve especificar um esquema de nomeação de conta de máquina ao criar um catálogo. Use curingas (marcas de hash) como espaços reservados para números sequenciais ou letras que aparecem no nome.

Ao especificar um esquema de nomenclatura, esteja ciente das seguintes regras:

- O esquema de nomeação deve conter pelo menos um caractere curinga. Você deve colocar todos os curingas juntos.
- O nome inteiro, incluindo curingas, deve conter pelo menos 2, mas não mais que 15 caracteres. Ele 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 (-).

Além disso, deixe espaço suficiente para crescimento ao especificar o esquema de nomenclatura. Considere este exemplo: Se você criar 1.000 contas de máquina com o esquema "veryverylong#", o último nome de conta criado (veryverylong1000) conterá 16 caracteres. Portanto, o esquema de nomeação resultará em um ou mais nomes de máquinas que excedem o máximo de 15 caracteres.

Você pode indicar se os valores sequenciais são números (0-9) ou letras (A-Z):

- **0-9**. Se selecionados, os curingas especificados são resolvidos para números sequenciais.

  > **Nota:**
  >
  > Se houver apenas um curinga (#), o nome das contas começa com 1. Se houver dois, o nome das contas começa com 01. Se houver três, o nome das contas começa com 001 e assim por diante.

- **A-Z**. Se selecionados, os curingas especificados são resolvidos em letras sequenciais.

Por exemplo, um esquema de nomenclatura de PC-Sales-## (com **0-9** selecionado) resulta em contas com os nomes PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

Opcionalmente, você pode especificar como os nomes das contas começam.

- Se você selecionar **0-9**, as contas serão nomeadas sequencialmente, começando com os números especificados. Insira um ou mais dígitos, dependendo de quantos curingas você usar no campo anterior. Por exemplo, se você usar dois caracteres curinga, insira dois dígitos ou mais.
- Se você selecionar **A-Z**, as contas serão nomeadas sequencialmente, começando com as letras especificadas. Insira uma ou mais letras, dependendo de quantos curingas você usar no campo anterior. Por exemplo, se você usar dois curingas, insira duas letras ou mais.

Credenciais de domínio

Selecione **Enter credentials** e insira as credenciais de um administrador com permissão para executar operações de conta no domínio de destino do Active Directory.

Use a opção **Check name** para 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 do domínio. Se a verificação for aprovada, o nome de domínio é preenchido automaticamente.

> **Nota:**
>
> Se o tipo de identidade selecionado em **Machine Identities** for **Hybrid Azure Active Directory joined**, as credenciais inseridas deverão ter recebido a permissão `Write userCertificate`.

Workspace Environment Management (opcional)

Esta página aparece somente quando você usa a edição Advanced ou Premium do Citrix DaaS.

Selecione um conjunto de configurações do Workspace Environment Management (WEM) ao qual você deseja vincular o catálogo. Um conjunto de configurações é um contêiner lógico usado para organizar um conjunto de configurações do WEM. Vincular um catálogo a um conjunto de configurações permite que você use o WEM para oferecer a melhor experiência de espaço de trabalho possível aos seus usuários.

> **Importante:**
>
> - Antes de vincular um catálogo a um conjunto de configurações, você deve configurar a implantação do serviço WEM. Faça login no Citrix Cloud e inicie o serviço WEM. Para obter mais informações, consulte Primeiros passos com o serviço Workspace Environment Management.
> - Se você já usa o WEM, as máquinas no catálogo que você está prestes a provisionar podem já estar presentes em um conjunto de configurações, por exemplo, por meio do Active Directory. Nesse caso, recomendamos que você use o Active Directory de forma consistente para executar a configuração e ignorar essa configuração.

Se o conjunto de configurações selecionado não contiver configurações relacionadas à configuração básica do WEM, a seguinte opção será exibida:

- **Apply basic settings to configuration set**. A opção permite que você comece a usar rapidamente o WEM aplicando configurações básicas ao conjunto de configurações. As configurações básicas incluem proteção contra picos de CPU, prevenção automática de picos de CPU e otimização inteligente da CPU. Para ver as configurações básicas, clique no link *aqui*. Para modificá-los, use o console do WEM.

Atualização do VDA (opcional)

> **Importante:**
>
> - Para garantir uma atualização tranquila, certifique-se de atender aos pré-requisitos e analisar os problemas conhecidos antes de atualizar os VDAs para as versões CR ou LTSR CU. Consulte Atualizar VDAs usando a interface Full Configuration.
> - Ao atualizar VDAs LTSR para versões de atualização cumulativa (CU) LTSR, certifique-se de que a versão dos VDA Upgrade Agents em execução nos VDAs seja 7.36.0.7 ou posterior. Para obter mais informações, consulte Atualizar VDAs usando a interface Full Configuration.

Esse recurso se aplica aos seguintes tipos de máquina:

- Máquinas persistentes provisionadas pelo MCS. Você as implanta usando o **Citrix Machine Creation Services** na página **Machine Management** durante a criação do catálogo.
- Máquinas que não são criadas usando o MCS (por exemplo, máquinas físicas). Você os implanta usando **Other service or technology** na página **Machine Management** durante a criação do catálogo.

Para obter mais informações sobre as duas opções, consulte Gerenciamento de máquinas.

Na página **VDA Upgrade**, selecione a versão do VDA para a qual atualizar. Se especificado, os VDAs no catálogo que têm o VDA Upgrade Agent instalado podem atualizar para a versão selecionada — imediatamente ou em um horário agendado.

> **Nota:**
>
> - Esse recurso suporta a atualização somente para o VDA mais recente. O momento em que você cria um agendamento de atualização do VDA ou atualiza um VDA determina a versão mais recente do VDA.
> - Depois de definir 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 **VDA Upgrade**, clique em Columns, na barra de ações, selecione **Machine Catalog > VDA Upgrade** e clique em **Save**.

Escolha uma faixa VDA que se adapte à sua implantação:

> **Importante:**
>
> Você pode alternar entre o VDA CR e o VDA LTSR, desde que a mudança seja de uma versão anterior para uma versão posterior. Você não pode mudar de uma versão posterior para uma versão anterior porque isso é considerado um downgrade. Por exemplo, você não pode fazer o downgrade de 2212 CR para 2203 LTSR (qualquer CU), mas pode fazer o upgrade de 2112 CR para 2203 LTSR (qualquer CU).

- **Latest CR VDA**. As versões atuais (CRs) oferecem os recursos e funcionalidades mais recentes e inovadores de virtualização de aplicativos, áreas de trabalho e servidores.
- **Latest LTSR VDA**. As versões de serviço de longo prazo (LTSRs) são recomendadas para os ambientes de produção das grandes empresas, 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 Atualização de VDAs.

Se você quiser habilitar a atualização do VDA posteriormente, poderá retornar a esta página editando o catálogo após sua criação. Para obter mais informações, consulte Defina as configurações de atualização do VDA editando um catálogo.

Resumo, nome e descrição

Na página **Summary**, revise as configurações especificadas. Insira um nome e uma descrição para o catálogo. Essas informações aparecem na interface de gerenciamento Full Configuration.

Quando terminar, selecione **Finish** para iniciar a criação do catálogo.

Em **Machine Catalogs**, o novo catálogo aparece com uma barra de progresso embutida.

Para ver os detalhes do progresso da criação:

1. Passe o mouse sobre o catálogo da máquina.
2. Na dica de ferramenta exibida, clique em **View details**.

   É exibido um gráfico de progresso passo a passo, onde você pode ver o seguinte:

   - Histórico das etapas
   - Progresso e tempo de execução da etapa atual
   - Etapas restantes

Consideração importante sobre a configuração de propriedades personalizadas

As propriedades personalizadas devem ser definidas corretamente em `Set-ProvScheme` e `New-ProvScheme` nos ambientes do GCP e Azure. Se você especificar propriedades personalizadas não

existentes, receberá a seguinte mensagem de erro e os comandos não serão executados.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

Consideração importante sobre a configuração dos parâmetros ProvScheme

Quando você usa o MCS para criar um catálogo, você recebe um erro se:

- Definir os seguintes `New-ProvScheme` parâmetros em hipervisores sem suporte ao criar um catálogo de máquinas:

Parâmetro	Hipervisores compatíveis
`UseWriteBackCache`	VMware
	Hyper-V
	Citrix Hypervisor
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	Citrix Hypervisor

- Atualizar os seguintes parâmetros de `Set-ProvScheme` depois de criar o catálogo de máquinas:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

O que fazer a seguir

Para obter informações sobre a criação de catálogos de hipervisores específicos, consulte:

- Criar um catálogo da AWS
- Criar um catálogo do Citrix Hypervisor
- Criar um catálogo do Google Cloud Platform
- Criar um catálogo do Microsoft Azure
- Criar um catálogo do Microsoft System Center Virtual Machine Manager
- Criar um catálogo da Nutanix
- Crie um catálogo do VMware

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.

Mais informações

- Gerenciamento de imagens do Citrix Virtual Apps and Desktops
- Conexões e recursos
- Criar catálogos ingressados em identidades de máquinas
- Gerenciar catálogos de máquinas

Criar um catálogo da AWS

December 20, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização da AWS.

> **Nota:**
>
> Antes de criar um catálogo da AWS, você precisa concluir a criação de uma conexão com a AWS. Consulte Conexão com a AWS.

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. Essa VM de preparação está 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.

Esse grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, sendo o GUID gerado aleatoriamente.

Locação da 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 EC2 de clientes diferentes podem residir no mesmo equipamento de hardware físico. Locação dedicada significa que suas instâncias do EC2 são executadas somente no hardware com as outras instâncias que você implantou. Outros clientes não usam o mesmo equipamento de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando a interface Full Configuration ou o PowerShell.

Configurar a locação de host dedicada da AWS usando a interface Full Configuration

Quando você usa o MCS para criar um catálogo para provisionar máquinas na AWS, a página **Machine Catalog Setup > Security** apresenta as seguintes opções:

- **Use shared hardware**. Essa configuração é adequada para a maioria das implantações. Vários clientes compartilham equipamentos de hardware, mesmo que não interajam entre si. Usar um hardware compartilhado é a opção mais barata para executar suas instâncias do Amazon EC2.
- **Use dedicated host**. Um host dedicado do Amazon EC2 é um servidor físico com capacidade de instância do EC2 totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM. Os hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado dos tipos de instância C4 Large é limitado à execução de 16 instâncias. Consulte o site da AWS para obter mais informações.

  Os requisitos de provisionamento para os hosts da AWS incluem:

  - Uma imagem (AMI) importada da BYOL (traga sua própria licença). Com hosts dedicados, use e gerencie suas licenças existentes.
  - Uma alocação de hosts dedicados com utilização suficiente para atender às solicitações de provisionamento.
  - Ativação do **posicionamento automático**.

  Essa configuração é adequada para implantações com restrições de licenciamento ou requisitos de segurança que precisam do uso de um host dedicado. Com um host dedicado, você tem um host físico inteiro e é cobrado por hora. Possuir esse host permite que você gire quantas instâncias do EC2 o host permitir, sem mais cobranças.

Como alternativa, você pode provisionar hosts dedicados da AWS por meio do PowerShell. Para isso, use o cmdlet `New-ProvScheme` com o parâmetro `TenancyType` definido como `Host`. Consulte a Documentação do Citrix Developer para obter mais informações.

- **Use dedicated instance**. 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 da AWS, mas não paga pelo host inteiro. Você não precisa se preocupar com a capacidade do host, mas a taxa cobrada é pelas instâncias é mais alta.

Configurar a locação de host dedicada da AWS usando o PowerShell

Você pode criar um catálogo de máquinas com a locação de host definida por meio do PowerShell.

Um host dedicado [EC2] da Amazon é um servidor físico com capacidade de instância [EC2] totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM.

Os hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado dos tipos de instância C4 Large é limitado à execução de 16 instâncias. Consulte o site da AWS para obter mais informações.

Os requisitos de provisionamento para os hosts da AWS incluem:

- Uma imagem (AMI) importada da BYOL (traga sua própria licença). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para atender às solicitações de provisionamento.
- Ativar o **posicionamento automático**.

Para provisionar a um host dedicado na AWS usando o PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro TenancyType definido como *Host*.

Consulte a Documentação do Citrix Developer para obter mais informações.

Capturar a propriedade da instância da AWS

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, você seleciona uma AMI para representar a imagem mestre/de ouro do catálogo. A partir dessa AMI, o MCS usa um instantâneo do disco. Em versões anteriores, se você quisesse funções ou marcações em suas máquinas, usaria o console da AWS para defini-las individualmente. Essa funcionalidade é ativada por padrão.

> **Dica:**
>
> Para usar a captura de propriedade da instância da AWS, você deve ter uma VM associada à AMI.

Para melhorar esse processo, o **MCS lê** as propriedades da instância a partir da qual a AMI foi obtida e aplica a função de Identity Access Management (IAM) e as marcas da máquina às máquinas provisionadas de um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo localiza a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são armazenadas em um Launch Template da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturada.

As propriedades capturadas incluem:

- Funções de IAM –aplicadas a instâncias provisionadas.
- Marcações –aplicadas a instâncias provisionadas, seus discos e NICs. Essas marcações são aplicadas a recursos temporários da Citrix, incluindo: objetos e bucket S3, e AMIs, instantâneos e modelos de execução.

> **Dica:**
>
> A marcação de recursos temporários da Citrix é opcional e pode ser configurada usando a propriedade personalizada `AwsOperationalResourcesTagging`. Para aplicar marcas com êxito e criar um catálogo da AWS com marcação de recursos operacionais, não exclua a instância do EC2 que foi usada para criar a imagem AMI.

Capturar a propriedade da instância da AWS

Você pode usar este recurso especificando uma propriedade personalizada, `AwsCaptureInstanceProperti`
, ao criar um esquema de provisionamento para uma conexão de hospedagem da AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

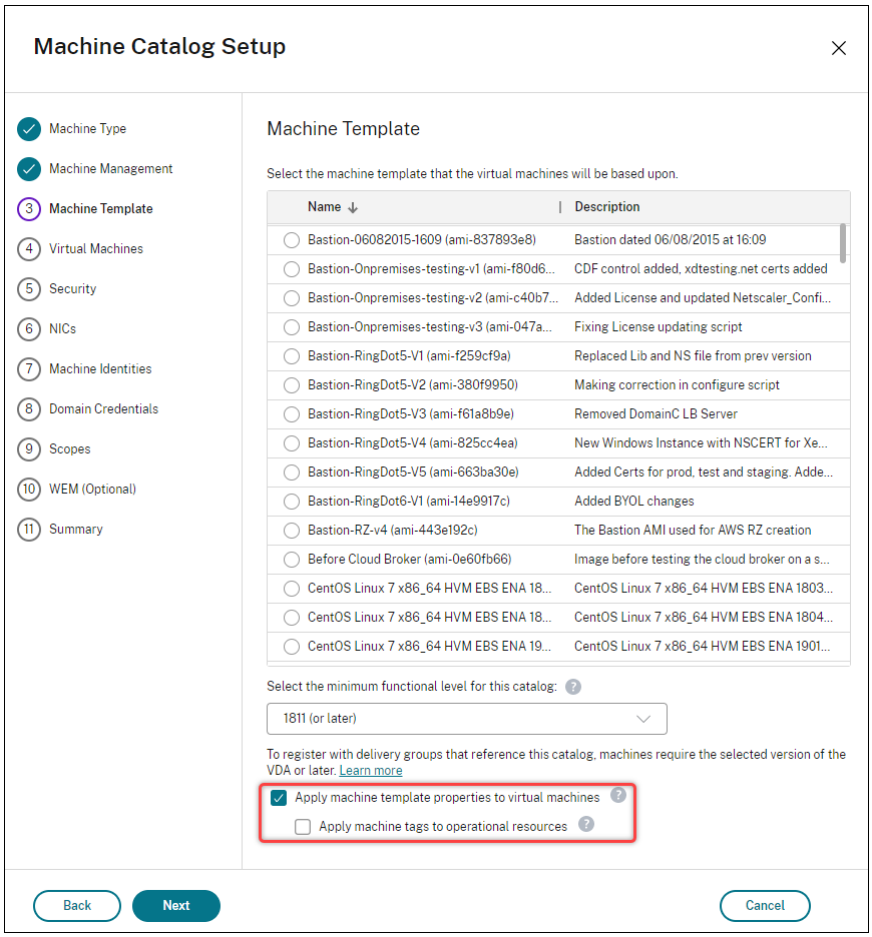
Consulte a Documentação do Citrix Developer para obter mais informações.

> **Nota:**
>
> O `AwsCaptureInstanceProperties` está obsoleto.

Aplicar propriedades de instância da AWS e marcar recursos operacionais com tags na interface Full Configuration

Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode controlar se as propriedades de função e marcação com tag do IAM devem ser aplicadas a essas máquinas. Você

também pode controlar se as marcas de máquina devem ser aplicadas aos recursos operacionais. Você tem as duas opções a seguir:



- Aplicar propriedades de modelo de máquina a máquinas virtuais, em **Apply machine template properties to virtual machines**
  - Controla se as propriedades de tag e função do IAM associadas ao modelo de máquina selecionado devem ser aplicadas às máquinas virtuais no catálogo.
- Aplicar marcas de máquina a recursos operacionais, em **Apply machine tags to operational resources**
  - Controla se as marcas de máquina devem ser aplicadas a cada item criado em seu ambiente da AWS, o que facilita o provisionamento de máquinas. Os recursos operacionais são criados como subprodutos da criação de catálogos. Incluem recursos temporários e persistentes, como preparação, instância de VM e AMI.

Marcar um recurso operacional AWS

Uma Amazon Machine Image (AMI) representa um tipo de dispositivo virtual usado para criar uma máquina virtual dentro do ambiente de nuvem Amazon Cloud, comumente chamado de EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Quando cria um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem de ouro do catálogo.

> **Importante:**
>
> A criação de catálogos por meio da captura de uma propriedade de instância e um modelo de execução é necessária para usar a marcação de recursos operacionais.

Para criar um catálogo da AWS, você deve primeiro criar uma AMI para a instância que você quer que seja a imagem de ouro. O MCS lê as marcas dessa instância e as incorpora ao modelo de execução. As marcas do modelo de execução são então aplicadas a todos os recursos da Citrix criados no seu ambiente da AWS, incluindo:

- Máquinas virtuais
- Discos VM
- Interfaces de rede VM
- Buckets do S3
- Objetos do S3
- Modelos de execução
- AMIs

Marcar um recurso operacional

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell no 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 nova propriedade personalizada `AwsOperationalResourcesTagging`. A sintaxe dessa propriedade é:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" ...<standard provscheme parameters
>
```


Criar um catálogo usando um perfil de máquina

Você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou iniciar a versão do modelo e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume do EBS, tipo de instância, otimização do EBS, Elastic Graphics e outras configurações compatíveis da AWS.

Você pode usar uma instância (VM) AWS EC2 ou a versão AWS Launch Template como entrada do perfil da máquina.

> **Nota:**
>
> As propriedades de volume do EBS são derivadas somente de um perfil de máquina.

Considerações importantes

Considerações importantes ao criar um catálogo de máquinas MCS:

- Se você adicionar os parâmetros de propriedade de hardware da máquina nos comandos `New-ProvScheme` e `Set-ProvScheme`, os valores fornecidos nos parâmetros substituirão os valores no perfil da máquina.
- Se você definir `AwsCaptureInstanceProperties` como **`true`** e não definir a propriedade `MachineProfile`, somente as tags e funções do IAM serão capturadas.
- Você não pode definir `AwsCaptureInstanceProperties` e `MachineProfile` ao mesmo tempo.

  > **Nota:
  >
  > O `AwsCaptureInstanceProperties` está obsoleto.

- Você deve fornecer explicitamente os valores das seguintes propriedades:
  - TenancyType
  - Grupo de Segurança
  - NIC ou rede virtual
- Você pode ativar `AwsOperationalResourcesTagging` somente se ativar `AwsCaptureInstancePr` ou especificar um perfil de máquina.

Considerações importantes após criar um catálogo de máquinas MCS:

- Somente as novas VMs adicionadas ao catálogo são afetadas pela alteração.
- Você não pode alterar de um catálogo baseado em perfil de máquina para um catálogo não baseado em perfil de máquina.

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 o comando `asnp citrix*` para carregar os módulos do 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
<!--NeedCopy-->
```

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'
<!--NeedCopy-->
```

5. Conclua a criação do catálogo. Para obter mais informações, consulte Citrix PowerShell SDK.

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina:

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-0
    xxxxxxxx).vm"
<!--NeedCopy-->
```

Criar um catálogo com a versão do modelo de execução

Você pode criar um catálogo de máquinas MCS com uma versão do modelo de execução como entrada do perfil da máquina. Você também pode atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução e de uma versão de modelo de execução para uma VM.

No console da AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de execução juntamente com o número da versão. Quando você especifica a versão do modelo de execução como uma entrada de perfil de máquina ao criar ou atualizar um catálogo de máquinas, as propriedades dessa versão do modelo de execução são copiadas para as VMs VDA provisionadas.

As propriedades a seguir podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidos nos comandos `New-ProvScheme` ou `Set-ProvScheme`, eles terão precedência sobre os valores de perfil da máquina dessas propriedades.

- Oferta de serviço
- Redes
- Grupos de segurança
- Tipo de locação

> **Nota:**
>
> Se a oferta de serviço não for fornecida no modelo de execução 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 execução como uma entrada de perfil da máquina:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Obtenha a lista de versões de modelo de execução de um modelo de execução. Por exemplo:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Crie um pool de identidades se não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Crie um esquema de provisionamento com uma versão do modelo de execução como entrada do 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"
<!--NeedCopy-->
```

Você também pode substituir parâmetros como oferta de serviço, grupos de segurança, locação e redes. 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-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
    `
-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large Instance.
   serviceoffering"
<!--NeedCopy-->
```

6. Registre o esquema de provisionamento como um catálogo de agente. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Conclua a criação do catálogo. Para obter mais informações, consulte Citrix PowerShell SDK

Você também pode atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução e de uma versão de modelo de execução para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução:

```
 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
     `
 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
     (lt-0bxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
    launchtemplateversion"
```



```
<!--NeedCopy-->
```

- Para atualizar a entrada de um catálogo de perfis de máquina de uma versão do modelo de execução 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"
<!--NeedCopy-->
```

Criar um catálogo de VMs habilitadas com o acelerador do Elastic Graphics

Usando o fluxo de trabalho baseado em perfil de máquina, você pode criar um catálogo de VMs habilitadas com o acelerador do Elastic Graphics. Você pode usar uma VM ou um modelo de execução como uma entrada de perfil de máquina.

As etapas detalhadas para criar um catálogo são:

1. Ative um acelerador do Elastic Graphics em uma VM ou modelo de execução. Para obter informações sobre como ativar o acelerador do Elastic Graphics, consulte Como trabalhar com o Elastic Graphics.
2. Verifique o tipo de acelerador do Elastic Graphics usado pela VM ou pela versão do modelo de execução. Se a chave `ElasticGpuType` não estiver presente nos dados adicionais, a VM ou o modelo de execução não tem o acelerador do Elastic Graphics ativado.

   - Por exemplo, para uma VM:

   ```
   (Get-Item -LiteralPath 'XDHyp:\HostingUnits\abc-resources\us-eat-1a.availibilityzone\abcelastic (i-0584xxxxxab8b2206).vm').AdditionalData
   <!--NeedCopy-->
   ```

   - Por exemplo, para um modelo de execução:

   ```
   (Get-Item -LiteralPath 'XDHyp:\HostingUnits\abc-resources\ElasticGC (lt-015f531351188cd2e).launchtemplate\lt-015f531351188cd2e (1).launchtemplateversion).AdditionalData
   <!--NeedCopy-->
   ```

3. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina selecionando uma especificação de modelo ou um modelo de execução. Você pode criar o catálogo de máquinas usando comandos do PowerShell.

> **Nota:**
>
> O catálogo de máquinas deve atender aos pré-requisitos do Elastic Graphics para a criação bem-sucedida do catálogo de máquinas. Portanto, certifique-se de que o tipo de instância do EC2 seja compatível com o Elastic Graphics. Para obter informações, consulte Conceitos básicos de Elastic Graphics.

Filtrar instâncias de VM

Uma instância de VM da AWS que você usa como uma 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 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 devem ser ignorados do início absoluto (ou final 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 sem incluir 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
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

- Para retornar uma matriz de registros que terminam com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
<!--NeedCopy-->
```

- Para retornar uma matriz de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

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 cadeia de caracteres fornecida corresponder à parte do nome de uma AMI, a AMI será incluída no `Get` resultante. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘ apollo ’
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '`: se uma AMI tiver pelo menos uma dessas tags, ela será incluída no `Get` resultante. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Nota:**
>
> Dois valores de tag são suportados. O valor da marca **Not Tagged** corresponde aos itens que não têm a tag especificada em sua lista de tags. O valor da marca **All values** corresponde aos itens que têm a tag, independentemente do valor da tag. Caso contrário, a correspondência só acontece se o item tiver a tag e o valor for igual ao fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: se a AMI corresponder à ID fornecida, ela será incluída no `Get` resultante. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

Filtragem pelo 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
<!--NeedCopy-->
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs estão incluídas em um campo `AdditionalData` chamado **Warning**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

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 da AWS.

Mais informações

- Conexões e recursos
- Conexão com a AWS
- Criar catálogos de máquinas

Criar um catálogo do Citrix Hypervisor

August 30, 2023

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"
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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"
<!--NeedCopy-->
```

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)
```



```
<!--NeedCopy-->
```

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\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   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

Criar um catálogo do Google Cloud Platform

September 5, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos 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 Conexão com ambientes de nuvem do Google.

Preparar uma instância de VM mestre e um disco permanente

> **Dica:**
>
> Disco permanente é o termo do Google Cloud para disco virtual.

Para preparar a sua instância de VM mestre, crie e configure uma instância de VM com propriedades que correspondam à configuração desejada para as instâncias do VDA clonadas no seu catálogo de máquinas planejado. A configuração não se aplica somente ao tamanho e ao tipo da instância. Também inclui atributos de instância, como metadados, tags, atribuições de GPU, marcas de rede e propriedades da conta de serviço.

Como parte do processo, 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 do VDA clonadas que compõem o catálogo de máquinas. As instâncias clonadas herdam as propriedades (exceto as propriedades de VPC, sub-rede e disco permanente) 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 prepare o disco permanente para a instância.

Recomendamos que você crie manualmente um instantâneo do disco. Isso permite que você use uma convenção de nomenclatura significativa para controlar as versões, oferece mais opções para gerenciar versões anteriores da sua imagem mestre e economiza tempo na criação do catálogo de máquinas. Se você não criar o seu próprio instantâneo, o MCS cria um instantâneo temporário para você (que é apagado no final do processo de provisionamento).

Criar um catálogo de máquinas

> **Nota:**
>
> Crie os 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 bucket e objeto para obter mais informações.

Siga as orientações em Criar catálogos de máquinas. A descrição a seguir é exclusiva para os catálogos do Google Cloud.

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione **Create Machine Catalog** na barra de ações.
3. Na página **Machine Type**, selecione **Multi-session OS** e, em seguida, selecione **Next**.
   - O Citrix DaaS também oferece suporte a SO de sessão única.
4. Na página **Machine Management**, selecione as opções **Machines that are power managed** e **Citrix Machine Creation Services** e selecione **Next**. Se houver vários recursos, selecione um no menu.
5. Na página **Master Image**, complete as etapas conforme necessário e clique em **Next**.
   a) Selecione um instantâneo ou uma VM como a imagem mestre. 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 a seleção de zona.
   b) Para usar uma VM existente como perfil de máquina, selecione **Use a machine profile** e depois selecione a VM.

      > **Nota:**
      >
      > Atualmente, as VMs desse catálogo herdam as configurações de ID do conjunto de criptografia de disco, tamanho da máquina, tipo de armazenamento e zona do perfil da máquina.

   c) Selecione o nível funcional mínimo do catálogo.
6. Na página **Storage**, selecione o tipo de armazenamento usado para conter o sistema operacional desse catálogo de máquinas. Cada uma das opções de armazenamento a seguir tem características únicas de preço e desempenho. (Um disco de identidade é sempre criado usando o disco permanente padrão por zona.)
   - Disco permanente padrão
   - Disco permanente balanceado
   - Disco permanente SSD

   Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte https://cloud.google.com/compute/docs/disks/.
7. Na página **Virtual Machines**, especifique quantas VMs você deseja criar, confira a especificação detalhada das VMs e selecione **Next**. Se você usar grupos de nós de locatário único para catálogos de máquinas, certifique-se de selecionar **apenas** as zonas em que os nós de locatário único reservados estão disponíveis. Consulte Habilitar a seleção de zona.
8. Na página **Disk Settings**, você pode definir as seguintes configurações:

- Escolha se deseja ativar o cache de write-back. Depois de ativar o cache de write-back, você pode fazer o seguinte:
  - Configurar o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
  - Selecionar 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 permanente padrão
    * Disco permanente balanceado
    * Disco permanente SSD

    Para obter detalhes sobre as opções de armazenamento do GCP, consulte https://cloud.google.com/compute/docs/disks/.
  - Selecione o tipo para o disco de cache de write-back.
    * **Use non-persistent write-back cache disk**. Se selecionado, o disco de cache de write-back não persistirá para as VMs provisionadas. O disco é excluído durante os ciclos de energia e todos os dados redirecionados para o disco serão perdidos.
    * **Use persistent write-back cache disk**. Se selecionado, o disco de cache de write-back persistirá para as VMs provisionadas. Habilitar essa opção aumenta os custos de armazenamento.
- Quando a otimização de armazenamento MCS (MCS I/O) está habilitada, você pode escolher se deseja reter os discos do sistema para VDAs durante os ciclos de alimentação de energia. Para obter mais informações, consulte Ativar atualizações de otimização de armazenamento MCS.
- 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 (CMEKs). Para obter mais informações, consulte Usar chaves de criptografia gerenciadas pelo cliente (CMEK).

  > **Nota:**
  >
  > Ele está disponível somente na interface **Manage > Full Configuration**.

  Depois de criar as chaves, você pode selecionar uma das chaves na lista. Você não pode alterar a chave depois de criar o catálogo. O Google Cloud não é compatível com a rotação de chaves em imagens ou discos permanentes 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 ficam inutilizáveis até que a chave seja reativada ou restaurada.

9. Na página **Machine Identities**, selecione uma conta do Active Directory e, em seguida, selecione **Next**.
   - Se você selecionar **Create new Active Directory accounts**, selecione um domínio e insira a sequência de caracteres que representa o esquema de nomenclatura para as contas de computador de VMs provisionadas criadas no Active Directory. O esquema de nomenclatura de conta pode conter de 1 a 64 caracteres e não pode conter espaços em branco ou caracteres não ASCII ou especiais.
   - Se você selecionar **Use existing Active Directory accounts**, selecione **Browse** para navegar até as contas de computador existentes do Active Directory para as máquinas selecionadas.
10. Na página **Domain Credentials**, selecione **Enter credentials**, digite o nome de usuário e a senha, selecione **Save** e selecione **Next**.
    - A credencial digitada deve ter permissões para realizar operações na conta do Active Directory.
11. Na página **Scopes**, selecione escopos para o catálogo de máquinas e, em seguida, selecione **Next**.
    - Você pode selecionar escopos opcionais ou selecionar **custom scope** para personalizar os escopos conforme necessário.
12. Na página **Summary**, confirme as informações, especifique um nome para o catálogo e selecione **Finish**.

    > **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 concluída, o catálogo será listado. Você pode verificar se as máquinas foram criadas nos grupos de nós de destino no console do Google Cloud.

Usar PowerShell para 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 parâmetro do PowerShell `New-ProvScheme CustomProperties`.

> **Dica:**
>
> Use o parâmetro PowerShell `New-ProvScheme CustomProperties` somente para conexões de hospedagem baseadas em nuvem. Se você deseja provisionar máquinas usando

> um disco de cache de write-back persistente para uma solução local (por exemplo, Citrix Hypervisor), o PowerShell não é necessário porque o disco persiste automaticamente.

Esse parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas MCS. A propriedade `PersistWBC` só é usada quando o parâmetro `UseWriteBackCache` é especificado, e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco foi criado.

> **Nota:**
>
> Esse comportamento se aplica ao Azure e ao GCP, em que o disco de cache de write-back padrão do MCSIO é excluído e recriado durante o ciclo de energia. Você pode optar por manter o disco para evitar a exclusão e a recriação do disco de cache de write-back do MCSIO.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes do suporte a `PersistWBC` incluem:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

> **Nota:**
>
> Esse exemplo só se aplica ao Azure. As propriedades são diferentes no ambiente do 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 Virtual Apps and Desktops desliga a máquina por meio da interface de gerenciamento.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina por meio da interface de gerenciamento.

> **Nota:**
>
> Se a propriedade`PersistWBC` for omitida, o padrão da propriedade será **false** e o cache de write-back será excluído quando a máquina for desligada por meio da interface de gerenciamento.

Por exemplo, uso do parâmetro `CustomProperties` para definir `PersistWBC` como true:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--NeedCopy-->
```

> **Importante:**
>
> A propriedade `PersistWBC` só pode ser definida usando o cmdlet `New-ProvScheme` do PowerShell. Tentar alterar `CustomProperties` em um esquema de provisionamento após a criação não tem impacto no catálogo da máquina e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, definir `New-ProvScheme` para usar o cache de write-back ao definir a propriedade `PersistWBC` como true:

```
1 New-ProvScheme
2 -CleanOnBoot
3 -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>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
     GoldImages.resourcegroup\W10MCSIO-01
     _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8  "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
      CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
      adSubnetScale1.network" }
```



```
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

Melhorar o desempenho de inicialização com o MCSIO

Você pode melhorar o desempenho de inicialização dos discos gerenciados do Azure e do 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` são:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
       />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
      Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
5 ``` ```<!--NeedCopy-->
6 ```` ```Groups" Value="benvaldev5RG3" />
7 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
      />
8 </CustomProperties>
9 <!--NeedCopy-->
```

Para ativar esse recurso, defina a propriedade personalizada `PersistOSDisk` como **true**. Por exemplo:

```
1 New-ProvScheme
2 -CleanOnBoot
3 -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>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
      GoldImages.resourcegroup\W10MCSIO-01
      _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
```



```
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
       CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
       adSubnetScale1.network" }
9
10  -ProvisioningSchemeName "BV-WBC1-CAT1"
11  -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
       folder\Standard_D2s_v3.serviceoffering"
12  -UseWriteBackCache
13  -WriteBackCacheDiskSize 127
14  -WriteBackCacheMemorySize 256
15  <!--NeedCopy-->
```

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 do hardware são capturadas da VM da imagem mestre ou do instantâneo. Algumas propriedades que você define explicitamente, por exemplo, `StorageType`, `CatalogZones` e `CryptoKeyIs`, 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”`. Esse comando 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.
- Você também pode atualizar a imagem mestre; no entanto, quando você atualiza a imagem mestre, as propriedades do 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 programada é a hora atual.
> - `DurationInMinutes` com um número negativo (por exemplo, —1) indica que não há limite superior na janela de tempo do cronograma.

Criar um catálogo de máquinas com perfil de máquina como modelo de instância

Você pode selecionar um modelo de instância do GCP como uma entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP, portanto, são muito econômicos.

Para criar um novo catálogo de máquinas com perfil de máquina como um modelo de instância usando comandos do PowerShell:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Encontre um modelo de instância em seu projeto do GCP usando o seguinte comando:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Crie um novo catálogo de máquinas com perfil de máquina como 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.template
<!--NeedCopy-->
```

   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 os comandos do PowerShell.

Para alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

   Para obter informações sobre o comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Usar o PowerShell para criar um catálogo com VM protegida

Você pode criar um catálogo de máquinas MCS com propriedades de VM protegida. Uma máquina virtual protegida é reforçada por um conjunto de controles de segurança que fornecem integridade verificável das instâncias do Compute Engine usando recursos avançados de segurança de plataforma, como reinicialização segura, Trusted Platform Module virtual, firmware UEFI e monitoramento de integridade.

O MCS suporta a criação do catálogo usando o fluxo de trabalho do perfil da máquina. Se você usar o fluxo de trabalho do perfil de máquina, deverá habilitar as propriedades de VM protegida de uma instância de VM. Em seguida, você pode usar essa instância de VM como uma entrada de perfil de máquina.

Para criar um catálogo de máquinas MCS com VM protegida usando o fluxo de trabalho do perfil da máquina.

1. Ative as opções de VM protegida de uma instância de VM no console do Google Cloud. Consulte Guia de início rápido: ativar opções de VM protegida.
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 o comando `asnp citrix*` para carregar os módulos do 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
<!--NeedCopy-->
```

3. Conclua a criação do catálogo de máquinas.

Para atualizar o 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
<!--NeedCopy-->
```


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
<!--NeedCopy-->
```

2. Reinicie as VMs.

Importar máquinas do Google Cloud criadas manualmente

Você pode *criar uma conexão com o Google Cloud* e a seguir *criar um catálogo contendo máquinas do Google Cloud*. Em seguida, você pode ligar e desligar manualmente as máquinas do Google Cloud por meio do Citrix DaaS. Com esse recurso, você pode:

- Importar máquinas com SO multissessão do Google Cloud criadas manualmente para um catálogo de máquinas do Citrix Virtual Apps and Desktops.
- Remover as máquinas com SO multissessão do Google Cloud criadas manualmente de um catálogo do Citrix Virtual Apps and Desktops.
- Usar os recursos existentes de gerenciamento de energia do Citrix Virtual Apps and Desktops para gerenciar a energia das máquinas com SO multissessão Windows do Google Cloud. Por exemplo, defina um agendamento de reinicialização para essas máquinas.

Essa funcionalidade não requer alterações no fluxo de trabalho de provisionamento existente do Citrix Virtual Apps and Desktops nem a remoção de qualquer recurso existente. Recomendamos que você use o MCS para provisionar máquinas na interface Full Configuration do Citrix DaaS, 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 boas opções para instalações maiores porque fornecem controle, uso e administração centralizados dos recursos corporativos compartilhados do Google Cloud. Para obter mais informações, consulte o site de documentação do Google.

Com esse recurso, o MCS (Machine Creation Services) oferece suporte ao provisionamento e ao gerenciamento de catálogos de máquinas implantados em VPCs compartilhadas. Esse suporte, que é funcionalmente equivalente ao suporte fornecido atualmente nas VPCs locais, difere em duas áreas:

1. Você deve conceder permissões extras para a conta de serviço usada para criar a conexão de host. Esse processo permite que o MCS acesse e use os recursos da VPC compartilhada.

2. 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 de imagens.

Novas permissões necessárias

É necessária uma conta de serviço do Google Cloud com permissões específicas ao criar a conexão do host. Essas permissões adicionais devem ser concedidas a todas as contas de serviço usadas para criar conexões de host baseadas em VPC compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas no 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 compartilhadas.

No máximo quatro permissões extras devem ser concedidas à conta de serviço associada à conexão de host para aceitar à VPC compartilhada:

1. **compute.firewalls.list** –Essa permissão é obrigatória. Permite que o MCS recupere a lista de regras de firewall presentes na VPC compartilhada.
2. **compute.networks.list** –Essa permissão é obrigatória. Permite que o MCS identifique as redes VPC compartilhadas disponíveis para a conta de serviço.
3. **compute.subnetworks.list** –Essa permissão é opcional, dependendo de como você usa as VPCs. Permite que o MCS identifique as sub-redes nas VPCs compartilhadas visíveis. Essa permissão já é necessária ao usar VPCs locais, mas também deve ser atribuída no projeto host da VPC compartilhada.
4. **compute.subnetworks.use** –Essa permissão é opcional, dependendo de como você usa as VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionadas. Essa permissão já é necessária para usar VPCs locais, mas também deve ser atribuída no projeto host da VPC compartilhada.

Ao usar essas permissões, considere que existem abordagens diferentes com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão no nível do projeto:
  - Permite o acesso a todas as VPCs compartilhadas dentro do projeto host.
  - Requer que as permissões 3 e 4 sejam atribuídas à conta de serviço.
- Permissão no nível da sub-rede:
  - Permite o acesso a sub-redes específicas dentro da VPC compartilhada.
  - As permissões 3 e 4 são intrínsecas à atribuição de nível de sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que corresponde às suas necessidades organizacionais e aos padrões de segurança.

> **Dica:**
>
> Para obter mais informações sobre as diferenças entre as permissões no nível do projeto e no nível da sub-rede, consulte a documentação do Google Cloud.

Regras de firewall

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como o disco do sistema de imagem mestre para o catálogo. Quando esse processo ocorre, o disco é conectado temporariamente a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e de saída. Isso é feito por meio de um par de regras de firewall deny-all: uma para tráfego de entrada e outra para tráfego de saída. Ao usar os VCPs 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 um número mínimo de novas permissões necessárias para usar VPCs compartilhadas. As VPCs compartilhadas são recursos corporativos de nível superior e normalmente têm protocolos de segurança mais rígidos. 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 maior prioridade a elas. Aplique uma nova tag de destino a cada uma das regras, usando o seguinte valor:

```
citrix-provisioning-quarantine-firewall
```

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura regras de firewall que contenham essa tag de destino. Em seguida, ele examina as regras quanto à sua exatidão 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 será exibida:

```
"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 na interface Full Configuration do Citrix DaaS, conclua as etapas a seguir para adicionar contas de serviço do projeto que você pretende provisionar:

1. Crie uma função do IAM.
2. Adicione a conta de serviço usada para criar uma conexão de host CVAD à função do IAM do projeto host da VPC compartilhada.
3. Adicione a conta de serviço do Cloud Build do projeto que você pretende provisionar à função do IAM do projeto host da VPC compartilhada.
4. Crie regras de firewall.

Crie uma função do IAM Determine o nível de acesso da função —*acesso no nível do projeto* ou um modelo mais restrito usando o *acesso no nível da sub-rede*.

Acesso no nível do projeto para a função do IAM. Para a função do IAM no nível do projeto, inclua as seguintes permissões:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função do IAM no nível do projeto:

1. No console do Google Cloud, navegue para **IAM & Admin > Roles**.
2. Na página **Roles**, selecione **CREATE ROLE**.
3. Na página **Create Role**, especifique o nome da função. Selecione **ADD PERMISSIONS**.
   a) Na página **Add permissions**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filter table**. Selecione a permissão e, em seguida, selecione **ADD**.
   b) Selecione **CREATE**.

Subnet-level IAM role. Essa função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` depois de selecionar **CREATE ROLE**. Para esse nível de acesso do IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função do IAM no nível da sub-rede:

1. No console do Google Cloud, navegue para **VPC network** > **Shared VPC**. A página **Shared VPC** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.
2. Na página **Shared VPC**, selecione a sub-rede que deseja acessar.
3. No canto superior direito, selecione **ADD MEMBER** para adicionar uma conta de serviço.
4. Na página **Add members**, conclua estas etapas:
   a) No campo **New members**, digite o nome da sua conta de serviço e selecione a sua conta de serviço no menu.

   b) Selecione o campo **Select a role** e depois **Compute Network User**.
   c) Selecione **SAVE**.

5. No console do Google Cloud, navegue para **IAM & Admin** > **Roles**.
6. Na página **Roles**, selecione **CREATE ROLE**.
7. Na página **Create Role**, especifique o nome da função. Selecione **ADD PERMISSIONS**.

   a) Na página **Add permissions**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filter table**. Selecione a permissão e, em seguida, selecione **ADD**.
   b) Selecione **CREATE**.

Adicionar uma conta de serviço à função do IAM do projeto host Depois de criar uma função do IAM, siga estas etapas para adicionar uma conta de serviço ao projeto host:

1. No console do Google Cloud, navegue até o projeto host e vá para **IAM & Admin > IAM**.
2. Na página **IAM**, selecione **ADD** para adicionar uma conta de serviço.
3. Na página **Add members**:

   a) No campo **New members**, digite o nome da sua conta de serviço e selecione a sua conta de serviço no menu.
   b) Selecione um campo de função, digite a função do IAM que você criou e, em seguida, selecione a função no menu.
   c) Selecione **SAVE**.

Agora, a conta de serviço já está configurada para o projeto host.

Adicionar a conta de serviço do Cloud Build à VPC compartilhada Cada assinatura do Google Cloud tem uma conta de serviço que tem, como nome, o número do ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar qual é o número do ID do projeto selecionando **Home** e **Dashboard** no console do Google Cloud:

Na tela, procure **Project Number** abaixo da área **Project Info**.

Execute as etapas a seguir para adicionar a conta de serviço do Cloud Build à VPC compartilhada:

1. No console do Google Cloud, navegue até o projeto host e vá para **IAM & Admin** > **IAM**.
2. Na página **Permissions**, selecione **ADD** para adicionar uma conta.
3. Na página **Add members**, conclua estas etapas:

   a) No campo **New members**, digite o nome da conta de serviço do Cloud Build e selecione a sua conta de serviço no menu.

b) Selecione o campo **Select a role**, digite `Computer Network User` e, em seguida, selecione a função no menu.
c) Selecione **SAVE**.

Criar regras de firewall Como parte do processo de masterização, o MCS copia a imagem da máquina selecionada e a usa para preparar o disco do sistema de imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que executa scripts de preparação. Essa 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 exige duas regras de firewall *deny all* (uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall em *Host Project* da seguinte forma:

1. No console do Google Cloud, navegue até o projeto host e, em seguida, para **VPC network > Firewall**.
2. Na página **Firewall**, selecione **CREATE FIREWALL RULE**.
3. Na página **Create a firewall rule**, preencha estes dados:
   - **Name**. Digite um nome para a regra.
   - **Network**. Selecione a rede VPC compartilhada à qual a regra de firewall de entrada se aplica.
   - **Priority**. Quanto menor for o valor, maior será a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
   - **Direction of traffic**. Selecione **Ingress**.
   - **Action on match**. Selecione **Deny**.
   - **Targets**. Use o padrão, **Specified target tags**.
   - **Target tags**. Digite `citrix-provisioning-quarantine-firewall`.
   - **Source filter**. Use o padrão, **IP ranges**.
   - **Source IP ranges**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
   - **Protocols and ports**. Selecione **Deny all**.
4. Selecione **CREATE** para criar a regra.
5. Repita as etapas de 1 a 4 para criar outra regra. Em **Direction of traffic**, selecione **Egress**.

Adicionar uma conexão Depois de adicionar as interfaces de rede à instância do Cloud Connector, adicione uma conexão.

Habilitar a seleção de zona

O Citrix DaaS oferece suporte à seleção de zona. Com a seleção de zona, você especifica as zonas nas quais deseja criar as VMs. Com a seleção de zona, os administradores podem colocar nós de locatário

único nas zonas de sua escolha. Para configurar a locação única, você deve fazer o seguinte no Google Cloud:

- Reservar um nó de locatário único no Google Cloud
- Criar a imagem mestre do VDA

Como reservar um nó de locatário único no 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 reservado no grupo de nós. Essas características incluem o número de vGPUs, a quantidade de memória alocada para o 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 executar etapas extras ao criar uma imagem de VM mestre. As instâncias de máquina no Google Cloud têm uma propriedade chamada *node affinity labels*. As instâncias usadas como imagens mestre para catálogos implantados no nó de locatário único exigem um *node affinity label* que corresponda ao nome do **target node group**. Para 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 Definir um rótulo de afinidade de nó ao criar uma instância.
- Para uma instância existente, defina o rótulo usando a linha de comando **gcloud**. Para obter detalhes, consulte Definir um rótulo de afinidade de nó para uma instância existente.

> **Nota:**
>
> Se você pretende usar a locação única com uma VPC compartilhada, consulte Nuvem privada virtual compartilhada.

Definir um rótulo de afinidade de nó ao criar uma instância Para definir o rótulo de afinidade do nó:

1. No console do Google Cloud, navegue até **Compute Engine > VM instances**.
2. Na página **VM instances**, selecione **Create instance**.
3. Na página **Instance creation**, digite ou configure a informação necessária e selecione **management, security, disks, networking, sole tenancy** para abrir o painel de configurações.

4. Na guia **Sole tenancy**, selecione **Browse** para visualizar os grupos de nós disponíveis no projeto atual. A página **Sole-tenant node** é exibida, mostrando uma lista de grupos de nós disponíveis.
5. Na página **Sole-tenant node**, selecione o grupo de nós aplicável na lista e selecione **Select** para voltar à guia **Sole tenancy**. O campo de rótulos de afinidade do nós é preenchido com as informações selecionadas. Essa configuração garante que os catálogos de máquinas criados a partir da instância sejam implantados no grupo de nós selecionado.
6. Selecione **Create** para criar a instância.

Definir um rótulo de afinidade de nó para uma instância existente Para definir o rótulo de afinidade do nó:

1. Na janela de terminal do Google Cloud Shell, use o comando *gcloud compute instances* para definir um rótulo de afinidade de nó. Inclua as seguintes informações no comando **gcloud**:

   - **Nome da VM**. Por exemplo, use uma VM existente chamada `s*2019-vda-base`.*
   - **Nome do grupo de nós**. Use o nome do grupo de nós que você criou anteriormente. Por exemplo, `mh-sole-tenant-node-group-1`.
   - **A zona em que a instância reside**. Por exemplo, a VM reside em `*us-east-1b* zone`.

   Por exemplo, digite o seguinte comando na janela do terminal:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Para obter mais informações sobre o comando *gcloud compute instances*, consulte a documentação do Google Developer Tools em https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Navegue até a página **VM instance details** da instância e verifique se o campo **Node Affinities** é preenchido com o rótulo.

Criar um catálogo de máquinas Depois de definir o rótulo de afinidade do nó, configure o catálogo de máquinas.

Usar chaves de criptografia gerenciadas pelo cliente (CMEK)

Você pode usar chaves de criptografia gerenciadas pelo cliente (CMEK) para catálogos do MCS. Ao usar essa funcionalidade, você atribui a função `CryptoKey Encrypter/Decrypter` do serviço Key Management Service do Google Cloud ao agente de serviço do Compute Engine. A conta Citrix DaaS deve ter as permissões corretas no projeto em que a chave está armazenada. Consulte Ajudar 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`. Esse formulário é diferente da conta de serviço padrão do Compute Engine.

> **Nota:**
>
> Essa conta de serviço do Compute Engine talvez não apareça na tela **IAM Permissions** do Google Console. Nesse caso, use o comando `gcloud` conforme descrito em Ajudar a proteger recursos usando chaves do Cloud KMS.

Atribuir permissões à conta Citrix DaaS

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões de KMS no *nível do projeto* ou permissões de KMS no *nível do recurso*. Consulte Permissões e funções para obter mais informações.

Permissões no nível do projeto Uma opção é fornecer à conta Citrix DaaS permissões no nível do projeto para navegar pelos recursos do Cloud KMS. Para isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua essa função personalizada à sua conta Citrix DaaS. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

Permissões de nível do recurso Na outra opção, de permissões no nível do recurso, no console do Google Cloud, navegue até a `cryptoKey` que você usa para o provisionamento de MCS. Adicione uma conta Citrix DaaS a um keyring ou chave que você usa para provisionamento de catálogo.

> **Dica:**
>
> Com essa opção, você não pode procurar chaves regionais para o seu projeto no inventário porque a conta do Citrix DaaS não tem permissões de lista de nível do projeto nos recursos do Cloud KMS. No entanto, você ainda pode provisionar um catálogo usando o CMEK especificando o `cryptoKeyId` correto nas propriedades personalizadas `ProvScheme`, como descrito abaixo.

Provisionar com CMEK usando propriedades personalizadas

Ao criar o 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>'
<!--NeedCopy-->
```

`cryptoKeyId` deve ser especificada no seguinte formato:

`projectId:location:keyRingName:cryptoKeyName`

Por exemplo, se você quiser usar a chave `my-example-key` no keyring `my-example-key-ring` na região `us-east1` e no projeto com ID `my-example-project-1`, suas configurações personalizadas `ProvScheme` serão 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>'
<!--NeedCopy-->
```

Todas as imagens e discos provisionados do MCS relacionados a esse esquema de provisionamento usam essa chave de criptografia gerenciada pelo cliente.

> **Dica:**
>
> Se você usar chaves globais, o local das propriedades do cliente deverá indicar `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"/>`.

Rotação de chaves gerenciadas pelo cliente

O Google Cloud não é compatível com a rotação de chaves em imagens ou discos permanentes existentes. Depois que uma máquina é provisionada, ela é 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 keyrings Os keyrings não podem ser renomeados ou excluídos. Além disso, você pode incorrer em encargos imprevistos ao configurá-los. Ao excluir ou remover um keyring, 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.
<!--NeedCopy-->
```

> **Dica:**
>
> Para obter mais informações, consulte Editing or deleting a key ring from the console.

Compatibilidade de acesso uniforme no nível do 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 do IAM que concede permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com 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 no Google Cloud. Para obter informações de configuração, consulte Requerer acesso uniforme no nível do bucket.

Google Cloud Marketplace

Você pode navegar e selecionar imagens oferecidas pela Citrix no Google Cloud Marketplace para criar catálogos de máquinas. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso.

Para pesquisar o produto Citrix VDA VM no Google Cloud Marketplace, acesse https://console.cloud.google.com/marketplace/.

Você pode usar uma imagem personalizada ou uma imagem pronta da Citrix no Google Cloud Marketplace para atualizar uma imagem de um catálogo de máquinas.

> **Nota:**
>
> Se o perfil da máquina não contiver informações sobre o tipo de armazenamento, o valor será derivado das propriedades personalizadas.

As imagens compatíveis do Google Cloud Marketplace são:

- Windows 2019 Single Session
- Windows 2019 Multi Session
- Ubuntu

Exemplo de uso de uma imagem pronta da 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
<!--NeedCopy-->
```

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 Google Cloud Platform.

Mais informações

- Conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas

Criar um catálogo de máquinas do HPE Moonshot (prévia)

December 6, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes HPE Moonshot.

> **Nota:**
>
> - Crie 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 OS Deployment on Moonshot User Guide.

Você pode criar um catálogo de máquinas do HPE Moonshot usando:

- Interface Full Configuration
- Comandos do PowerShell

Criar um catálogo de máquinas usando a interface Full Configuration

No assistente **Machine Catalog Setup**:

1. Na página **Operating System**, selecione **Multi-session OS** ou **Single-session OS**.
2. Na página **Machine Management**, selecione **Machines that are power managed** e **Another service or technology**.
3. Na página **Virtual Machines**, adicione máquinas e suas contas de máquinas do Active Directory. Você pode fazer o seguinte:
   - Clique em **Add Machines** para adicionar máquinas manualmente. A janela **Select 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 máquinas associadas.
   - Clique em **Add CSV File** 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 **Scopes** e **Summary** não contêm informações específicas do HPE Moonshot.

Criar um catálogo de máquinas usando comandos do PowerShell

Execute os comandos `New-BrokerCatalog` e `New-BrokerMachine` do PowerShell para criar um catálogo de agentes e importar máquinas para o catálogo do agente.

Por exemplo:


```
1 New-BrokerCatalog  -AdminAddress "localhost:19097" -AdminClientIP "
    103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine  -AdminAddress "localhost:19097" -AdminClientIP "
    103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

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 HPE Moonshot.

Mais informações

- Criar e gerenciar conexões
- Conexão com o HPE Moonshot
- Criar catálogos de máquinas

Criar um catálogo do Microsoft Azure

December 20, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem 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 por meio de uma imagem do Azure Resource Manager

Essas informações são um complemento às orientações em Criar catálogos de máquinas.

Uma imagem pode ser um disco, um instantâneo ou a versão imagem de uma definição de imagem na 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. Para obter informações gerais sobre imagens, consulte Criar catálogos de máquinas.

> **Dica:**
>
> O uso de disco não gerenciado para provisionar a VM está preterido.

Durante a preparação da imagem, uma máquina virtual (VM) de preparação é criada com base na VM original. Essa VM de preparação está 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. 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`, sendo o GUID gerado aleatoriamente. Por exemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

No assistente de criação de catálogo de máquinas:

- As páginas **Create machine catalogs** e **Machine Management** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Master Image**, selecione uma imagem que você deseja usar como imagem mestre para todas as máquinas no catálogo. O assistente **Select an image** é exibido. Siga estas etapas para selecionar uma imagem:

  1. (Aplicável somente às conexões configuradas com imagens compartilhadas com ou entre locatários) Selecione a assinatura em que a imagem reside.
  2. Selecione um grupo de recursos.
  3. Navegue até o Azure VHD, a Galeria de Computação do Azure ou a versão de imagem do Azure.

  Ao selecionar uma imagem, considere o seguinte:

  - Verifique se um Citrix VDA está instalado na imagem.
  - Se você selecionar um VHD conectado a uma VM, deverá desligá-la 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 Galeria de Computação do Azure compartilhada com essa assinatura. Nessas assinaturas, somente galerias compartilhadas são exibidas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens com um locatário (entre assinaturas) e Compartilhar imagens entre locatários.

- O uso de um perfil de máquina com início confiável como **Security Type** é obrigatório quando você seleciona uma imagem ou instantâneo com início confiável habilitado. Em seguida, você pode ativar ou desativar o SecureBoot e o vTPM especificando seus valores no Perfil de Máquina. Para obter informações sobre o início confiável do Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- Você pode criar um esquema de provisionamento usando o disco de SO efêmero no Windows com início confiável. Ao selecionar uma imagem com início confiável, você deve selecionar um perfil de máquina com início confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando o disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
- Quando a replicação de imagem está em andamento, você pode prosseguir e selecionar a imagem como a imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode demorar mais para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída dentro de uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo não se completará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.
- Quando você seleciona 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 sistema operacional Windows, no tipo de segurança, no suporte à hibernação e no ID do conjunto de criptografia de disco da imagem mestre.
- Você pode provisionar um catálogo de VM 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 antiga que não tenha informações de geração é uma imagem Gen1.

Escolha se você deseja que as VMs no catálogo herdem as configurações de um perfil de máquina. Por padrão, a caixa de seleção **Use a machine profile (mandatory for Azure Active Directory)** está mercada. Clique em **Select a machine profile** para navegar até a especificação de uma VM ou modelo ARM a partir de uma lista de grupos de recursos.

Valide a especificação do modelo ARM para garantir que possa 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. Há 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 **Next**. Mensagens de erro são exibidas 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
<!--NeedCopy-->
```

Exemplos de configurações que as máquinas virtuais podem herdar de um perfil de máquina incluem:

- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado aos discos OS e MCSIO)
- Tamanho da máquina (salvo indicação em contrário)
- Tags colocadas na VM

Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Machine Catalogs**, selecione o catálogo para exibir seus detalhes no painel inferior. Em seguida, clique na guia **Template Properties** 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 **View all**.

Se desejar que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Use a host group** 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. Quando você usa 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 precisa atender aos requisitos regulamentares ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

> **Importante:**
>
> - Somente são exibidos os grupos de hosts que têm o posicionamento automático do Azure habilitado.
> - O uso de um grupo de hosts altera a página **Virtual Machines** oferecida posterior-

> mente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são mostrados nessa página. Além disso, as zonas de disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Storage and License Types** só aparece quando você usa uma imagem do Azure Resource Manager.

  Os seguintes tipos de armazenamento podem ser usados no catálogo de máquinas:

  - **Premium SSD**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência adequada para VMs com cargas de trabalho intensivas de E/S.
  - **Standard SSD**. 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.
  - **Azure ephemeral OS disk**. 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. Leve em consideração os seguintes aspectos ao usar um disco de SO efêmero:
    * O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados 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.
    * Não é possível usar a opção **Retain VM and system disk during power cycless** oferecida posteriormente no assistente.

> **Nota:**
>
> O disco de identidade é sempre criado usando SSD Standard, independentemente do tipo de armazenamento que você escolher.

O tipo de armazenamento determina quais tamanhos de máquina são oferecidos na página **Máquinas Virtuais** do assistente. O MCS configura discos premium e padrão para usar o Armazenamento com Redundância Local (LRS). O LRS faz várias cópias síncronas dos dados do disco em um único data center. Os discos de SO efêmeros do Azure usam o disco local das VMs para armazenar o sistema operacional. Para obter detalhes sobre os tipos de armazenamento do Azure e a replicação de armazenamento, consulte o seguinte:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/

- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selecione se deseja usar as licenças existentes do Windows ou do Linux.

- Licenças do Windows: o uso de licenças do Windows junto com imagens do Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs do Windows no Azure a um custo reduzido. Existem dois tipos de licenças:
  * **Windows Server license**. Possibilita que você use suas licenças do Windows Server ou do Azure Windows Server, permitindo que você use os Benefícios Híbridos do Azure. Para obter detalhes, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. O Azure Hybrid Benefit reduz o custo de execução de VMs no Azure para a taxa de computação básica, dispensando o custo de licenças extras do Windows Server da galeria do Azure.
  * **Windows Client license**. Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e do Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de acesso para cliente e licenças de gerenciamento.

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando do 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/en-us/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/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Como alternativa, você pode usar o SDK PowerShell `Get-Provscheme` para fazer a verificação. Por exemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre esse cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenças do Linux: com as licenças BYOS (traga sua própria assinatura) do Linux, você não precisa pagar pelo software. A cobrança da 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 na 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 como RHEL_BYOS em `New-ProvScheme`:

```
1 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>'
2 <!--NeedCopy-->
```

Exemplo de configuração de LicenseType como SLES_BYOS em `Set-ProvScheme`:

```
1 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>'
2 <!--NeedCopy-->
```

> **Nota:**
>
> Se o valor `LicenseType` estiver vazio, os valores padrão serão Azure Windows Server License ou Azure Linux License, dependendo do valor de OsType.

Exemplo de configuração de LicenseType como vazio:

```
1 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>'
2 <!--NeedCopy-->
```


Consulte os seguintes documentos para entender os tipos de licença e seus benefícios:

- 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

A Galeria de Computação do Azure é um repositório para gerenciar e compartilhar imagens. Ele permite que você disponibilize suas imagens em toda a organização. Recomendamos que você armazene uma imagem na Galeria de Computação do Azure ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos de SO VDA. Depois que você selecionar **Place prepared image in Azure Compute Gallery**, aparece a seção **Azure Compute Gallery settings**, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

- **Ratio of virtual machines to image replicas**. Permite especificar a proporção de máquinas virtuais para réplicas de imagem que você deseja que o Azure mantenha. Por padrão, o Azure mantém uma única réplica de imagem para cada 40 máquinas não persistentes. Em máquinas persistentes, o número assume o valor padrão 1.000.
- **Maximum replica count**. Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 10.

- Na página **Virtual Machines**, indique quantas VMs você deseja criar. Você deve especificar pelo menos um e selecionar um tamanho de máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.
- A página **NICs** não contém informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Disk Settings**, escolha se deseja ativar o cache write-back. Com o recurso de otimização de armazenamento do MCS ativado, você pode definir as seguintes configurações ao criar um catálogo: Essas configurações se aplicam aos ambientes Azure e GCP.

  Depois de ativar o cache de write-back, você pode fazer o seguinte:

  - Configurar o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
  - Selecionar 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:
    * Premium SSD
    * Standard SSD
    * Standard HDD

- Escolha se deseja que o disco de cache write-back persista para as VMs provisionadas. Selecione **Enable write-back cache** para disponibilizar as opções. Por padrão, a opção **Use non-persistent write-back cache disk** está selecionada.
- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/
- Selecione o tipo para o disco de cache de write-back.
  * **Use non-persistent write-back cache disk**. Se selecionado, o disco de cache write-back é excluído durante os ciclos de alimentação de energia. Todos os dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache 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 **Template Properties**. Se o disco temporário for usado, você verá **Non-persistent Write-back Cache Disk** e seu valor será **Yes (using VM's temporary disk)**. Caso contrário, você verá **Non-persistent Write-back Cache Disk** e seu valor será **No (not using VM's temporary disk)**.
  * **Use persistent write-back cache disk**. Se selecionado, o disco de cache de write-back persistirá para as VMs provisionadas. Habilitar a opção aumenta os custos de armazenamento.
- Escolha se deseja reter VMs e discos do sistema para VDAs durante os ciclos de alimentação de energia.

  Retain VM and system disk during power cycles. Disponível quando você seleciona **Enable write-back cache**. Por padrão, VMs e discos de sistema são excluídos no desligamento e recriados na inicialização. Se você quiser reduzir o tempo de reinicialização da VM, selecione essa opção. Lembre-se de que ativar essa opção também aumenta os custos de armazenamento.
- Escolha se deseja ativar a economia de custos de armazenamento selecionando **Enable storage cost saving**. Se ativada, economize nos custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Standard quando a VM for desligada. A VM muda para suas configurações originais na reinicialização. A opção se aplica aos discos de armazenamento e cache de write-back. Como alternativa, 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 as mudanças no tipo de armazenamento no futuro. Para obter mais informações, consulte este artigo da Microsoft.

  - Escolha se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia no 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 no catálogo. Para obter mais informações, consulte Criptografia do servidor do Azure.

- Na página **Resource Group**, escolha se deseja criar grupos de recursos ou usar grupos existentes.

  - Se você optar por criar grupos de recursos, selecione **Next**.
  - Se você optar por usar grupos de recursos existentes, selecione grupos na lista **Available Provisioning Resource Groups**. **Lembre-se**: selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Será exibida uma mensagem se você escolher muito poucos. Talvez você queira selecionar mais do que o mínimo necessário se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que o catálogo é criado.

  Para obter mais informações, consulte Azure resource groups.

- Na página **Machine Identities**, escolha um tipo de identidade e configure identidades para máquinas nesse catálogo. Se você selecionar as VMs como **Azure Active Directory joined**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:

  1. No campo **Identity type**, selecione **Azure Active Directory joined**. A opção **Azure AD security group (optional)** é exibida.
  2. Clique em **Azure AD security group: Create new**.
  3. Insira o nome do grupo e clique em **Create**.
  4. Siga as instruções na tela para fazer logon no Azure.
     Se o nome do grupo não existir no Azure, um ícone verde é exibido. Caso contrário, uma mensagem de erro é exibida solicitando que você insira um novo nome.
  5. Para adicionar o grupo de segurança a um grupo de segurança atribuído, selecione **Join an assigned security group as a member** e clique em **Select a group** para escolher um grupo atribuído para ingressar.
  6. Insira o esquema de nomenclatura da conta da máquina para as VMs.

Após a criação do catálogo, o Citrix DaaS acessa o Azure em seu nome 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 no catálogo são adicionadas automaticamente ao grupo de segurança.

Adicionar VMs com um esquema de nomenclatura diferente a esse catálogo exige que você entre no Azure. O Citrix DaaS pode então acessar o Azure e criar uma regra de associação dinâmica com base no novo esquema de nomenclatura.

Ao excluir esse catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.

> **Nota:**
>
> Para renomear o grupo de segurança do Azure AD após a criação do catálogo, edite o catálogo e acesse **Azure AD Security Group** na navegação à esquerda. Os nomes dos grupos de segurança do Azure AD não devem conter os seguintes caracteres: `@ "\ / ; : # . * ? = < > | [ ] ( )'`.

- As páginas **Domain Credentials** e **Summary** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.

Conclua o assistente.

Condições para que o disco temporário do Azure seja elegível para disco de cache write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem atendidas:

- 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 escolhido da VM do Azure deve incluir um disco temporário.
- Não é necessário ativar o disco de SO efêmero
- Aceite 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 do cache de write-back + espaço reservado para o arquivo de paginação + 1 GB de espaço no buffer).

Usar PowerShell para criar um catálogo 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 do PowerShell `New-ProvScheme CustomProperties`. As propriedades personalizadas são:

- `UseTempDiskForWBC`. Essa propriedade indica se você está aceitando usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como true durante a execução `New-ProvScheme` se você quiser usar o disco temporário como disco de cache write-back. Se essa propriedade não for especificada, o parâmetro será definido como False por padrão.

Por exemplo, uso do 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>'
<!--NeedCopy-->
```

> **Nota:**
>
> Depois de confirmar o catálogo da máquina para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar o VHD posteriormente.

Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back durante a criação do catálogo de máquinas.

Cenário	Resultado
Todas as condições para usar o disco temporário para cache write-back estão satisfeitas.	O arquivo WBC `mcsdif.vhdx` é colocado no disco temporário.
O disco temporário não tem espaço suficiente para o uso do cache write-back.	É criado um disco VHD ‘MCSWCDisk’e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

Cenário	Resultado
O disco temporário tem espaço suficiente para o uso do cache write-back, mas `UseTempDiskForWBC` está definido como false.	É criado um disco VHD 'MCSWCDisk'e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

Usar PowerShell para 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 parâmetro do PowerShell `New-ProvScheme CustomProperties`.

> **Dica:**
>
> Use o parâmetro PowerShell `New-ProvScheme CustomProperties` somente para conexões de hospedagem baseadas em nuvem. Se você deseja provisionar máquinas usando um disco de cache de write-back persistente para uma solução local (por exemplo, Citrix Hypervisor), o PowerShell não é necessário porque o disco persiste automaticamente.

Esse parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas MCS. A propriedade `PersistWBC` só é usada quando o parâmetro `UseWriteBackCache` é especificado, e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco foi criado.

> **Nota:**
>
> Esse comportamento se aplica ao Azure e ao GCP, em que o disco de cache de write-back padrão do MCSIO é excluído e recriado durante o ciclo de energia. Você pode optar por manter o disco para evitar a exclusão e a recriação do disco de cache de write-back do MCSIO.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes do suporte a `PersistWBC` incluem:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```


> **Nota:**
>
> Esse exemplo só se aplica ao Azure. As propriedades são diferentes no ambiente do 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 Virtual Apps and Desktops desliga a máquina por meio da interface de gerenciamento.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina por meio da interface de gerenciamento.

> **Nota:**
>
> Se a propriedade`PersistWBC` for omitida, o padrão da propriedade será **false** e o cache de write-back será excluído quando a máquina for desligada por meio da interface de gerenciamento.

Por exemplo, uso do parâmetro `CustomProperties` para definir `PersistWBC` como true:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--NeedCopy-->
```

> **Importante:**
>
> A propriedade `PersistWBC` só pode ser definida usando o cmdlet `New-ProvScheme` do PowerShell. Tentar alterar `CustomProperties` em um esquema de provisionamento após a criação não tem impacto no catálogo da máquina e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, definir `New-ProvScheme` para usar o cache de write-back ao definir a propriedade `PersistWBC` como true:

```
1 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\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Melhorar o desempenho de inicialização com o MCSIO

Você pode melhorar o desempenho de inicialização dos discos gerenciados do Azure e do 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` são:

```
<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<!--NeedCopy-->
``<!--NeedCopy-->
```Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
```


```

```
8 </CustomProperties>
9 <!--NeedCopy-->
```

Para ativar esse recurso, defina a propriedade personalizada `PersistOSDisk` como **true**. Por exemplo:

```
1  New-ProvScheme
2  -CleanOnBoot
3  -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>"
4  -HostingUnitName "adSubnetScale1"
5  -IdentityPoolName "BV-WBC1-CAT1"
6  -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
      GoldImages.resourcegroup\W10MCSIO-01
      _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7  -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
       CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
       adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la na interface **Full configuration** e nos 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. Acesse o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a interface de rede e a VM. No menu **...**, na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Include parameters** se quiser criar uma especificação de modelo para o provisionamento de catálogos.
3. Clique em **Adicionar à biblioteca** para modificar a especificação do modelo posteriormente.

4. Na página **Importando modelos**, insira as informações necessárias, como **Nome**, **Assinatura**, **Grupo de recursos**, **Local** e **Versão**. Clique em **Próximo: Editar modelo**.
5. Você também precisa de uma interface de rede como um recurso independente se quiser provisionar catálogos. Portanto, você deve remover todos os `dependsOn` especificados na especificação do modelo. Por exemplo:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. Crie **Revisar+Criar** e crie a especificação do modelo.
7. Na página **Especificações do modelo**, verifique a especificação do modelo que você acabou de criar. Clique na especificação do modelo. No painel esquerdo, clique em **Versões**.
8. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação do modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação do modelo.

Você pode obter informações sobre a especificação e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação do modelo, execute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Para obter informações sobre a versão da especificação do modelo, execute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

Usar a especificação do 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 usar a interface **Full Configuration** ou os comandos do PowerShell.

Usando a interface **Full Configuration**: consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Usando comandos do PowerShell:

1. Abra uma 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>
[-LoggingId <Guid>]
[-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

     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/EastUs.region/vm.folder/MasterDisk.vm'
MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'
[-ProvisioningSchemeName] <String>
[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]
[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>] [<CommonParameters>]
<!--NeedCopy-->
```

Catálogos de máquinas com início confiável

Para criar com êxito um catálogo de máquinas com início confiável, use:

- Um perfil de máquina com início confiável
- Um tamanho de VM que ofereça suporte ao início confiável
- Uma versão de Windows VM que ofereça suporte ao início confiável Atualmente, o Windows 10, 2016, 2019 e 2022 oferecem suporte ao início confiável.

> **Importante:**
>
> O início confiável requer a criação de novas VMs. Você não pode ativar o início confiável em VMs existentes que foram inicialmente criadas sem ele.

Para exibir os itens de inventário da oferta do Citrix DaaS e determinar se o tamanho da VM suporta o início confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
3. Execute o seguinte comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
   - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM é compatível com o início confiável.
   - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não é compatível com o início confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que suportam o início confiável:

```
(Get-AzComputeResourceSku | where {
 $\_.Locations.Contains($region) -and ($\_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Veja a seguir exemplos que descrevem se o tamanho da VM oferece ou não suporte ao início confiável após a execução do comando do Azure PowerShell.

- *Exemplo 1*: se a VM do Azure oferecer suporte somente à Geração 1, a VM não é compatível com o início confiável. Portanto, o recurso `TrustedLaunchDisabled` não é exibido depois que você executa o comando do Azure PowerShell.
- *Exemplo 2*: se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` for **True**, o tamanho da VM de Geração 2 não é compatível com o início confiável.
- *Exemplo 3*: se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` não for exibido após a execução do comando PowerShell, o tamanho da VM de Geração 2 não é compatível com o início confiável.

Para obter mais informações sobre o início confiável de máquinas virtuais do Azure, consulte o documento da Microsoft Início confiável para máquinas virtuais do Azure.

Erros ao criar catálogos de máquinas com o início confiável

Você verá os erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com início confiável:

Cenário	Erro
Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado	`MachineProfileNotSupportedForUnmanagedCata`
Se você selecionar um perfil de máquina compatível com início confiável ao criar um catálogo com disco não gerenciado como imagem mestre	`SecurityTypeNotSupportedForUnmanagedDisk`
Se você não selecionar um perfil de máquina ao criar um catálogo gerenciado com a origem de uma imagem mestre com início confiável como o tipo de segurança	`MachineProfileNotFoundForTrustedLaunchMaste`
Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre	`SecurityTypeConflictBetweenMasterImageAndMa`
Se você selecionar um tamanho de VM que não ofereça suporte ao início confiável, mas usar uma imagem mestre compatível com início confiável ao criar um catálogo	`MachineSizeNotSupportTrustedLaunch`

Usar valores de propriedade do perfil da máquina

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

- Zona de disponibilidade
- ID do grupo de hosts dedicados
- ID do conjunto de criptografia de disco
- Tipo de sistema operacional
- Tipo de licença
- Tipo de armazenamento

Se essas propriedades personalizadas não forem definidas explicitamente, os valores da propriedade serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como o 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 no perfil da máquina e não estiverem definidas nas propriedades personalizadas, os valores padrão das propriedades serão usados sempre que aplicável.

A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` tem todas as propriedades definidas ou os valores são derivados de MachineProfile.

- Cenário 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 valores a seguir são definidos como propriedades personalizadas para o catálogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
          machinecreation" xmlns:xsi="http://www.w3.org/2001/
          XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
          -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
          "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
          " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
          DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
          value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

  - MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem somente LicenseType e OsType.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Os valores a seguir 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>
<!--NeedCopy-->
```

- 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 valores a seguir 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>
<!--NeedCopy-->
```

- 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 valores a seguir 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>
<!--NeedCopy-->
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não está definida. Exemplo:
  * CustomProperties definem StorageType
  * MachineProfile define LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

Os valores a seguir 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>
<!--NeedCopy-->
```

- Se OsType não estiver em CustomProperties nem em MachineProfile, então:
  * O valor é lido a partir da imagem mestre.
  * Se a imagem mestre for um disco não gerenciado, OsType será 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, nesse 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>
<!--NeedCopy-->
```

- Cenários Set-ProvScheme
  - Um catálogo existente com:
    - CustomProperties para `StorageAccountType` e OsType
    - MachineProfile `mpA.vm` que define Zones
  - Atualizações:
    - MachineProfile 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 valores a seguir 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>
<!--NeedCopy-->
```

  - Um catálogo existente com:
    - CustomProperties para `StorageAccountType` e OsType
    - MachineProfile `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 valores a seguir 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>
<!--NeedCopy-->
```

- Um catálogo existente com:
  * CustomProperties para `StorageAccountType` e OsType
  * MachineProfile `mpA.vm` que define Zones
- Atualizações:
  * Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  * `ServiceOffering` não está especificado

  `Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

  Os valores a seguir 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>
<!--NeedCopy-->
```


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 do 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 não baseado em perfil de 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 e grupo de segurança de rede 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, ocorrerá um erro.

Você pode recuperar o número máximo de NICs associadas a um tamanho de VM selecionado. Uma propriedade PowerShell chamada `MaxNetworkInterfaces` exibe a contagem máxima da NIC quando você executa o comando `get-item` do PowerShell com o parâmetro `AdditionalData`.

Recuperar a contagem máxima da NIC

Para recuperar a contagem máxima da NIC:

1. Abra uma janela do **PowerShell** no host Delivery Controller.
2. Execute o comando `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 da NIC.

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 no host Delivery Controller.
2. Execute o comando `asnp citrix*` para carregar os módulos do 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" }

     <!--NeedCopy-->
     ```

   - 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 que tenha várias NICs. Você também pode criar uma nova VM e anexar uma interface de rede na página de Rede do portal do Azure.

     b) Execute o comando `New-ProvScheme` com a VM como uma 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 `NetworkInterfaceCount` do perfil da 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 Delivery Controller.
2. Execute o comando `asnp citrix*` para carregar os módulos do 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" }

<!--NeedCopy-->
```

- Se estiver criando um catálogo de máquinas com base 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 que tenha várias NICs.
  b) Execute o comando `Set-ProvScheme` com a VM como uma 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 executar o ciclo de alimentação de energia na VM existente durante a janela de tempo de atualização. Para obter mais informações sobre a atualização de uma VM existente, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Provisionar VMs do catálogo com o agente do Azure Monitor instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e atuar nos dados de telemetria de seus ambientes do Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos computacionais, como máquinas virtuais, e entrega os dados para o Azure Monitor. Atualmente, ele oferece suporte à coleção de métricas de Logs de eventos, Syslog e Desempenho e a envia para fontes de dados do Azure Monitor Metrics e do Azure Monitor Logs.

Para habilitar o monitoramento identificando de forma exclusiva 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: verifique se você tem 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 um DCR, consulte Criar uma regra de coleta de dados. Um DCR é específico da plataforma (Windows ou Linux). Certifique-se de criar um DCR de acordo com a plataforma necessária.
  A 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 espaço de trabalho, consulte Criar um espaço de trabalho do Log Analytics. Quando você coleta logs e dados, as informações são armazenadas em um espaço de trabalho. Um espaço de trabalho tem um ID de espaço de trabalho e um ID de recurso exclusivos. O nome do espaço de trabalho deve ser exclusivo para um determinado grupo de recursos. Depois de criar um espaço de trabalho, configure fontes de dados e soluções para armazenar seus dados no espaço de trabalho.
- Incluiu a extensão do monitor na lista branca: as extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões definidas na lista branca da Citrix. Para ver a lista de extensões na lista branca, use o comando PoSH `Get-ProvMetadataConfiguration`.
- Imagem mestre: 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 poderá levar a arquivos remanescentes e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para provisionar VMs de catálogo com o AMA ativado:

1. Configure um modelo de perfil de máquina.
   - Se você quiser usar uma máquina virtual 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 **Resources**. Isso invoca a instalação do agente na VM modelo.

   > **Nota:**
   >
   > Se você precisar criar um catálogo Linux, configure uma máquina Linux.

   - Se você quiser usar a especificação do modelo como modelo de um perfil de máquina:

a) Configure uma especificação de modelo.

b) Adicione a seguinte associação de extensão e regra de coleta de dados à especificação do modelo gerado:

```
{

"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>"
      }

     }

<!--NeedCopy-->
```

2. Crie ou atualize um catálogo de máquinas MCS existente.

- Para criar um novo catálogo MCS:
  a) Selecione a especificação de VM ou modelo como um perfil de máquina na interface Full Configuration.
  b) Continue com as próximas etapas para criar o catálogo.
- Para atualizar um catálogo MCS existente, use os seguintes comandos PoSH:
  - Para que as novas VMs obtenham o modelo de perfil de máquina atualizado, execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName "name"
-MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-machine-profile.vm"
<!--NeedCopy-->
```

  - Para atualizar as VMs existentes com o modelo de perfil de máquina atualizado:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

3. Ligue as máquinas virtuais do catálogo.
4. Acesse o portal do Azure e verifique se a extensão do monitor está instalada na VM e se a VM aparece nos recursos do DCR. Depois de alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

Solução de problemas

Para obter informações para orientar a solução de problemas do agente do Azure Monitor, consulte o seguinte:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Usar o PowerShell para habilitar extensões de VM do Azure

Depois de selecionar a especificação do modelo ARM, execute os seguintes comandos do PowerShell para trabalhar com as extensões de VM do Azure:

- Para exibir a lista de extensões de VM do Azure com suporte: `Get-ProvMetadataConfiguration`

- Para adicionar mais extensões de VM: `Add-ProvMetadataConfiguration`. For example, `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  Se você tentar adicionar qualquer um dos itens a seguir, 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.

Localização do arquivo de paginação

Em ambientes do Azure, o local do arquivo de paginação é configurado quando você cria uma máquina virtual pela primeira vez. O formato da configuração do arquivo de paginação é: localização do arquivo de paginação [tamanho mínimo] [tamanho máximo] (o tamanho em MB). Para obter mais informações, consulte Como determinar o tamanho do arquivo de paginação apropriado.

Durante a preparação da imagem, quando você cria o esquema de provisionamento, o MCS determina a localização do arquivo de paginação com base em determinadas regras. Depois de criar o esquema de provisionamento, você não pode:

- Alterar o tamanho da máquina virtual
- Atualizar o perfil da máquina
- Alterar as propriedades EOS e MCS I/O

Determinação da localização do arquivo de paginação

Recursos como EOS e MCS I/O têm seu próprio local de arquivo de paginação esperado e são exclusivos entre si. A tabela a seguir mostra a localização esperada do arquivo de paginação para cada recurso:

Recurso	Local esperado do arquivo de paginação
EOS	Disco do sistema operacional
MCS I/O	Disco temporário do Azure primeiro, caso contrário, disco de cache de write-back

> **Nota:**
>
> Mesmo que você dissocie a preparação da imagem da criação do esquema de provisionamento, o MCS determina corretamente o local do arquivo de paginação. O local padrão do arquivo de paginação é o disco do SO.

Cenários de configuração do arquivo de paginação

A tabela a seguir descreve alguns dos cenários possíveis 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 de imagem de origem no disco temporário, enquanto o tamanho da máquina virtual especificado no esquema de provisionamento não tem disco temporário	O arquivo de paginação é colocado no SO
Preparação da imagem	Você define o arquivo de página de imagem de origem no disco do SO, enquanto o tamanho da VM especificado 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 de imagem de origem no disco temporário e ativa o disco de 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. O tamanho original da máquina virtual tem um disco temporário, enquanto a máquina virtual de destino não tem um disco temporário	Rejeita a alteração com uma mensagem de erro

Durante	Cenário	Resultado
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento. O tamanho original da máquina virtual não tem um disco temporário, enquanto a máquina virtual de destino tem um disco temporário	Rejeita a alteração com uma mensagem de erro

Atualizar configuração do arquivo de paginação

Usando os comandos do 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. Você pode fazer isso executando o seguinte comando `New-ProvScheme` durante a criação do catálogo de máquinas:

```
New-ProvScheme -CleanOnBoot `
    -HostingUnitName "zijinnet" `
    -IdentityPoolName "PageFileSettingExample" `
    -ProvisioningSchemeName "PageFileSettingExample" `
    -InitialBatchSizeHint 1 `
    -MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.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>'
<!--NeedCopy-->
```

Para obter informações sobre como criar um catálogo usando o SDK Remoto do PowerShell, consulte Creating a catalog using PowerShell.

Restrições:

- Você pode atualizar a configuração do arquivo de paginação quando você cria o esquema de provisionamento executando o comando `New-ProvScheme`. Não é possível alterar a configuração do arquivo de paginação posteriormente.
- Você deve fornecer todas as propriedades personalizadas (‘PageFileDiskDriveLetterOverride’ , ‘InitialPageFileSizeInMB’e ‘MaxPageFileSizeInMB’) no comando `New-ProvScheme` ou nenhuma delas.
- Esse recurso não é compatível no 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 do arquivo de paginação inicial e o tamanho máximo do arquivo de paginação como zero ao mesmo tempo.

Grupos de recursos do Azure

Os grupos de recursos de provisionamento do Azure fornecem uma maneira de provisionar as VMs que fornecem aplicativos e áreas de trabalho aos usuários. Você pode adicionar grupos de recursos do Azure vazios existentes ao criar um catálogo de máquinas do MCS ou criar novos grupos de recursos para você. 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 uma entidade de serviço de escopo completo 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 uma entidade 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.

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **Nota:**
>
> Se a propriedade personalizada `UseEphemeralOsDisk` estiver definida como **false** ou se não for especificado nenhum valor, todos os VDAs provisionados continuarão a usar um disco de SO provisionado.

Veja a seguir um exemplo de conjunto de propriedades personalizadas que devem ser 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"
                }

           ],
<!--NeedCopy-->
```

Como criar máquinas usando discos de SO efêmeros Os discos de SO efêmeros são controlados com base na propriedade `UseEphemeralOsDisk` do parâmetro `CustomProperties`.

Considerações importantes para discos efêmeros Para provisionar discos de sistema operacional efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve oferecer suporte a discos de SO efêmeros.
- O tamanho do cache ou disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco de SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

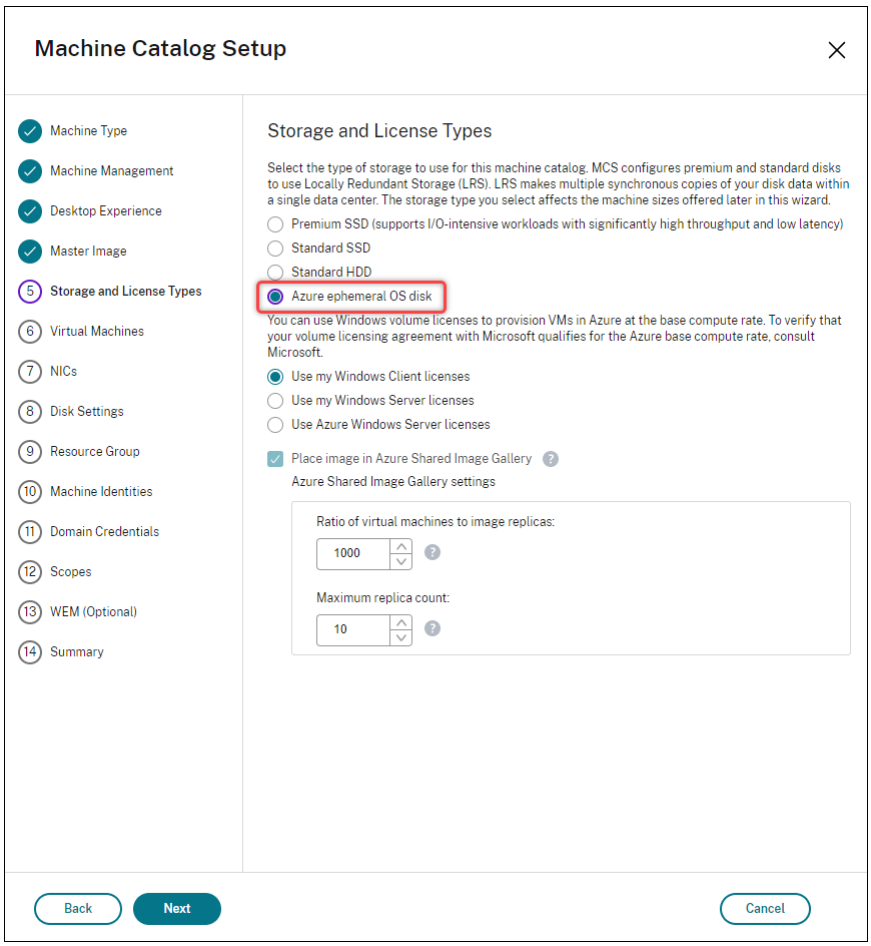
Considere também esses problemas nas seguintes situações:

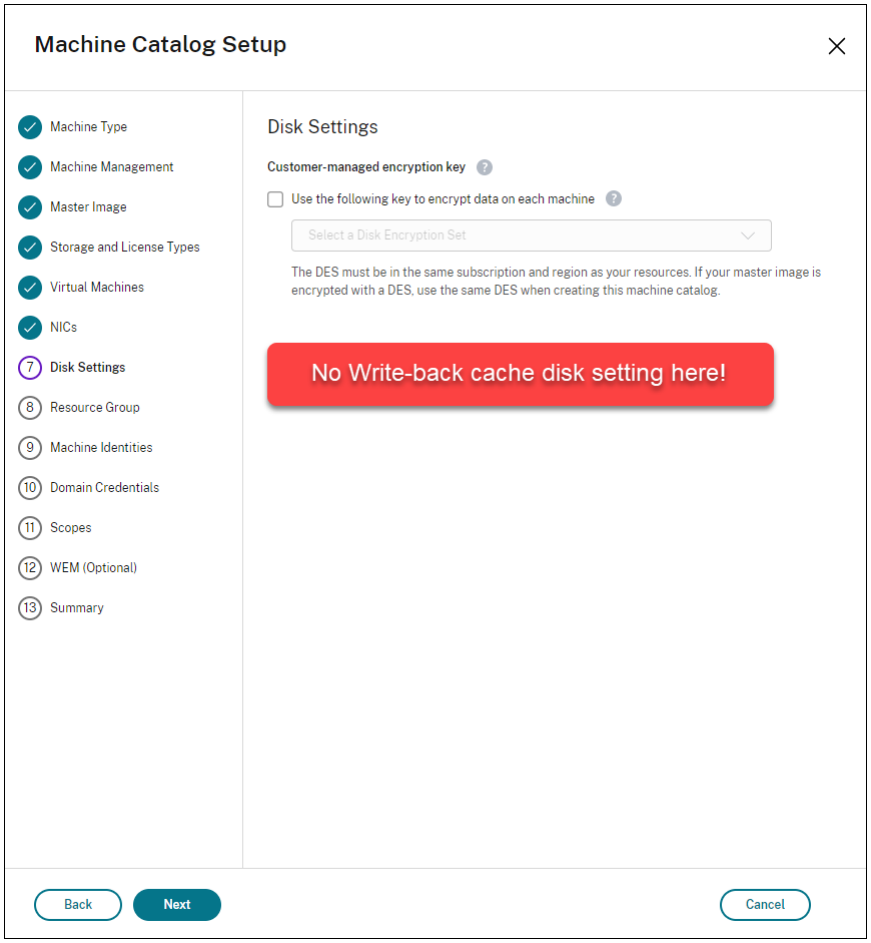
- Criação do esquema de provisionamento.
- Modificação do esquema de provisionamento.
- Atualização da imagem.

Otimização de armazenamento de disco efêmero do Azure e do MCS (Machine Creation Services) (MCS I/O) O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Não é possível criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- No assistente **Machine Catalog Setup**, se você selecionar **Azure ephemeral OS disk** na página **Storage and License Types**, você não terá a opção para configurações de disco de cache de write-back na página **Disk Settings**.





- 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 os dois recursos ativados, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

Criptografia 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 de seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Server-side encryption of Azure Disk Storage.

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco está criptografado, altere a chave atual no `DiskEncryptionSet`. Todos os recursos associados a essa alteração de `DiskEncryptionSet` devem ser criptografados com a nova chave.
- Quando você desabilita 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 habilitada novamente ou você atribua uma nova chave. Qualquer catálogo usando 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 esse recurso:

- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Depois de habilitar a chave de criptografia gerenciada pelo cliente, você não poderá desativá-la posteriormente. Se quiser desativar ou remover a chave de criptografia gerenciada pelo cliente, copie todos os dados para um disco gerenciado diferente que não esteja usando a chave de criptografia gerenciada pelo cliente.
- Os discos criados a partir de imagens personalizadas criptografadas usando criptografia no lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados usando as mesmas chaves gerenciadas pelo cliente. Esses discos devem estar na mesma assinatura.
- Os instantâneos criados a partir de discos criptografados com criptografia do lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados com as mesmas chaves gerenciadas pelo cliente.
- Discos, instantâneos e imagens criptografados com chaves gerenciadas pelo cliente não podem ser movidos para outro grupo de recursos e assinatura.
- Os discos gerenciados criptografados atualmente ou anteriormente usando a Criptografia de Disco do Azure não podem ser criptografados usando chaves gerenciadas pelo cliente.
- Consulte o site da Microsoft para ver as limitações dos conjuntos de criptografia de disco por região.

> **Nota:**
>
> Consulte Quickstart: Create a Key Vault using the Azure portal 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 dados nas máquinas provisionadas no catálogo. A criptografia no 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 no 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/SampleEncryption`

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos. Se a imagem estiver criptografada com um DES, use o mesmo DES ao criar o catálogo da máquina. Você não pode alterar o DES depois de criar o catálogo.

Se você criar um catálogo com uma chave de criptografia e depois desabilitar o DES correspondente no Azure, não poderá mais ligar as máquinas no catálogo ou adicionar máquinas a ele.

Se você quiser criar um catálogo de máquinas usando comandos do PowerShell, em que a chave de criptografia é uma chave gerenciada pelo cliente, faça o seguinte:

1. Abra uma janela do PowerShell.
2. Execute o comando `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 de Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma cadeia de caracteres 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>
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Conclua a criação do catálogo de máquinas.

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma especificação de modelo ou uma VM 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:

- Incompatível com todos os tamanhos de máquinas do Azure

- Incompatível com a criptografia de disco do Azure

Para criar um catálogo de máquinas com capacidade de criptografia no host:

1. Verifique se a assinatura tem o recurso de criptografia no host ativado ou não. Para fazer isso, consulte https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Se não estiver ativado, você deve ativar o recurso para a assinatura. Para obter informações sobre como ativar o recurso para sua assinatura, consulte https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Verifique se um determinado tamanho de VM do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute uma destas opções:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Crie uma especificação de modelo ou uma VM como entrada para o perfil da máquina no portal do Azure com a criptografia no host ativada.
   - 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 **Encryption at host** é ativada.
   - 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 especificação de modelo ou VM.
   - Disco de SO/Disco de dados: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma
   - Disco de SO efêmero: é criptografado somente pela chave gerenciada pela plataforma
   - Disco de cache: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma

   Você pode criar o catálogo de máquinas usando a interface Full Configuration ou executando comandos do PowerShell.

Recuperar criptografia nas informações do host de um perfil de máquina

Você pode recuperar a criptografia nas informações do host de um perfil de máquina executando 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 da máquina.

Por exemplo: quando a entrada do perfil da máquina for uma VM, execute o seguinte comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

Por exemplo: quando a entrada do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
    templatespecversion).AdditionalData
<!--NeedCopy-->
```

Criptografia dupla no disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Todos os catálogos criados com esse recurso têm todos os discos do lado do servidor criptografados 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 algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, 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 a interface Full Configuration e os comandos do PowerShell.
> - Você pode usar um fluxo de trabalho não baseado em perfil de máquina ou um fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
> - Se você usar um fluxo de trabalho não baseado em perfil de máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetId` armazenado.
> - Se você usa um perfil de máquina, pode usar uma especificação de VM ou modelo como uma entrada de perfil de máquina.

Limitações:

- A criptografia dupla não é suportada em Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desabilitar um Conjunto de Criptografia de Disco (DES) associado a um catálogo, as VMs do catálogo serão desativadas.

- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você só pode criar até 50 conjuntos de criptografia de disco por região por assinatura.
- Você não pode atualizar um catálogo de máquinas que já tenha um `DiskEncryptionSetId` com um `DiskEncryptionSetId` diferente.

Criar um catálogo de máquinas com criptografia dupla

1. Crie um Azure Key Vault e um DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Usar o portal do Azure para habilitar a criptografia dupla inativa para discos gerenciados.
2. Para procurar os conjuntos de criptografia de disco disponíveis em sua conexão de hospedagem:
   a) Abra uma janela do **PowerShell**.
   b) Execute os seguintes comandos do 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 do perfil da máquina, crie uma especificação de VM ou modelo como entrada do perfil da máquina.
   - Se você quiser usar uma VM como entrada de perfil de máquina:
     a) Crie uma VM no Portal do Azure.
     b) Navegue até **Disks>Key management** para criptografar a VM diretamente com um `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 Web Studio, siga um dos procedimentos a seguir, além das etapas em Criar catálogos de máquinas.

  - Se você não usar o fluxo de trabalho baseado em perfil de máquina, na página **Disk Settings**, selecione **Use the following key to encrypt data on each machine**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue a criar o catálogo.
  - Se estiver usando o fluxo de trabalho do perfil da máquina, na página **Master Image**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID do conjunto de criptografia de disco em suas propriedades.

  Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

- Se estiver usando comandos do PowerShell, faça o seguinte:
  - Se não estiver usando o fluxo de trabalho baseado no perfil da máquina, adicione a propriedade personalizada `DiskEncryptionSetId` no `New-ProvScheme` comando. 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"
<!--NeedCopy-->
```

  - Se estiver usando um 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
<!--NeedCopy-->
```

Conclua a criação do catálogo usando o SDK remoto do PowerShell. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

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) somente se o catálogo não tiver sido criptografado anteriormente.

- Se não estiver usando o fluxo de trabalho baseado no perfil da 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>'
<!--NeedCopy-->
```

- Se estiver usando um 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
<!--NeedCopy-->
```

Depois de bem-sucedidas, todas as novas VMs que você adiciona ao seu catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

Verificar se o catálogo está criptografado duas vezes

- No Web Studio:
  1. Navegue até **Machine Catalogs**.
  2. Selecione o catálogo que você deseja verificar. Clique na guia **Template Properties** localizada na parte inferior da tela.
  3. Em **Azure Details**, verifique o ID do conjunto de criptografia de disco em **Disk Encryption Set**. Se o ID do DES do catálogo estiver em branco, o catálogo não está criptografado.
  4. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.
- Usando o comando do PowerShell:
  1. Abra uma janela do **PowerShell**.
  2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
  3. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     <!--NeedCopy-->
     ```

  4. Recupere a propriedade personalizada DES Id do catálogo da máquina. Por exemplo:

     ```
     <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
         Value="/subscriptions
        /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
        -RG/providers/Microsoft.Compute/diskEncryptionSets/
        SampleEncryptionSet" />
     <!--NeedCopy-->
     ```

  5. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.

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:

- Crie um grupo de hosts.
- Crie hosts nesse grupo de hosts.
- Verifique se 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 por meio do seguinte script do 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>
<!--NeedCopy-->
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade de catálogo e não pode ser alterado depois que o catálogo é criado. Atualmente, a locação dedicada não é suportada no Azure.
- Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`.
- É necessário o posicionamento automático do Azure. 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 emitirá um erro durante a criação do catálogo.

Galeria de Computação do Azure

Use a Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas) como um repositório de imagens publicadas para máquinas provisionadas do MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação dos discos de SO, melhorando os tempos de início e de inicialização do aplicativo 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. Essa 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 proporção de réplica configurada e no máximo de réplicas configuradas.

> **Nota:**
>
> A funcionalidade da Galeria de Computação do Azure só é compatível com discos gerenciados. Não está disponível para catálogos de máquinas legadas.

Para obter mais informações, consulte Azure shared image gallery overview.

Acessar imagens da Galeria de Computação do Azure

Ao selecionar uma imagem a ser usada para criar um catálogo de máquina, você pode selecionar imagens criadas na Galeria de Computação do Azure. Essas imagens aparecem na lista de imagens na tela **Master Image** do assistente de Machine Catalog Setup.

Para que essas imagens apareçam, você deve:

1. Configurar um site do Citrix Virtual Apps and Desktops.
2. Conectar-se ao Azure Resource Manager.
3. No portal do Azure, criar 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 da imagem, crie uma versão da imagem.

Configurar a 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 esse recurso para um esquema de provisionamento e para alterar a taxa de réplica e os valores máximos de réplica.

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para dar suporte ao 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 estiver definida, o valor padrão será **False**.

`SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas de versão de imagem da galeria.

- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não estiver definida, os valores padrão serão usados. O valor padrão para discos de SO permanentes 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.
- Se a propriedade não estiver definida, o valor padrão será 10.
- Atualmente, o Azure oferece suporte a até 10 réplicas para uma versão única de imagem de galeria. Se a propriedade for definida com um valor maior do que o suportado pelo Azure, o MCS tentará usar o valor especificado. O Azure gera um erro, que registra o MCS deixa a contagem de réplicas atual inalterada.

> **Dica:**
>
> Ao usar a Galeria de Computação do Azure para armazenar uma imagem publicada para catálogos provisionados do 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-se o número de máquinas no catálogo pela taxa de réplica (arredondando para o valor inteiro mais próximo) e, em seguida, limitando o valor à contagem máxima de réplicas. Por exemplo, com uma taxa de réplica 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, mais de 81 têm 5 réplicas.

Caso de uso: Atualizando a taxa de réplica 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>'
<!--NeedCopy-->
```

Caso de uso: Convertendo um catálogo de instantâneos em um catálogo da Galeria de Computação do Azure Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas 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>'
<!--NeedCopy-->
```

> **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 estiver configurado para usar a galeria, a próxima operação de atualização do catálogo armazenará a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. O ciclo de energia das 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 dentro de algumas horas.

Caso de uso: Convertendo um catálogo da Galeria de Computação do Azure em um catálogo de instantâneos Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas 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>'
<!--NeedCopy-->
```

> **Dica:**
>
> Ao contrário da atualização de um instantâneo para um catálogo da Galeria de Computação do Azure, os dados personalizados de cada máquina ainda não foram atualizados para refletir as novas propriedades personalizadas. Execute o comando a seguir para ver as propriedades personalizadas originais da Galeria de Computação do Azure: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Depois que o comando `Set-ProvScheme` for concluído, o instantâneo da imagem ainda não foi criado. Depois que o catálogo estiver configurado para não usar a galeria, a próxima operação de atualização do catálogo armazenará 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. O ciclo de energia das 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.

Provisionar máquinas em zonas de disponibilidade especificadas

Você pode provisionar máquinas em zonas de disponibilidade específicas em ambientes do Azure. Você pode conseguir isso usando a interface Full Configuration ou o PowerShell.

> **Nota:**
>
> Se nenhuma zona for especificada, o MCS permitirá que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribuirá aleatoriamente as máquinas entre elas.

Configuração das zonas de disponibilidade na interface Full Configuration

Ao criar um catálogo de máquinas, você pode especificar zonas de disponibilidade nas quais deseja provisionar máquinas. Na página **Virtual Machines**, selecione uma ou mais zonas de disponibilidade nas quais você deseja criar máquinas.

Há dois motivos pelos quais nenhuma zona de disponibilidade está disponível: a região não tem zonas de disponibilidade ou o tamanho da máquina selecionada não está disponível.

Configuração de zonas de disponibilidade por meio do PowerShell

Com o PowerShell, você pode visualizar o Citrix DaaS que oferece itens de inventário por meio de `Get-Item`. Por exemplo, para visualizar a oferta de serviços da *Eastern US region* `Standard_B1ls`:

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
    name\East US.region\serviceoffering.folder\Standard_B1ls.
    serviceoffering"
2 <!--NeedCopy-->
```

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 por meio do 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 para um esquema de provisionamento.

Se for fornecida uma zona inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro será exibida fornecendo instruções sobre como corrigir o comando inválido.

> **Dica:**
>
> Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e será exibida uma mensagem de erro relevante.

Usar grupos de hosts e zonas de disponibilidade do Azure ao mesmo tempo

Há uma verificação prévia 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 hosts. A criação do catálogo falhará se a propriedade personalizada da zona de disponibilidade não corresponder à zona do grupo de hosts.

Para obter informações sobre a configuração de zonas de disponibilidade por meio do PowerShell, consulte Configuração de zonas de disponibilidade por meio do PowerShell.

Para obter informações sobre hosts dedicados do Azure, consulte Hosts dedicados do Azure.

A tabela a seguir descreve as várias combinações de zona de disponibilidade e zona de grupo de hosts e quais resultam na criação bem-sucedida ou com falha de um catálogo de máquinas.

Zona do grupo de hosts	Zona de disponibilidade em propriedade personalizada	Resultado da criação do catálogo de máquinas
Especificada. Por exemplo, o grupo de hosts está na Zona 1	Não especificada	Bem-sucedido. As máquinas são criadas na zona do grupo de hosts
Especificada. Por exemplo, o grupo de hosts está na Zona 1	Mesma zona da zona do grupo de hosts. Por exemplo, a zona na propriedade personalizada é definida como 1	Bem-sucedido. As máquinas são criadas na Zona 1
Especificada. Por exemplo, o grupo de hosts está na Zona 1	Diferente da zona do grupo de hosts. Por exemplo, a zona na propriedade personalizada é 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 prévias
Especificada. Por exemplo, o grupo de hosts está na Zona 1	Várias zonas especificadas. Por exemplo, zonas nas propriedades personalizadas são 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 prévias
Não especificada. Por exemplo, a zona do grupo de hosts é `None`	Não especificada	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 máquinas não são criadas em nenhuma zona
Não especificada. Por exemplo, a zona do grupo de hosts é `None`	Especificada. Por exemplo, as zonas na propriedade personalizada são 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 prévias

Disco efêmero do Azure

Os discos efêmeros do Azure permitem que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão.

> **Nota:**
>
> Os catálogos persistentes não oferecem suporte a discos de SO efêmeros.

Os 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.

Usando o PowerShell para configurar um disco efêmero

Para configurar um disco de SO efêmero do Azure para um catálogo, use o parâmetro `UseEphemeralOsDisk` em `Set-ProvScheme`. Defina o valor do parâmetro `UseEphemeralOsDisk` como **true**.

> **Nota:**
>
> Para usar esse 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>'
<!--NeedCopy-->
```

Armazenando um disco temporário do sistema operacional efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM ou em um disco de recursos. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não tenha um cache ou que tenha cache insuficiente. Essas VMs têm um disco temporário ou de recursos 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 (recurso) das VMs. O disco de cache tem preferência em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco de SO.
- Para atualizações, uma nova imagem 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.

Tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes do Azure que usam o MCS. Para VMs de destino, o MCS oferece suporte a:

- Disco de SO: SSD, SSD ou HDD premium
- Disco de cache de gravação: SSD, SSD ou HDD premium

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM oferece suporte ao tipo de armazenamento selecionado.
- Se sua configuração usar um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

> **Dica:**
>
> `StorageType` está configurado para um tipo de sistema operacional e uma conta de armazenamento. `WBCDiskStorageType` está configurado para o tipo de armazenamento de cache de gravação. Para um catálogo normal, é necessário `StorageType`. Se `WBCDiskStorageType` não estiver configurado, `StorageType` será usado como padrão para `WBCDiskStorageType`.

Se WBCDiskStorageType não estiver configurado, StorageType será usado como padrão para WBCDiskStorageType.

Configurando tipos de armazenamento

Para configurar os tipos de armazenamento para a VM, use o parâmetro `StorageType` em `New-ProvScheme`. Defina o valor do parâmetro `StorageType` como um dos tipos de armazenamento compatíveis.

Veja 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>'
<!--NeedCopy-->
```

Habilitar o armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica de forma síncrona 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.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser definido usando propriedades personalizadas existentes ou por meio do modelo **MachineProfile**. O armazenamento ZRS também é suportado com o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`. Você pode alterar a máquina existente do armazenamento LRS para o ZRS.

> **Nota:**
>
> - `StartsNow` indica que a hora de início programada é a hora atual.
> - `DurationInMinutes` com um número negativo (por exemplo, —1) indica que não há limite superior na janela de tempo do cronograma.

Limitações:

- Compatível somente com discos gerenciados
- Compatível apenas com unidades de estado sólido (SSD) premium e standard
- Não compatível com `StorageTypeAtShutdown`
- Disponível somente em determinadas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em grande escala. Portanto, para a primeira ativação, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

Defina o armazenamento com redundância de zona como o tipo de armazenamento em disco

Você pode selecionar armazenamento com redundância de zona durante a criação do catálogo inicial ou 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 `New-ProvScheme` do Powershell, use `Standard_ZRS` como o valor em `StorageAccountType`.
Por exemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se ele pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso do 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 armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento em disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante a criação do catálogo, o disco do sistema operacional do perfil da máquina `StorageType` é usado se as propriedades personalizadas não estiverem definidas.

VMs confidenciais do Azure (prévia)

VMs de computação confidencial do Azure garante que sua área de trabalho virtual seja criptografada na memória e protegida durante o uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho do perfil da máquina para criar esse catálogo. Você pode usar as especificações do modelo VM e ARM como uma entrada de perfil de máquina.

Considerações importantes sobre VMs confidenciais

As considerações importantes sobre os tamanhos de VM compatíveis e a criação de um catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM compatíveis: as VMs confidenciais aceitam os seguintes tamanhos de VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Criar um catálogo de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com as VMs Confidenciais do Azure usando a interface de Full Configuration e os comandos do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquina com VMs Confidenciais do Azure. Você pode usar uma especificação de modelo ou VM como a entrada do perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar ativadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:
    * VMGuestStateOnly: VM confidencial com apenas o estado de convidado da VM criptografado
    * DiskWithVMGuestState: VM confidencial com disco do sistema operacional e estado de convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco operacional normal quanto o efêmero podem ser criptografados.
  - Você pode obter informações da VM confidencial 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
    <!--NeedCopy-->
    ```

    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 adicional é `ConfidentialComputingType`.

- Você não pode alterar a imagem mestre ou o perfil da máquina do tipo de segurança confidencial para não confidencial ou do tipo de segurança não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

Criar um catálogo de máquinas com VM confidencial

1. Crie uma imagem mestre habilitada com uma VM confidencial. Consulte Início rápido: implantar uma VM confidencial com o modelo ARM e Início rápido: criar uma VM confidencial no AMD no portal do Azure para criar a VM mestre.
2. Use a VM mestre como um perfil de máquina ou crie uma especificação de modelo do Azure. Para obter informações sobre como criar uma especificação de modelo, consulte Criar uma especificação de modelo do Azure.
3. Crie o catálogo de máquinas baseado em perfil de máquina usando a interface Full Configuration ou os comandos do PowerShell.

   > **Nota:**
   >
   > Certifique-se de que a imagem mestre e a entrada do perfil da máquina estejam ativadas com o mesmo tipo de segurança confidencial.

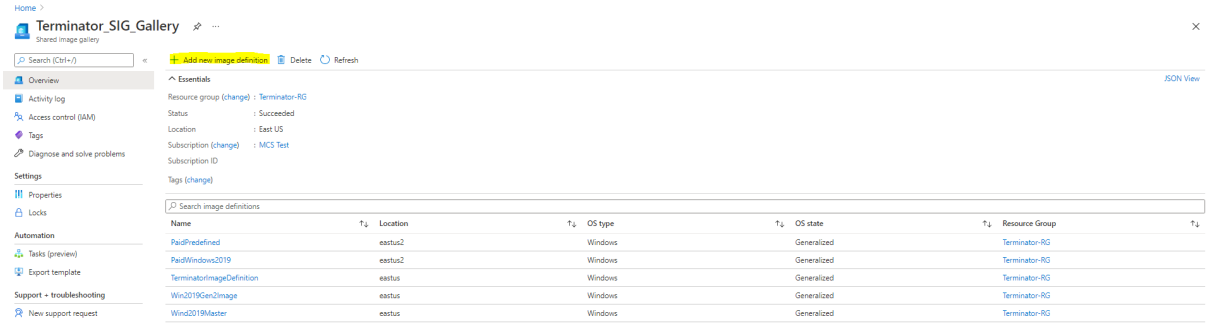
Azure Marketplace

O Citrix DaaS suporta o uso de uma imagem mestre no Azure que contém informações do 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 acrescentam informações do plano. O recurso Citrix DaaS é para imagens pagas.

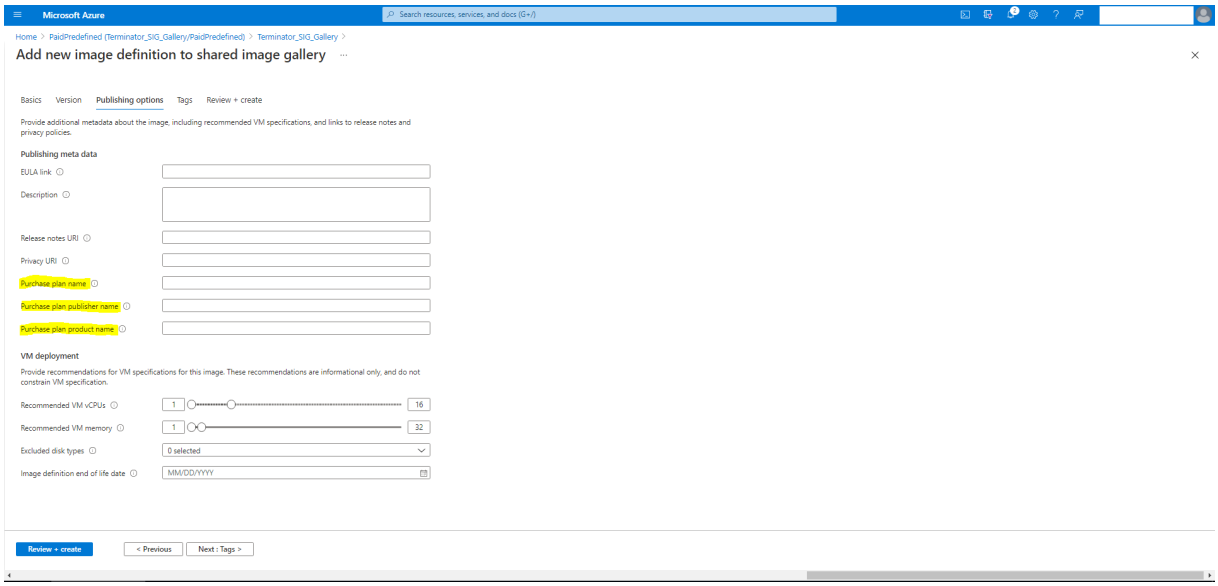
Verifique se a imagem criada na Galeria de Computação do Azure contém informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Computação do Azure no Citrix Studio. Opcionalmente, essas imagens podem ser usadas para uma imagem mestre. Para colocar a imagem em uma Galeria de Computação do Azure, crie uma definição de imagem em uma galeria.

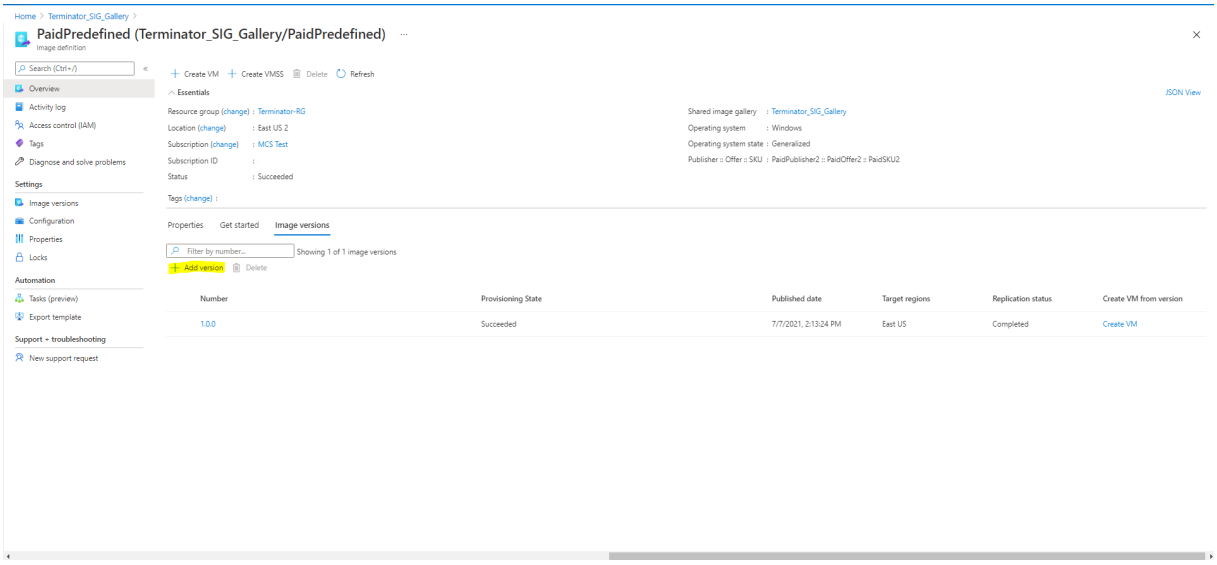


Na página **Publishing options**, verifique as informações do plano de compra.

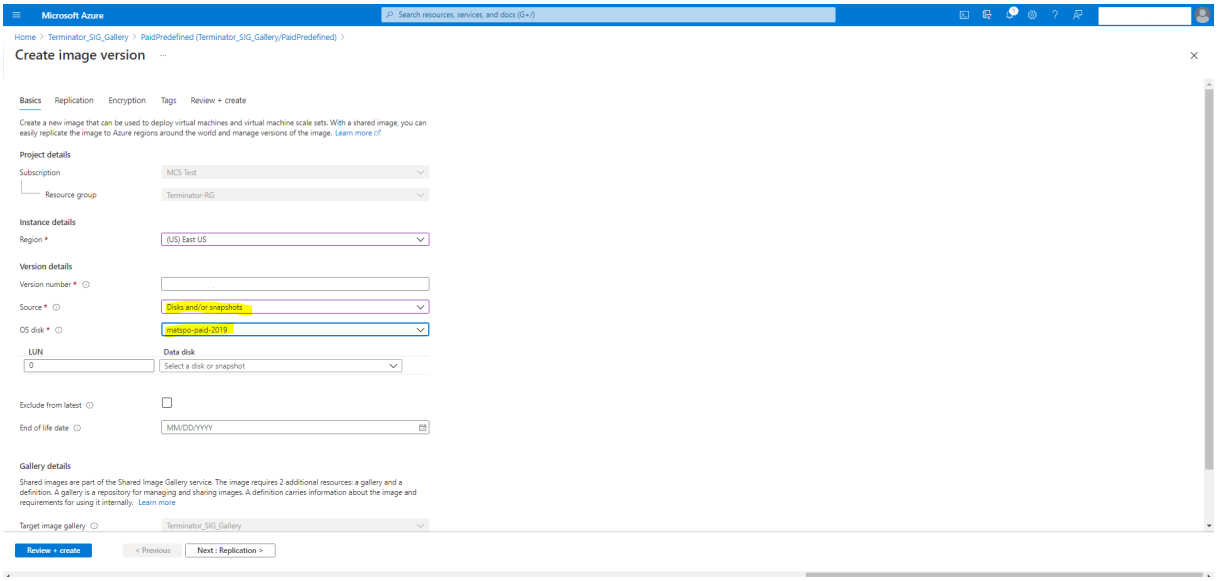
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. Se você deixar de preencher as informações do plano de compra, isso pode causar falha no processo do catálogo de máquinas.



Depois de verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Isso é usado como a imagem mestre. Clique em **Add version**:



Na seção **Version details**, selecione o instantâneo da imagem ou o disco gerenciado como origem:



Copiar marcações em todos os recursos

Você pode copiar marcações especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do sistema operacional, 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 especificação de modelo de ARM ou VM.

> **Nota:**
>
> Você deve adicionar a política nas marcações (consulte Atribuir definições de política para conformidade de marca) ou adicionar as marcações em uma origem de perfil de máquina para reter

> as marcações nos recursos.

Pré-requisitos

Crie a origem do perfil da máquina (especificação do modelo de ARM ou VM) para ter marcações na VM, nos discos e nas NICs dessa VM.

- Se você quiser ter uma VM como entrada de perfil de máquina, aplique as marcações na VM e em todos os recursos no portal do Azure. Consulte Aplicar marcas com o portal do Azure.
- Se você quiser ter a especificação do modelo ARM como uma entrada de perfil de máquina, adicione o seguinte bloco de marcações sob cada recurso.

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
6  <!--NeedCopy-->
```

> **Nota:**
>
> Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

Copiar marcações para os recursos de uma VM em um novo catálogo de máquinas

1. Crie um catálogo não persistente ou persistente com uma especificação de modelo de ARM ou VM como a entrada do perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

   > **Nota:**
   >
   > Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidas no perfil da máquina e o número de NICs que você deseja que as VMs usem.

Modificar marcações nos recursos de uma VM existente

1. Crie um perfil de máquina com as marcações em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
     MachineProfile <PathToYourMachineProfile>
2 <!--NeedCopy-->
```


3. Desative 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
<!--NeedCopy-->
```

5. Ligue a VM.
6. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes.

> **Nota:**
>
> Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidas no perfil da máquina e o número de NICs fornecidas em `Set-ProvScheme`.

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 Microsoft Azure.

Mais informações

- Conexões e recursos
- Conexão com o Microsoft Azure Resource Manager
- Criar catálogos de máquinas

Criar um catálogo do Microsoft System Center Virtual Machine Manager

December 21, 2022

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 Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de criar um catálogo do 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.
- Criar áreas de trabalho virtuais

MCS em compartilhamentos de arquivo 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 Biblioteca de Comunicações do Citrix Hypervisor (HCL) se conectem com êxito ao armazenamento SMB.

- As credenciais de usuário do VMM devem incluir acesso completo de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante os eventos de ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Ao usar o VMM 2012 SP1 com Hyper-V no Windows Server 2012: ao usar o SMB como armazenamento, ative o Provedor de Suporte de Segurança de Credencial de Autenticação (CredSSP) do Cloud Connector para máquinas Hyper-V. Para obter mais informações, consulte CTX 137465.

Usando uma sessão remota padrão do PowerShell V3, a HCL no Cloud Connector usa o CredSSP para abrir uma conexão com a máquina Hyper-V. Esse recurso passa credenciais de usuário criptografadas pelo 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 do VMM), para que os comandos de comunicação para o armazenamento funcionem corretamente.

As tarefas a seguir usam scripts do PowerShell que se originam na HCL. Os scripts são então enviados para a máquina Hyper-V para atuar no armazenamento SMB 3.0.

Consolidar imagem mestre: uma imagem mestre cria um novo esquema de provisionamento MCS (catálogo de máquinas). Ele clona e deixa a VM mestre pronta para criar novas VMs a partir do novo disco criado (e remove a dependência da VM mestre original).

ConvertVirtualHardDisk on the root\virtualization\v2 namespace

Exemplo:


```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

Criar disco de diferença: cria um disco de diferença a partir da imagem gerada pela consolidação da imagem. Depois, o disco de diferença é anexado a uma nova VM.

CreateVirtualHardDisk on the root\virtualization\v2 namespace

Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

Carregar discos de identidade: a HCL não pode carregar o disco de identidade diretamente 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 no Cloud Connector, a HCL deve primeiro copiar o disco de identidade através da máquina Hyper-V da seguinte forma.

1. A HCL carrega a identidade para a máquina Hyper-V através do compartilhamento de administrador.
2. A máquina Hyper-V copia o disco para o armazenamento SMB por meio de um script do PowerShell em execução na sessão remota do PowerShell.

   Uma pasta é criada na máquina Hyper-V e as permissões nessa pasta são bloqueadas apenas para o usuário do VMM (por meio da conexão remota do PowerShell).
3. A HCL exclui o arquivo do compartilhamento de administrador.
4. Quando a 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 excluída, para disponibilizá-la para reutilização.

Baixar discos de identidade: tal como acontece com os carregamentos, os discos de identidade passam pela máquina Hyper-V para a HCL. O processo a seguir cria uma pasta que só tem permissões de usuário do VMM no servidor Hyper-V se ela não existir.

1. A máquina Hyper-V copia o disco do armazenamento SMB para o armazenamento local Hyper-V usando um script do PowerShell em execução na sessão remota do PowerShell V3.
2. A HCL lê o disco do compartilhamento de administrador da máquina Hyper-V na memória.
3. A HCL exclui o arquivo do compartilhamento de administrador.

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 Microsoft System Center Virtual Machine Manager.

Mais informações

- Conexões e recursos
- Conexão com o Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas

Criar um catálogo da Nutanix

August 17, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização da Nutanix.

> **Nota:**
>
> Antes de criar um catálogo da Nutanix, você precisa concluir a criação de uma conexão com a Nutanix. Consulte Conexão com a Nutanix.

Criar um catálogo de máquinas usando um instantâneo Nutanix

O instantâneo que você seleciona é o modelo usado para criar as VMs no catálogo. Antes de criar o catálogo, crie imagens e instantâneos no Nutanix. Para obter mais informações, consulte a documentação do Nutanix.

No assistente de criação de catálogo:

- As páginas **Operating System** e **Machine Management** não contêm informações específicas ao Nutanix.
- 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 Prism Central (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 **Master Image**, selecione o instantâneo da imagem. O nome dos instantâneos do Acropolis deve ter o prefixo "XD_"para que sejam usados no Citrix Virtual Apps and Desktops. Use o console do Acropolis para renomear seus instantâneos, se necessário. Se você renomear instantâneos, reinicie o assistente de criação de catálogos 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. Essa opção está disponível apenas para conexões de PC Nutanix AHV. Existem dois tipos de NIC: **VLAN** e **OVERLAY**. Selecione uma ou mais NICs contidas na imagem mestre e, em seguida, selecione uma rede virtual associada para cada NIC.
- As páginas **Machine Identities**, **Domain Credentials**, **Scopes** e **Summary** não contêm informações específicas do Nutanix.

Limitação

Ao criar um catálogo MCS com a conexão de host Nutanix (especificamente, o Nutanix AHV plugin 2.7.1 e o Nutanix AHV plugin 2.5.1), o tamanho do disco rígido das VMs provisionadas é exibido incorretamente na interface **Full Configuration**.

- Nutanix AHV plugin 2.7.1: o tamanho exibido é muito menor (1 GB) do que o tamanho real do armazenamento (50 GB)
- Nutanix AHV plugin 2.5.1: o tamanho exibido é muito menor (32 GB) do que o tamanho real do armazenamento (60 GB)

O tamanho do disco rígido é exibido corretamente no console do Nutanix. Há uma atualização pendente do Nutanix para fornecer o tamanho adequado do disco.

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.

Mais informações

- Conexões e recursos

- Conexão com a Nutanix
- Conexão com soluções de nuvem e parceiros da Nutanix
- Criar catálogos de máquinas

Crie um catálogo do VMware

June 6, 2023

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas.

> **Nota:**
>
> Antes de criar um catálogo da VMware, você precisa concluir a criação de uma conexão com o VMware. Consulte Conexão com o VMware.

Criar um catálogo de máquinas usando um perfil de máquina

Você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A fonte da entrada do perfil da máquina é um modelo VMware. O perfil da 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 ser ambas habilitadas ou desabilitadas por vTPM. Esta regra se aplica a `New-ProvScheme` e `Set-ProvScheme`.
> - Se a imagem mestre estiver habilitada por vTPM, o modelo VMware só poderá vir da mesma fonte de VM que a imagem mestre.
> - A política de armazenamento criptografado só oferece suporte à clonagem completa.

O modelo VMware no perfil da máquina deve existir durante o ciclo de vida do catálogo para permitir o provisionamento de VMs no 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`.
- Como alternativa, 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

Com base em sistemas operacionais diferentes, você pode criar um catálogo de máquinas com configurações diferentes:

- Se o Windows 11 estiver instalado na imagem mestre, é necessário ter o vTPM ativado para a imagem mestre. Portanto, o modelo VMware, que é uma fonte do perfil da máquina, deve ter o vTPM anexado a ele.
- Se o Windows 10 estiver instalado na imagem mestre sem o vTPM conectado, você poderá criar um catálogo de máquinas com um modelo VMware que não seja vTPM como fonte do perfil da máquina.

Há outra configuração na qual você pode criar um catálogo de máquinas usando o modo de cópia completa em disco com o modelo de perfil de máquina aplicado com a política de armazenamento criptografado.

Para criar um catálogo de máquinas usando comandos do PowerShell com perfil de máquina como entrada:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute os seguintes comandos:
   - Para criar um catálogo de máquinas com o modelo VMware anexado ao vTPM como fonte de entrada do perfil de máquina e imagem mestre instalada no Windows 11:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$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"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
    ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Para criar um catálogo de máquinas com um modelo VMware que não tenha vTPM como fonte do perfil de máquina e imagem mestre instalada no Windows 10:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$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"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"  -Description "<string>"  -
    IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()  -SessionSupport "
    SingleSession" -ZoneUid "<Uid"
```



```
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Para criar um catálogo de máquinas usando o modo de cópia completa em disco com o modelo de perfil de máquina aplicado com a política de armazenamento criptografado:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$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
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

Solução de problemas

Se houver falha ao criar o catálogo, consulte CTX294978.

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 VMware.

Mais informações

- Conexões e recursos
- Conexão com o VMware
- Conexão com soluções de nuvem e parceiros do VMware
- Criar catálogos de máquinas

Criar catálogos de diferentes tipos de ingresso

July 4, 2023

Usando o MCS, você pode provisionar máquinas como não ingressadas no domínio, ingressadas no AD local, ingressadas no Azure AD ou ingressadas no Azure AD híbrido.

Para obter informações sobre como configurar identidades de máquina na interface Full Configuration, consulte Criar catálogos de máquina.

Para obter informações específicas sobre como criar catálogos ingressados em identidades de máquinas, consulte o seguinte:

- Criar catálogos ingressados no Azure Active Directory
- Criar catálogos habilitados para o Microsoft Intune
- Criar catálogos ingressados no Azure Active Directory híbrido
- Criar catálogos não ingressados no domínio

Criar catálogos ingressados no Azure Active Directory

December 6, 2023

Este artigo descreve como criar catálogos ingressados do Azure Active Directory (AD) usando o Citrix DaaS.

Para obter informações sobre requisitos, limitações e considerações, consulte Ingressado no Azure Active Directory.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recursos
   - Navegue até a interface de usuário do administrador do Citrix Cloud > menu de hambúrguer superior esquerdo > **Resource Locations**.
   - Clique em **+ Resource Location**.
   - Insira um nome para o novo local do recurso e clique em **Save**.
2. Criar 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.
3. Para excluir consistentemente dispositivos obsoletos do Azure AD e permitir que novos dispositivos ingressem no Azure AD, você pode atribuir a função Cloud Device Administrator à entidade de serviço de provisionamento. 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 fazer isso, habilite o gerenciamento de dispositivos ingressados no Azure AD de conexões de host usando a interface Full Configuration ou execute as seguintes etapas:
   a) Entre no portal do Azure e navegue até **Azure Active Directory > Roles and administrators**.
   b) Procure a função interna **Cloud Device Administrator** e clique em **Add assignments** para atribuir a função à entidade de serviço do aplicativo usado pela conexão de hospedagem.
   c) Use o Citrix Remote PowerShell SDK para executar os seguintes comandos para obter o `CustomProperties` existente da conexão de hospedagem. O `${HostingConnectionName}` se refere ao nome da conexão de hospedagem.
      i. Abra uma janela do **PowerShell**.
      ii. Execute o comando `asnp citrix*` para carregar os módulos do **PowerShell** específicos da Citrix.
      iii. Execute o comando a seguir para obter as propriedades personalizadas existentes da conexão de hospedagem.


```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

iv. Copie CustomProperties da conexão para um bloco de notas e anexe a configuração da propriedade `<Property xsi:type="StringProperty"Name="AzureAdDeviceManagement"Value="true"/>`.

v. Na janela do **PowerShell**, atribua uma variável às propriedades personalizadas modificadas. Por exemplo, `$UpdatedCustomProperties='<CustomProperties ...</CustomProperties>'`.

vi. Defina a propriedade personalizada de volta para a conexão de hospedagem:

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

vii. Execute o comando `(Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName } ).CustomProperties` para verificar as configurações atualizadas da propriedade personalizada.

Você pode criar catálogos ingressados no Azure AD usando a interface Full Configuration ou o **PowerShell**.

Usar a interface Full Configuration

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar catálogos ingressados no Azure AD, siga as orientações gerais nesse artigo, considerando os detalhes específicos dos catálogos ingressados no Azure AD.

No assistente de criação de catálogo:

1. Na página **Master Image**:
   - Selecione 2106 (ou posterior) como o nível funcional.
   - Selecione **Use a machine profile** e selecione a máquina apropriada na lista.
2. Na página **Machine Identities**, selecione **Azure Active Directory joined**. As máquinas criadas pertencem a uma organização e estão conectadas a uma conta do Azure AD que pertence a essa organização. Elas existem apenas na nuvem.

> **Nota:**
>
> - O tipo de identidade **Azure Active Directory joined** requer a versão 2106 ou posterior como o nível funcional mínimo para o catálogo.
> - As máquinas são ingressadas no Azure AD associado com o locatário ao qual a conexão de hospedagem está vinculada.

3. Os usuários devem receber acesso explícito no Azure para fazer login nas máquinas usando suas credenciais AAD. Consulte a seção Azure Active Directory ingressado para obter mais detalhes.

Usar o PowerShell

A seguir estão as etapas do **PowerShell** equivalentes às operações em Full Configuration. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

A diferença entre os catálogos ingressados no AD local e os ingressados no Azure AD está na criação do pool de identidades e do esquema de provisionamento.

Para criar um pool de identidades para catálogos ingressados no Azure AD:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
    WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
    NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
    -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Para criar um esquema de provisionamento para catálogos ingressados no Azure AD, o parâmetro **MachineProfile** é necessário em New-ProvScheme:

```
1 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 @{
2  "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
      US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
     azuread-vnet.virtualprivatecloud\Test_VNET.network" }
```



```
3   -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
       Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
       \AzureResource\serviceoffering.folder\Standard_DS1_v2.
       serviceoffering"
4 <!--NeedCopy-->
```

Todos os outros comandos usados para criar catálogos ingressados no Azure AD são os mesmos dos tradicionais catálogos ingressados no AD local.

Exibir o status do processo de ingresso no Azure AD

Na interface Full Configuration, o status do processo de ingresso do Azure AD é visível quando as máquinas ingressadas no Azure AD em um grupo de entrega estão em um estado ligado. Para exibir o status, use Search para identificar as máquinas e depois a guia **Details**, no painel inferior, para cada **Machine Identity**. As informações a seguir podem aparecer em **Machine Identity**:

- Ingressado no Azure AD
- Not yet joined to Azure AD

> **Nota:**
>
> Se as máquinas não estiverem no estado ingressado no Azure AD, elas não serão registradas no Delivery Controller. O status de registro delas aparece como **Initialization.**

Além disso, usando a interface Full Configuration, você pode descobrir por que as máquinas não estão disponíveis. Para isso, clique em uma máquina no nó **Search**, selecione **Registration** na guia **Details** no painel inferior e 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 pode habilitar o Rendezvous. Consulte Rendezvous V2 para obter detalhes.

Solucionar problemas

Se as máquinas não conseguirem ingressar no Azure AD, faça o seguinte:

- Verifique se a identidade gerenciada atribuída ao sistema está habilitada para as máquinas. As máquinas provisionadas pelo MCS devem ter essa opção ativada automaticamente. O processo de ingresso do Azure AD falha sem a identidade gerenciada atribuída ao sistema. Se a identidade gerenciada atribuída ao sistema não estiver ativada para as máquinas provisionadas pelo MCS, o motivo pode ser:
  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `AzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
- Verifique o status de provisionamento da extensão **AADLoginForWindows** das máquinas. O MCS depende dessa extensão para ingressar uma máquina virtual no Azure AD. Se a extensão **AADLoginForWindows** não existir, os motivos podem ser:
  - `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 falhas de provisionamento de **extensões AADLoginForWindows**, você pode verificar os logs em `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` na máquina provisionada pelo MCS.
- Verifique o status de ingresso e os logs de depuração do Azure AD executando o comando `dsregcmd /status /debug` 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 dispositivo do Azure AD está configurado corretamente executando `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }`.

  Certifique-se de que o valor de:

  - propriedade `AzureAdDeviceManagement` em `CustomProperties` é **true**
  - propriedade `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` em metadado é **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 dispositivo do Azure AD. Para resolver isso, atribua o `ServicePrincipal` com a função **Cloud Device Administrator**.

Grupo de segurança dinâmico do Azure Active Directory

As regras do 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[0-9]{3}$* no grupo de segurança dinâmico. Agora, se o nome da VM criada pela Citrix for algo que varia de Test001 a Test999, a VM será incluída no grupo de segurança dinâmico.

> **Nota:**
>
> Se o nome da VM criada por você manualmente for algo que varia de Test001 a Test999, a VM também será incluída no grupo de segurança dinâmico. Essa 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 Azure Active Directory (Azure AD). Ele 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.

Você pode usar os comandos do **PowerShell** para:

- Criar um catálogo de máquinas com o 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 o grupo de segurança do dispositivo ingressado no Azure AD

> **Importante:**
>
> - Para criar um catálogo de máquinas com o grupo de segurança dinâmico do Azure AD, adicionar máquinas ao catálogo e excluir o catálogo de máquinas, você deve ter o token de acesso do Azure AD. Para obter informações sobre como obter o token de acesso do Azure AD, consulte https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - Para solicitar um token de acesso no Azure AD, a Citrix solicita a permissão **Group.ReadWrite.All** para a API do Microsoft Graph. Um usuário do Azure AD que tenha permissão de consentimento de administrador de todos os locatários pode conceder permissão **Group.ReadWrite.All** para a API do Microsoft Graph. Para obter informações sobre como conceder consentimento de administrador de todos os locatários a um aplicativo no Azure Active Directory (Azure AD), consulte o documento da Microsoft https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/.

Criar um catálogo de máquinas com o grupo de segurança dinâmico do Azure AD

1. Na interface de usuário de configuração do catálogo de máquinas do console baseado na web, na página **Machine Identities**, selecione **Azure Active Directory joined**.
2. Faça login no Azure AD.
3. Obtenha o token de acesso para a API do MS Graph. Use esse token de acesso como um valor de parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**.
4. Execute o comando a seguir para verificar se o nome do grupo de segurança dinâmico existe no locatário.

```
Get-AcctAzureADSecurityGroup
 – AccessToken  $AzureADAccessToken
 – Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Crie um catálogo de máquinas usando o ID do locatário, o token de acesso e o grupo de segurança dinâmico. Execute o comando a seguir 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
<!--NeedCopy-->
```

Habilitar o recurso de grupo de segurança para um catálogo do Azure AD

Você pode ativar o recurso de segurança dinâmico para um catálogo do Azure AD que foi criado sem o recurso de grupo de segurança dinâmico ativado. Para isso:

1. Crie manualmente um novo grupo de segurança dinâmico. Você também pode reutilizar um grupo de segurança dinâmico existente.
2. Faça login no Azure AD e obtenha o token de acesso para a API do MS Graph. Use esse token de acesso como um valor de parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**.

> **Nota:**
>
> Para obter informações sobre as permissões exigidas pelo usuário do Azure AD, consulte https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Execute o comando a seguir para conectar o pool de identidades ao grupo de segurança dinâmico do Azure AD criado.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Se você atualizar o esquema de nomenclatura, a Citrix atualizará o esquema de nomenclatura para uma nova regra de associação. Se você excluir o catálogo, a regra de associação será excluída, não o grupo de segurança.

Excluir um catálogo de máquinas com o grupo de segurança do dispositivo ingressado no Azure AD

Quando você exclui um catálogo de máquinas, o grupo de segurança do dispositivo ingressado no Azure AD também é excluído.

Para excluir o grupo de segurança dinâmico do Azure AD, faça o seguinte:

1. Faça login no Azure AD.
2. Obtenha o token de acesso para a API do MS Graph. Use esse token de acesso como valor do parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**.
3. Execute o seguinte comando:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Criar um grupo de segurança dinâmico do Azure AD em um grupo de segurança existente atribuído ao Azure AD

Você pode criar um grupo de segurança dinâmico do Azure AD em um grupo de segurança existente atribuído ao Azure AD. Você pode fazer o seguinte:

- Obter informações do grupo de segurança.
- Obter todos os grupos de segurança atribuídos ao Azure AD que são sincronizados a partir do servidor AD local ou dos 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 o grupo de segurança dinâmico do Azure AD como um membro do grupo atribuído do Azure AD.
- Remover a associação entre o grupo de segurança dinâmico do Azure AD e o grupo de segurança atribuído ao Azure AD quando o grupo de segurança dinâmico do Azure AD for excluído juntamente com o catálogo da máquina.

Você também pode ver mensagens de erro explícitas quando alguma das operações falhar.

Requisito:

Você deve ter o token de acesso à API do MS Graph quando executar os comandos do **PowerShell**.

Para obter o token de acesso:

1. Abra o Microsoft Graph Explorer e faça login no Azure AD.
2. Certifique-se de ter consentimento para as permissões **Group.ReadWrite.All** e **GroupMember.ReadWrite.All**.
3. Obtenha o token de acesso do Microsoft Graph Explorer. Use esse token de acesso ao executar os comandos do **PowerShell**.

Para obter informações do grupo de segurança por ID de grupo:

1. Obtenha o token de acesso.
2. Encontre a ID do objeto do grupo no portal do Azure.
3. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
<!--NeedCopy-->
```

Para obter grupos de segurança por nome de exibição do grupo:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```


Para obter os grupos de segurança cujo nome de exibição contém uma sub-sequência de caracteres:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

Para obter todos os grupos de segurança atribuídos ao Azure AD que são sincronizados a partir do servidor AD local ou dos grupos de segurança atribuídos aos quais as funções do Azure AD podem ser atribuídas:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

Para obter todos os grupos de segurança dinâmicos do Azure AD:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Para obter os grupos de segurança atribuídos ao Azure AD com o número máximo de registros:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Para adicionar o grupo de segurança dinâmico do Azure AD como um membro do grupo de segurança atribuído do Azure AD:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Para obter os membros do grupo de segurança atribuídos do Azure AD:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Nota:**
>
> `Get-AcctAzureADSecurityGroupMember` fornece somente os membros diretos do tipo de grupo de segurança sob o grupo de segurança atribuído do Azure AD.

Para remover a associação entre o grupo de segurança dinâmico do Azure AD e o grupo de segurança atribuído ao Azure AD quando o grupo de segurança dinâmico do Azure AD for excluído juntamente com o catálogo da máquina:

1. Obtenha o token de acesso.
2. Execute o seguinte comando do **PowerShell** no console do **PowerShell**:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Modificar o nome do grupo de segurança dinâmico do Azure AD

Você pode modificar o nome do grupo de segurança dinâmico do Azure AD 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 Azure AD sejam consistentes com as informações armazenadas no portal do Azure.

> **Nota:**
>
> Os grupos de segurança dinâmicos do Azure AD 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 Azure AD usando a interface Full Configuration e os comandos do **PowerShell**.

Para modificar o nome do grupo de segurança dinâmico do Azure AD usando o **PowerShell**:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `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 Azure AD não puder ser modificado.

Criar catálogos habilitados para o Microsoft Intune

November 28, 2022

Este artigo descreve como criar catálogos habilitados para o Microsoft Intune usando o Citrix DaaS. Você pode ativar o Microsoft Intune usando a interface Full Configuration ou o PowerShell.

Para obter informações sobre requisitos, limitações e considerações, consulte Microsoft Intune.

Usar a interface Full Configuration

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Esse recurso requer a seleção de **Azure Active Directory joined** em **Machine Identities** durante a criação do catálogo. Siga as orientações gerais no artigo, levando em consideração os detalhes específicos do recurso.

No assistente de criação de catálogo:

- Na página **Machine Identities**, selecione **Azure Active Directory joined** e depois **Enroll the machines in Microsoft Intune**. Se habilitado, registre as máquinas no Microsoft Intune para gerenciamento.

Usar o PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações em Full Configuration.

Para registrar máquinas no Microsoft Intune usando o Remote PowerShell SDK, use o parâmetro `DeviceManagementType` em `New-AcctIdentityPool`. Esse recurso requer que o catálogo seja ingressado no Azure AD e que o Azure AD possua a licença correta do Microsoft Intune. Por exemplo:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
    IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
    AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
    NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
    ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Solução de problemas

Se as máquinas não conseguirem se registrar no Microsoft Intune, faça o seguinte:

- Verifique se as máquinas provisionadas pelo MCS estão ingressadas no Azure AD. As máquinas não conseguem se registrar no Microsoft Intune se não estiverem ingressadas no Azure AD. Consulte https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html para solucionar problemas de ingresso no Azure AD.
- Verifique se o seu locatário do Azure AD recebeu a licença apropriada do Intune. Consulte https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses para obter os requisitos de licença do Microsoft Intune.
- Verifique o status de provisionamento da extensão **AADLoginForWindows** das máquinas. O MCS depende dessa extensão para ingressar uma máquina virtual no Azure AD e se registar no Microsoft Intune. Se a extensão **AADLoginForWindows** não existir, os motivos podem ser:
  - `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 instalação da extensão **AADLoginForWindows** está bloqueada pela política do Azure.
- Para solucionar falhas de provisionamento de extensões **AADLoginForWindows**, você pode verificar os logs em `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` na máquina provisionada pelo MCS.
- Verifique os logs de eventos do Windows em **Logs de Aplicativos e Serviços > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

Criar catálogos ingressados no Azure Active Directory híbrido

December 6, 2023

Este artigo descreve como criar catálogos ingressados no Azure Active Directory (AD) híbrido usando o Citrix DaaS.

Você pode criar catálogos ingressados no Azure AD usando a interface Full Configuration ou o PowerShell.

Para obter informações sobre requisitos, limitações e considerações, consulte Ingressado no Hybrid Azure Active Directory.

Usar a interface Full Configuration

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar catálogos ingressados no Azure AD híbrido, siga as orientações gerais nesse artigo, considerando os detalhes específicos dos catálogos ingressados no Azure AD híbrido.

No assistente de criação de catálogo:

- Na página **Machine Identities**, selecione **Hybrid Azure Active Directory joined**. As máquinas criadas são pertencentes a uma organização e conectadas com uma conta do Active Directory Domain Services que pertence à organização. Elas existem na nuvem e no local.

> **Nota:**
>
> Se você selecionar **Hybrid Azure Active Directory joined** como o tipo de identidade, cada máquina no catálogo deverá ter uma conta de computador do AD correspondente.

Usar o PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações em Full Configuration. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

A diferença entre os catálogos ingressados no AD local e os ingressados no Azure AD híbrido está na criação do pool de identidades e das contas de máquina.

Para criar um pool de identidades juntamente com as contas para catálogos ingressados no Azure AD 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-d2f2-49
    d2-ab12-bae5bbd0df05"
New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
<!--NeedCopy-->
```

> **Nota:**
>
> `$password` é a senha correspondente para uma conta de usuário do AD com permissões de gravação.

Todos os outros comandos usados para criar catálogos ingressados no Azure AD híbrido são os mesmos dos tradicionais catálogos ingressados no AD local.

Exibir o status do processo de ingresso no Azure AD híbrido

Na interface Full Configuration, o status do processo de ingresso do Azure AD híbrido é visível quando as máquinas ingressadas no Azure AD híbrido em um grupo de entrega estão em um estado ligado. Para exibir o status, use Search para identificar as máquinas e depois a guia **Details**, no painel inferior, para cada **Machine Identity**. As informações a seguir podem aparecer em **Machine Identity**:

- Hybrid Azure AD joined
- Not yet joined to Azure AD

> **Nota:**
>
> - Pode haver um atraso para ingressar no Azure AD híbrido quando a máquina for ligada inicialmente. Isso é causado pelo intervalo de sincronização de identidade da máquina padrão (30 minutos do Azure AD Connect). A máquina entra no estado de ingressado no Azure AD híbrido somente depois que as identidades da máquina são sincronizadas com o Azure AD por meio do Azure AD Connect.
> - Se as máquinas não estiverem no estado ingressado no Azure AD híbrido, elas não serão registradas no Delivery Controller. O status de registro delas aparece como **Initialization**.

Além disso, usando a interface Full Configuration, você pode descobrir por que as máquinas não estão disponíveis. Para isso, clique em uma máquina no nó **Search**, selecione **Registration** na guia **Details** no painel inferior e leia a dica de ferramenta para obter informações adicionais.

Solucionar problemas

Se as máquinas não conseguirem ingressar no Azure AD híbrido, faça o seguinte:

- Verifique se a conta da máquina foi sincronizada com o Azure AD por meio do portal do Microsoft Azure AD. Se sincronizada, **Not yet joined to Azure AD** aparece, indicando o status de registro pendente.

  Para sincronizar contas de máquina com o Azure AD, certifique-se de que:

  - A conta da máquina está na unidade organizacional (UO) que está configurada para ser sincronizada com o Azure AD. As contas de máquina sem o atributo **UserCertificate** não são sincronizadas com o Azure AD, 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 Azure AD Connect deve ter sido sincronizado pelo menos uma vez depois que a conta de máquina foi criada. Caso contrário, execute manualmente o comando `Start-ADSyncSyncCycle -PolicyType Delta` no console do PowerShell da máquina do Azure AD Connect para disparar uma sincronização imediata.

- Verifique se o par de chaves do dispositivo gerenciado pela Citrix para ingressar no Azure AD híbrido foi enviado corretamente para a máquina consultando o valor de **DeviceKeyPairRestored** em **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verifique se o valor é 1. Se não for, os possíveis motivos 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. Estar ingressada no domínio local é um pré-requisito do ingresso no Azure AD híbrido.

- Verifique as mensagens de diagnóstico executando o comando `dsregcmd /status /debug` na máquina provisionada pelo MCS.

  - Se o ingresso no Azure AD híbrido for bem-sucedido, **AzureAdJoined** e **DomainJoined** são **YES** na saída da linha de comando.

  - Caso contrário, consulte a documentação da Microsoft para solucionar os problemas: https://docs.microsoft.com/en-us/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 do PowerShell para reparar o certificado do usuário:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
   UserCertificate
<!--NeedCopy-->
```

Para obter mais informações sobre o problema do certificado do usuário, consulte CTX566696.

Criar catálogos não ingressados no domínio

November 10, 2022

Este artigo descreve como criar catálogos não ingressados no domínio usando o Citrix DaaS.

Para obter informações sobre requisitos, limitações e considerações, consulte Não ingressado no domínio.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recursos
   - Navegue até a interface de usuário do administrador do Citrix Cloud > menu de hambúrguer superior esquerdo > **Resource Locations**.
   - Clique em **+ Resource Location**.
   - Insira um nome para o novo local do recurso e clique em **Save**.
2. Criar uma conexão de hospedagem. Consulte a seção Criar e gerenciar conexões para obter detalhes.

Usando o Citrix DaaS, você pode criar catálogos com base em grupos de trabalho ou máquinas não ingressadas no domínio. A criação de máquinas não ingressadas no domínio depende de como o grupo de identidade da conta foi criado. O grupo de identidades de conta é o mecanismo usado pelo MCS para criar e rastrear nomes de máquinas durante o provisionamento do catálogo.

Você pode criar catálogos não ingressados no domínio usando a interface Full Configuration ou o PowerShell.

Usar a interface Full Configuration

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar catálogos não ingressados no domínio, siga as orientações gerais nesse artigo, considerando os detalhes específicos aos catálogos não ingressados no domínio.

No assistente de criação de catálogo:

- Na página **Machine Identities**, selecione **Non-domain-joined**. As máquinas criadas não são ingressadas em nenhum domínio.

> **Nota:**
>
> O tipo de identidade **Non-domain-joined** requer a versão 1811 ou posterior do VDA como o nível funcional mínimo para o catálogo. Para disponibilizá-lo, atualize o nível funcional mínimo, se necessário.

Usar o PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações em Full Configuration.

Você pode criar um pool de identidades para catálogos não ingressados no domínio usando o SDK do PowerShell remoto.

Por exemplo, em versões anteriores, todos os campos do Active Directory eram fornecidos em uma única instância:

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
      IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
      -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
      Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

O MCS agora usa os novos parâmetros do PowerShell, **WorkgroupMachine** e **IdentityType**, para criar um pool de identidades para catálogos não ingressados no domínio. Usando o mesmo exemplo acima, os parâmetros eliminam a necessidade de especificar todos os parâmetros específicos do AD, incluindo credenciais de administrador de domínio:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
      WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
      NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
      ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Todos os outros comandos usados para criar catálogos não ingressados no domínio são os mesmos dos tradicionais catálogos ingressados no Active Directory local.

Gerenciar catálogos de máquinas

December 20, 2023

> **Nota:**
>
> Este artigo descreve como gerenciar catálogos usando a interface Full Configuration. Se você criou o catálogo usando a interface de Implantação rápida e continuar usando essa interface para gerenciar o catálogo, siga Gerenciar catálogos no Quick Deploy.

Introdução

Você pode adicionar ou remover máquinas a partir de um catálogo de máquinas, renomear, alterar a descrição ou gerenciar 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 que contêm máquinas em pool aleatórias criadas por meio do Machine Creation Services (MCS) fazem a manutenção das máquinas atualizando a imagem usada no catálogo e, depois, atualizando as máquinas. Esse método permite que você atualize um grande número de máquinas do usuário com eficiência.
- Para catálogos que contêm máquinas estáticas atribuídas permanentemente, você pode gerenciar a imagem ou o modelo que esses catálogos usam atualmente, mas somente as máquinas adicionadas aos catálogos posteriormente são criadas usando a nova imagem ou modelo.
- No caso de catálogos de acesso remoto ao PC, você gerencia atualizações para as máquinas dos usuários fora da interface de gerenciamento Full Configuration. Usando ferramentas de distribuição de software de terceiros, execute a tarefa de forma individual ou coletiva.

Para obter informações sobre como criar e gerenciar conexões com hipervisores de host e serviços de nuvem, consulte Connections and resources.

> **Nota:**
>
> O MCS não suporta o Windows 10 IoT Core e Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

Sobre instâncias persistentes

Ao atualizar a imagem mestre de um catálogo MCS contendo máquinas persistentes, todas as novas máquinas adicionadas ao catálogo usam a imagem atualizada. As máquinas existentes continuam usando a imagem mestre original. O processo de atualização de uma imagem é feito da mesma maneira para todos os outros tipos de catálogo. Considere o seguinte:

- Em catálogos de discos persistentes, as máquinas pré-existentes não são atualizadas com a nova imagem, mas todas as novas máquinas adicionadas ao catálogo usam a nova imagem.

- No caso de catálogos de discos não persistentes, a imagem da máquina é atualizada na próxima vez somente se a máquina for reiniciada no Studio ou no PowerShell. Se a máquina for reiniciada a partir do hipervisor fora do Studio, o disco não será redefinido.
- Em catálogos que não persistem, se você quiser ter imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

Adicionar máquinas a um catálogo

Antes de começar:

- Verifique se o host de virtualização (hipervisor ou provedor de serviço de nuvem) tem processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- É necessário ter contas de computador do Active Directory não utilizadas em quantidade suficiente. Se estiver usando contas existentes, o número de máquinas que você pode adicionar é limitado pelo número de contas disponíveis.
- Se você usar a interface de gerenciamento de Full Configuration para criar contas de computador do Active Directory para as máquinas adicionais, deverá 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 restritas do AD, adicione todos os conectores de nuvem que você pretende usar na tela **Logon to**....

Para adicionar máquinas a um catálogo:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Add Machines** na barra de ações.
3. Na página **Full Configuration**, selecione o número de máquinas virtuais a serem adicionadas.
4. Na página **Machine Identities**, defina as configurações da seguinte forma:
    - Selecione uma identidade na lista.
    - Se aplicável, indique se deseja criar contas ou usar as existentes e a localização (domínio) dessas contas.

      Se não houver contas existentes do Active Directory suficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas.

      Se você usar contas existentes do Active Directory, navegue até as contas ou selecione **Import** e especifique o arquivo .csv que contém o nome das contas. Verifique se há contas

suficientes para todas as máquinas que você está adicionando. A interface Full Configuration gerencia essas contas. Permita que o Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

- Se esse pool de identidades for usado por outros catálogos, você não poderá alterá-lo para um pool diferente usando Full Configuration. Em vez disso, use o cmdlet **Set-ProvScheme** do PowerShell. Para obter mais informações, consulte a documentação do Citrix Virtual Apps and Desktops SDK.
- Especifique um esquema de nomenclatura de conta usando marcas de hash para indicar onde os números ou letras sequenciais aparecem. Por exemplo, um esquema de nomenclatura de PC-Sales-## (com 0-9 selecionado) resulta em contas de computador com os nomes PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.
- Opcionalmente, você pode especificar como 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 depois disso.

5. Na página **Domain Credentials**, selecione **Enter credentials** e insira as credenciais do usuário com permissões suficientes para criar contas de máquina.

As máquinas são criadas como um processo em segundo plano, podendo levar bastante tempo quando muitas máquinas são criadas. A criação da máquina continua mesmo se você fechar a interface de gerenciamento Full Configuration.

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 catálogos provisionados pelo MCS.

Para adicionar máquinas em massa a um catálogo, execute as seguintes etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Add Machines** na barra de ações. A janela **Adicionar máquinas** é exibida.
3. Selecione **Add CSV File**. A janela **Add Machines in Bulk** é aberta.
4. Selecione **Download CSV Template**.
5. Preencha o arquivo de modelo.
6. Arraste ou navegue até o arquivo para carregá-lo.
7. Selecione **Validate** para realizar verificações de validação na importação.

8. Selecione **Import** 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`.
> - O nome das VMs diferencia maiúsculas e minúsculas. Ao inserir caminhos de máquinas virtuais, certifique-se de inserir o nome das VMs corretamente.

Ao editar o arquivo de modelo CSV, tenha em mente o seguinte:

- 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 junto com atribuições de usuário. Digite seus dados no seguinte formato:
  - No caso de 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 no caso de contas de máquina:
    - Domain\ComputerName1
    - Domain\ComputerName2
  - Em caso de pares de nome de usuário e VM:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Compute
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Compute
  - No caso de VMs apenas:
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Compute
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Compute

    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 **Full Configuration > Hosting > Add Connections and Resources**. 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, espalhe-as por diferentes arquivos 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 **Add Machines**. O CSV exportado de máquinas pode ser usado como um modelo ao adicionar máquinas em massa. Para exportar máquinas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Add Machines** na barra de ações. A janela **Adicionar máquinas** é exibida.
3. Selecione **Export to CSV file**. É baixado um arquivo CSV que contém uma lista das máquinas.
4. Abra o arquivo CSV para adicionar ou editar máquinas conforme o 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:**
>
> - Esse recurso não está disponível para acesso remoto ao PC e catálogos provisionados pelo MCS.
> - A exportação e a importação de máquinas em arquivos CSV apenas têm suporte entre catálogos do mesmo tipo.

Recuperar avisos e erros associados a um catálogo

Você pode receber erros e avisos históricos para entender os problemas com seu catálogo de máquinas MCS e corrigi-los.

Usando os comandos do PowerShell, você pode:

- Obter uma lista de erros ou avisos
- Alterar o estado do aviso de **New** para **Acknowledged**
- Excluir os erros ou avisos

Para executar os comandos do PowerShell:

1. Abra uma janela do PowerShell.

2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.

Para obter uma lista de erros e avisos:

Execute o comando `Get-ProvOperationEvent`.

- Sem parâmetros: recebe todos os erros e avisos
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: recebe todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `EventId`: recebe um erro ou aviso específico que corresponde a esse ID de evento
- Com o parâmetro `Filter`: recebe erros ou avisos por meio de filtro personalizado

Para alterar o estado de erros ou avisos de **New** para **Acknowledged**:

Execute o comando `Confirm-ProvOperationEvent`.

- Com o parâmetro `EventId`: define o estado de um erro ou aviso específico que corresponde a esse ID de evento. Você pode obter a saída `EventId` de um erro ou aviso específico como uma 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 **Acknowledged**.

Para excluir os erros ou avisos:

Execute o comando `Remove-ProvOperationEvent`.

- Com o parâmetro `EventId`: remove um erro ou aviso específico que corresponde a esse ID de evento Você pode obter a saída `EventId` de um erro ou aviso específico como uma 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 Citrix PowerShell SDK.

Excluir máquinas de um catálogo

Depois de excluir uma máquina de um catálogo de máquinas, os usuários não podem mais acessá-la, portanto, antes de excluir uma máquina, certifique-se de que:

- Foi feito backup dos dados do usuário ou os dados não são mais necessários.

- Todos os usuários fizeram logoff. Ativar o modo de manutenção impede que sejam estabelecidas novas conexões a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **View Machines** na barra de ações.
3. Selecione uma ou mais máquinas e, em seguida, selecione **Delete** 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 manter, desabilitar ou excluir suas contas do Active Directory.

Quando você exclui 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 mantê-los.

Quando você exclui máquinas não persistentes de um catálogo, elas são automaticamente excluídas do hipervisor ou do serviço de nuvem.

Excluir máquinas sem acesso ao hipervisor

Ao excluir uma VM ou um esquema de provisionamento, o MCS precisa remover as marcas da VM e, às vezes, também do disco básico, para que os recursos incluídos nas opções de exclusão não sejam mais rastreados ou identificados pelo MCS. No entanto, alguns desses recursos só podem ser acessados por meio do hipervisor. Use a opção `PurgeDBOnly` em `Remove-ProvVM` no PowerShell para excluir objetos de recursos da VM, como VM, disco básico, imagem no ACG e assim por diante, do banco de dados, mesmo quando não há acesso ao hipervisor.

Essa opção está ativada em:

- todos os hipervisores compatíveis
- VMs persistentes e não persistentes

Limitações

Você não pode usar os comandos -PurgeDBOnly e -ForgetVM ao mesmo tempo.

Use o comando PurgeDBOnly

Ao executar o comando do PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`, a operação de exclusão pode falhar nos seguintes cenários:

- A conexão do host está no modo de manutenção
- Credenciais inválidas
- Falha na autenticação
- Operação não autorizada
- O hipervisor está inacessível

> **Nota:**
>
> Remove-provVM -ForgetVM atinge apenas as 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 aviso é exibido:

`Try to use -PurgeDBOnly option to clean DDC database.`

Use a opção `-PurgeDBOnly` no comando `Remove-ProvVM` do PowerShell para excluir referências de uma VM do banco de dados MCS. Por exemplo,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

Editar um catálogo

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Edit Machine Catalog** na barra de ações.
3. Na página **Scopes**, altere os escopos.
4. Na página **VDA Upgrade**, altere ou selecione a versão do VDA para a qual atualizar. Para obter mais informações, consulte Atualização de VDA.
5. 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 somente às máquinas que você adicionar ao catálogo posteriormente. As máquinas existentes permanecem inalteradas.

   - Na página **Virtual Machines**, altere o tamanho da máquina e as zonas de disponibilidade nas quais você deseja criar máquinas.

     > **Nota:**
     >
     > – Somente os tamanhos de máquina que o catálogo suporta são mostrados.
     > – Se necessário, selecione **Show only machine sizes used in other machine catalogs** para filtrar a lista de tamanhos de máquina.

   - Na página **Machine Profile**, escolha se deseja usar ou alterar um perfil de máquina.

- (Somente quando o catálogo estiver configurado com um host de grupo dedicado) Na página **Dedicated host group**, escolha se deseja alterar um grupo de host.
- Na página **Storage and License Types**, escolha se deseja alterar o tipo de armazenamento, o tipo de licença e as configurações da Galeria de Computação do Azure (disponível somente quando a opção **Place prepared image in Azure Gallery** está em uso).

> **Nota:**
>
> Se a configuração recém-selecionada não suportar o tamanho atual da máquina, uma caixa de diálogo de aviso é exibida, informando que a alteração da configuração redefinirá a configuração do tamanho da máquina. Se você optar por continuar, um ponto vermelho aparece ao lado do menu **Virtual Machines**, 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 por meio de uma imagem do Azure Resource Manager.

Para catálogos de acesso remoto a PC, as seguintes páginas estão visíveis:

- Na página **Power Management**, altere as configurações de gerenciamento de energia e selecione uma conexão de gerenciamento de energia.
- Na página **Organizational Units**, adicione ou remova unidades organizacionais do Active Directory.

6. Na página **Description**, altere a descrição do catálogo.
7. Clique em **Apply** para aplicar as alterações feitas e clique em **Save** para sair.

Renomear um catálogo

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Rename Machine Catalog** na barra de ações.
3. Digite o novo nome.

Excluir um catálogo

Antes de excluir um catálogo, certifique-se de que:

- Todos os usuários fizeram logoff e não há sessões desconectadas em execução.
- O modo de manutenção está ativado para todas as máquinas do catálogo, de modo que novas conexões não possam ser estabelecidas.
- Todas as máquinas do 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. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Delete Machine Catalog** na barra de ações.
3. Se o catálogo contiver máquinas persistentes, indique se essas máquinas também devem ser excluídas do hipervisor ou do serviço de nuvem. Se você optar por fazer isso, escolha se deseja manter, desabilitar ou excluir as contas de computador do Active Directory.
4. Se necessário, selecione **Hide progress** para executar a exclusão em segundo plano.

> **Nota:**
>
> - Quando você exclui um catálogo do Azure Resource Manager, as máquinas associadas e os grupos de recursos são excluídos do Azure, mesmo que você opte por mantê-los.
> - Quando você exclui um catálogo contendo máquinas não persistentes, essas máquinas são excluídas do hipervisor ou do serviço de nuvem.
> - Quando o hipervisor ou serviço de nuvem fica 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 somente do banco de dados do site da Citrix. Para fazer isso, selecione o catálogo de máquinas no nó **Machine Catalogs** e execute a exclusão mostrada na guia **Troubleshoot**. Lembre-se de que essa 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 dos catálogos de sessão única e multissessão. Essas contas poderão ser usadas para outras máquinas.
- Adicionar contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam em vigor. Não use barra (/) no nome de uma unidade organizacional.

Para gerenciar contas do Active Directory:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Manage AD accounts** 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: redefinir todas elas ou inserir uma senha que se aplique a todas as contas.

Você pode redefinir as senhas se não souber as senhas da conta atual, mas deve ter permissão para executar uma redefinição de senha. Se você inserir uma senha, a senha será alterada nas contas à medida que elas são importadas. Se você excluir uma conta, escolha se a conta em um Active Directory deve ser mantida, desabilitada ou excluída.

Indique se as contas do Active Directory serão mantidas, desativadas ou excluídas quando você 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 suas áreas de trabalho, você poderá revertê-la 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 de um catálogo persistente, considere o seguinte: somente as máquinas adicionadas ao catálogo posteriormente são criadas usando a nova imagem. Não implantamos a nova imagem nas máquinas existentes no catálogo.

Depois que uma máquina é atualizada, ela reinicializa automaticamente.

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 nova.

1. No hipervisor ou provedor de serviços de nuvem, tire um instantâneo da VM atual e dê um nome significativo ao instantâneo. Esse 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 vDisk pessoal, atualize o inventário.
5. Desligue a VM.
6. Faça um instantâneo da VM e dê a ele um nome significativo que seja reconhecido quando você 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 na interface de gerenciamento de Full Configuration. 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 somente por meio do console XenCenter do XenServer.

Alterar a imagem mestre

Para implantar uma nova imagem mestre em todas as máquinas em um catálogo:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Change Master Image** na barra de ações.
3. Na página **Master Image**, selecione o host e a imagem que você deseja implantar.

   > **Dica:**
   >
   > Para um catálogo criado pelo 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, é criada uma entrada relacionada à nota se você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como null (-). Para exibir o histórico de notas da imagem, selecione o catálogo, clique em **Template Properties** no painel inferior e, em seguida, clique em **View note history**.

4. Na página **Rollout Strategy**, escolha quando as máquinas no catálogo de máquinas serão alteradas com a nova imagem: no próximo desligamento ou imediatamente.

   > **Nota:**
   >
   > A página **Rollout Strategy** não está disponível para VMs persistentes porque a implantação só se aplica a VMs não persistentes.

5. Verifique as informações na página **Summary** e selecione **Finish**. Cada máquina reinicializa automaticamente depois de ser atualizada.

   Para acompanhar o andamento da atualização, localize o catálogo em **Machine Catalogs** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo. Para um catálogo não persistente, você pode acompanhar o status de atualização da sua imagem na coluna **Image Update**, que inclui **Fully updated**, **Partially updated**, **Pending update** e **Preparing image**.

   > **Dica:**

> Para exibir a coluna **Image Update**, selecione o ícone **Columns to Display** na barra de ações, selecione **Machine Catalog > Image Status** e clique em **Save**.

Se você estiver atualizando um catálogo usando o SDK do PowerShell, poderá especificar um modelo de hipervisor (`VMTemplates`), como alternativa a uma imagem ou a um instantâneo de uma imagem.

Estratégia de implantação:

A alteração da imagem no próximo desligamento afetará imediatamente todas as máquinas que não estejam em uso no momento, ou seja, máquinas que não têm uma sessão de usuário ativa. Um sistema que está em uso recebe a atualização quando a sessão ativa atual termina.

> **Nota:**
>
> A estratégia de implantação só é aplicável a VMs não persistentes.

Considere o seguinte:

- Novas sessões não podem ser iniciadas até que a atualização seja concluída nas máquinas aplicáveis.
- No caso de máquinas de sessão única, as máquinas são imediatamente atualizadas quando não estão em uso ou quando os usuários não estão conectados.
- No caso de um SO de sessão única com máquinas secundárias, as reinicializações não ocorrem automaticamente. Elas devem ser desligadas e reinicializadas manualmente.

> **Dica:**
>
> Limite o número de máquinas reinicializadas usando as configurações avançadas de uma conexão de host. Use essas configurações para modificar as ações tomadas para um determinado catálogo; as configurações avançadas variam dependendo do hipervisor.

Se você quiser ativar o agendamento de reinicialização única 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`

Exemplo:

- Para criar um agendamento de reinicialização das VMs no catálogo chamado **BankTellers** para começar em 3 de fevereiro de 2022, entre 2h e 4h.


```
New-BrokerCatalogRebootSchedule -Name BankTellers
-CatalogName BankTellers
-StartDate "2022-02-03"
-StartTime "02:00"
-Enabled $true
-RebootDuration 120
<!--NeedCopy-->
```

- Para criar um agendamento de reinicialização das VMs no catálogo com o UID 17 para começar em 3 de fevereiro de 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM é configurada para exibir uma caixa de mensagem com o título **WARNING: Reboot pending** e a mensagem **Save your work** em cada sessão do 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
<!--NeedCopy-->
```

- Para renomear o agendamento de reinicialização do catálogo chamado **Old Name** para **New Name**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- Para exibir todos os agendamentos de reinicialização do catálogo com o UID 1 e renomear o agendamento de reinicialização do catálogo com o UID 1 para **New name**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Para definir o agendamento de reinicialização do catálogo chamado **Accounting** para exibir uma mensagem com o título **WARNING: Reboot pending e a mensagem Save your work** dez minutos antes da reinicialização de cada VM. A mensagem aparece em todas as sessões do usuário nessa VM.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- Para exibir todos os agendamentos de reinicialização que estão desativados e habilitar todos os agendamentos de reinicialização desativados.


```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Para definir o agendamento de reinicialização do catálogo com o UID 17 para exibir a mensagem **Rebooting in %m% minutes** em quinze, dez e cinco minutos antes da reinicialização de cada máquina virtual.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- Para configurar o fuso horário do catálogo chamado **MyCatalog**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

Reverter a imagem mestre

Depois de implantar uma imagem atualizada/nova, você poderá revertê-la. Isso pode ser necessário se ocorrerem problemas com as máquinas recentemente atualizadas. Quando você faz a reversão, as máquinas no catálogo voltam para a última imagem funcional. Os novos recursos que exigem a imagem mais recente não estarão mais disponíveis. Tal como acontece com a implantação, a reversão de uma máquina inclui uma reinicialização.

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo e, em seguida, selecione **Roll Back Master Image** na barra de ações.
3. Especifique quando aplicar a imagem anterior às máquinas, conforme descrito para a operação de distribuição.

A reversão é aplicada apenas a 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 **Machine Catalogs** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em determinados cenários, incluindo os seguintes. (A opção **Roll Back Master Image** não fica visível.)

- Você não tem permissão para reverter.
- O catálogo não foi criado usando o MCS.
- O catálogo foi criado usando uma imagem do disco de SO.
- O instantâneo usado para criar o catálogo tornou-se corrompido.
- As alterações do usuário nas máquinas no catálogo não persistem.
- As máquinas no catálogo estão sendo executadas.

Alterar o nível funcional ou desfazer a alteração

Altere o nível funcional do 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 novos.

Antes de alterar o nível funcional de 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 ser atualizadas.

Para alterar o nível funcional de um catálogo:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo. A guia **Details** no painel inferior exibe informações da versão
3. Selecione **Change Functional Level**. Se a interface de gerenciamento detectar que o catálogo precisa alterar o nível funcional, ela exibirá uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser alteradas, uma mensagem explica o motivo. Para garantir que todas as máquinas funcionem corretamente, recomendamos que você resolva esses problemas antes de clicar em **Change**.

Após a conclusão da atualização do catálogo, você pode reverter as máquinas para suas versões anteriores do VDA selecionando o catálogo e escolhendo **Undo Functional Level Change** na barra de ações.

Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Não é possível alterar as configurações associadas ao sistema operacional e gerenciamento da máquina. O catálogo clonado herda essas configurações do original.
- A clonagem de um catálogo pode levar algum tempo para ser concluída. Se necessário, selecione **Hide progress** para executar a clonagem em segundo plano.
- O catálogo clonado herda o nome do original e tem um sufixo `Copy`. Você pode mudar o nome. Consulte Renomear um catálogo.
- Após a conclusão da clonagem, atribua o catálogo clonado a um grupo de entrega.
- Você pode criar um catálogo vazio por meio da 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. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Clone** na barra de ações.

3. Na janela **Clone Selected Machine Catalog**, exiba as configurações do catálogo clonado e defina as configurações conforme aplicável. Selecione **Next** para prosseguir para a próxima página.
4. Na página **Summary**, exiba um resumo das configurações e selecione **Finish** para iniciar a clonagem.
5. Se necessário, selecione **Hide progress** 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 da organização.

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, primeiro planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas com até cinco níveis de profundidade (excluindo a pasta raiz padrão).
- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós em **Full Configuration** (como os nós **Machine Catalogs** e **Applications**) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outros nós ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nos diferentes nós.

Para criar uma pasta de catálogo, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Create Folder** na barra **Action**.
3. Insira um nome para a nova pasta e clique em **Done**.

> **Dica:**
>
> Se você criar uma pasta em um local não desejado, poderá arrastá-la para o local correto.

Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Exiba os catálogos por pasta. Você também pode ativar **View all** acima da hierarquia de pastas para exibir todos os catálogos de uma vez só.
3. Clique com o botão direito do mouse em um catálogo e selecione **Move Machine Catalog**.
4. Selecione a pasta para a qual deseja mover o catálogo e clique em **Done**.

> **Dica:**
>
> Você pode arrastar um catálogo para uma pasta.

Gerenciar pastas de catálogo

Você pode excluir, renomear e mover pastas de catálogo.

Você só poderá excluir uma pasta se ela e suas subpastas não contiverem catálogos.

Para gerenciar uma pasta, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Action**, conforme necessário:
   - Para renomear a pasta, selecione **Rename Folder**.
   - Para excluir a pasta, selecione **Delete Folder**.
   - Para mover a pasta, selecione **Move Folder**.
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 catálogo.

Ação	Permissões necessárias
Criar pastas de catálogo	Create Machine Catalog Folder
Excluir pastas de catálogo	Remove Machine Catalog Folder
Mover pastas do catálogo	Move Machine Catalog Folder
Renomear pastas de catálogo	Edit Machine Catalog Folder

Ação	Permissões necessárias
Mover catálogos para pastas	Edit Machine Catalog Folder e Edit Machine Catalog Properties

Configurar o upgrade automático para VDAs

> **Importante:**
>
> - Para garantir uma atualização tranquila, certifique-se de atender aos pré-requisitos e analisar os problemas conhecidos antes de atualizar os VDAs para as versões CR ou LTSR CU. Consulte Atualizar VDAs usando a interface Full Configuration.
> - Ao atualizar VDAs LTSR para versões de atualização cumulativa (CU) LTSR, certifique-se de que a versão dos VDA Upgrade Agents em execução nos VDAs seja 7.36.0.7 ou posterior. Para obter mais informações, consulte Atualizar VDAs usando a interface Full Configuration.
> - Você pode alternar entre o VDA CR e o VDA LTSR, desde que a mudança seja de uma versão anterior para uma versão posterior. Você não pode mudar de uma versão posterior para uma versão anterior porque isso é considerado um downgrade. Por exemplo, você não pode fazer o downgrade de 2212 CR para 2203 LTSR (qualquer CU), mas pode fazer o upgrade de 2112 CR para 2203 LTSR (qualquer CU).
> - Você também pode atualizar VDAs usando o PowerShell. Consulte Upgrade de VDAs usando o PowerShell.

Com o recurso, você pode fazer o seguinte:

- Fazer upgrade de VDAs por catálogo
- Editar ou cancelar um upgrade de VDA agendado
- Definir as configurações de atualização do VDA após a criação do catálogo
- Fazer upgrade de VDAs por máquina

> **Nota:**
>
> - Quando você programa atualizações do VDA para um catálogo, somente podem ser atualizados os VDAs no catálogo que têm o VDA Upgrade Agent instalado.
> - A atualização de um VDA falha quando a máquina está no modo de manutenção ou quando uma sessão está sendo executada na máquina.

Tipos de máquinas compatíveis

Esse recurso se aplica aos seguintes tipos de máquina:

- Máquinas persistentes provisionadas pelo MCS (AD joined, Azure AD joined e non-domain-joined). Você as implanta usando o **Citrix Machine Creation Services** na página **Machine Management** durante a criação do catálogo.
- Máquinas de acesso ao PC remoto
- Citrix HDX Plus for Windows 365 machines
- Outras máquinas persistentes provisionadas usando tecnologias ou serviços de provisionamento que não são da Citrix. Você adiciona essas máquinas ao DaaS para gerenciamento usando **Other service or technology** na página **Machine Management** durante a criação do catálogo.

Para obter mais informações sobre as opções **Citrix Machine Creation Services** e**Other service or technology**, consulte Gerenciamento de máquinas.

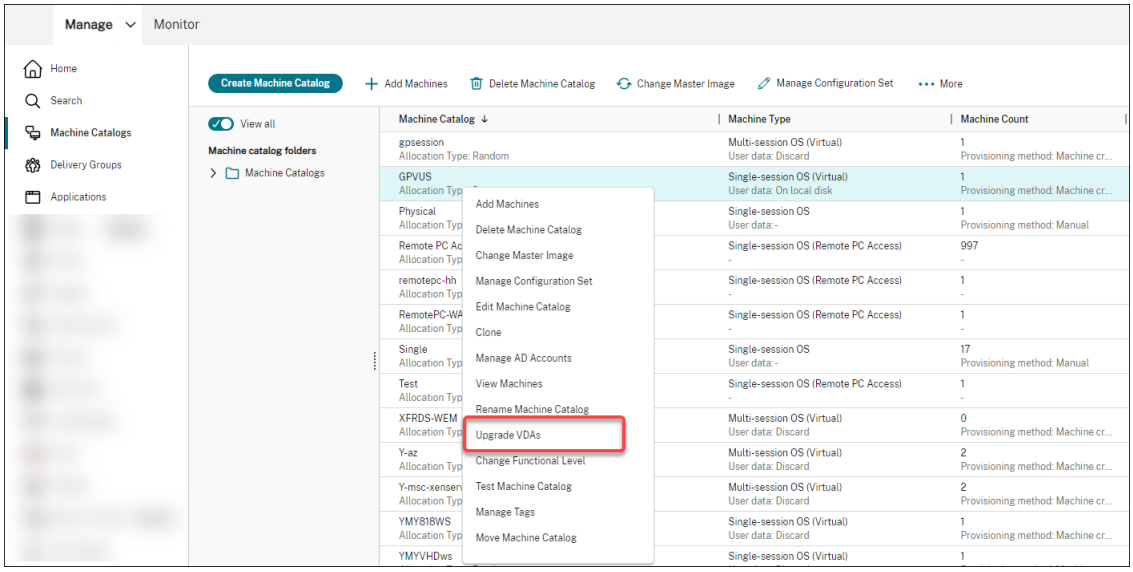
> **Nota:**
>
> Para máquinas provisionadas pelo MCS, somente máquinas estáticas persistentes são suportadas. Máquinas aleatórias não são suportadas, mesmo que sejam persistentes.

Fazer upgrade de VDAs por catálogo

> **Nota:**
>
> Ao programar atualizações de VDA para um catálogo, esteja ciente de que todas as máquinas do catálogo serão incluídas no escopo de atualização. Portanto, recomendamos fazer backup dessas máquinas antes de iniciar a atualização.

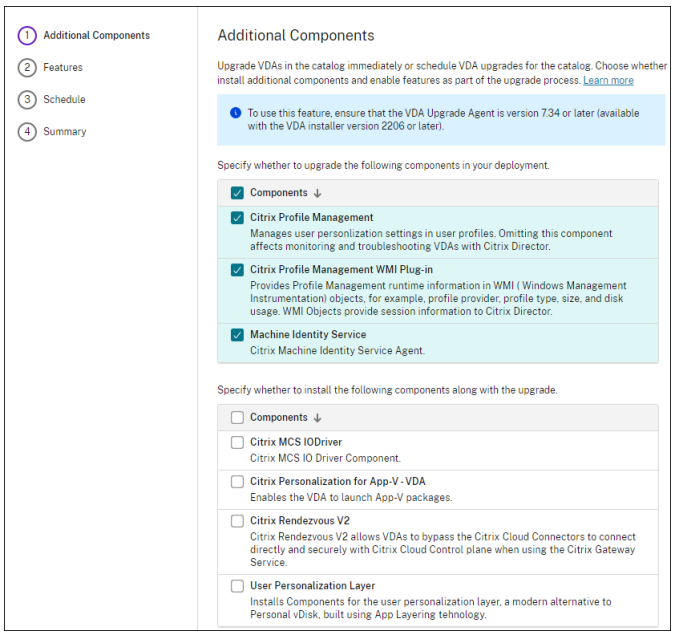
Depois de habilitar a atualização do VDA para um catálogo, você pode atualizar VDAs no catálogo imediatamente ou agendar atualizações para o catálogo. Para isso, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs**.
2. Selecione o catálogo e, em seguida, use **Upgrade VDAs** no menu contextual ou na barra de ações. (Clique com o botão direito do mouse para exibir o menu contextual.) A janela VDA Upgrade é exibida.



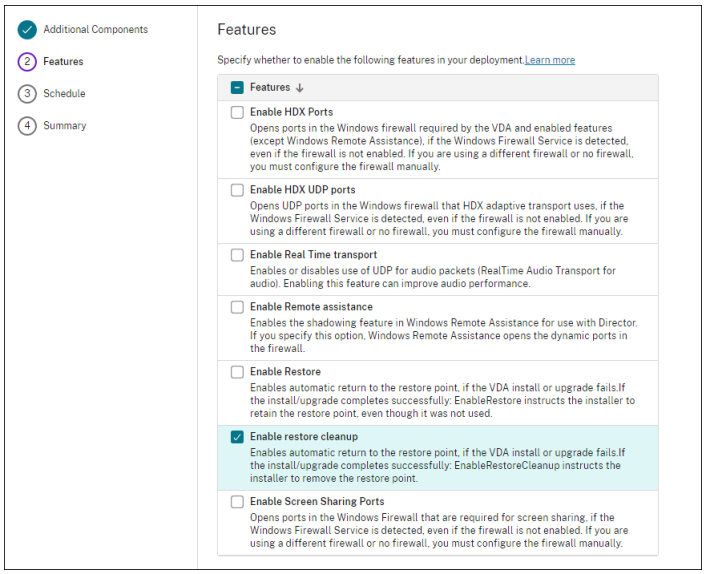
3. Escolha se deseja atualizar componentes adicionais em sua implantação. Você também pode optar por instalar determinados componentes além do upgrade. Se um componente exigir configuração, você deverá clicar no botão **Configure** e definir as configurações do componente para continuar. Depois de configurar, você pode clicar em **Editar** para alterar a configuração.

> **Importante:**
>
> - Para usar o recurso de componentes adicionais, certifique-se de que seu VDA Upgrade Agent seja da versão 7.34 ou posterior, que está incluída na versão 2206 ou posterior do instalador do VDA.
>
> **Nota:**
>
> - Se você optar por não atualizar um componente, o componente permanecerá intacto em sua implantação.
> - Para obter uma lista completa dos componentes adicionais, consulte Instalar VDAs.



4. Clique em **Avançar**.
5. Escolha se deseja ativar alguma das funções listadas. Clique em **Avançar**.

> **Nota:**
>
> Por padrão, a caixa de seleção **Enable restore cleanup** está marcada. Recomendamos ativar a função de restauração. Com a função ativada, um ponto de restauração do sistema é criado antes do início da atualização. 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.



6. Escolha se deseja atualizar os VDAs imediatamente ou em um horário agendado.

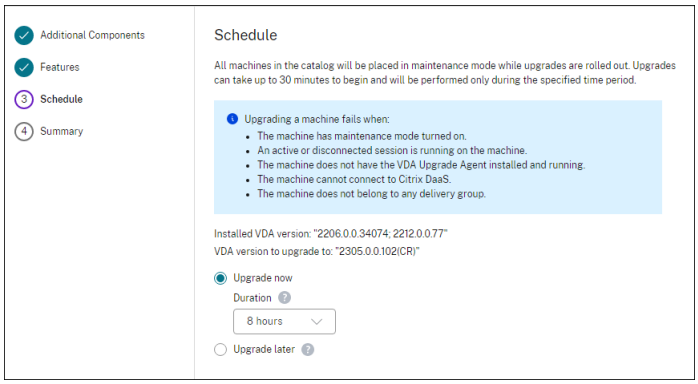
- Para atualizar os VDAs imediatamente, selecione **Upgrade now** e especifique uma duração.

  A duração é a quantidade de tempo, em horas, após a qual o Serviço de Upgrade do VDA interrompe a inicialização de upgrades adicionais. As atualizações em andamento serão concluídas. Durante esse período, o DaaS começa a atualizar os VDAs quando se tornam elegíveis (por exemplo, não há mais sessões ativas).

  Quanto mais VDAs precisarem ser atualizados, maior será a duração. Recomendamos selecionar um valor alto (por exemplo, 12 horas). Caso contrário, dependendo do número de VDAs, ainda pode haver VDAs que o DaaS não consiga atualizar nesse intervalo de tempo.

- Para agendar os upgrades, selecione **Upgrade later** e especifique quando você deseja que os upgrades ocorram.

  Você pode agendar os upgrades somente para os próximos sete dias. As atualizações programadas se aplicam somente às máquinas que estão atualmente no catálogo. Se você adicionar máquinas ao catálogo posteriormente, mas quiser atualizá-las também, cancele a atualização agendada e, em seguida, recrie uma programação.



7. Clique em **Avançar**.
8. Revise suas opções na página **Summary** e clique em **Finish** para aplicar suas configurações e sair da janela.

> **Nota:**
>
> - A opção **Upgrade VDAs** está disponível somente depois que você habilita a atualização do VDA para o catálogo. Para ativar a atualização do VDA, edite o catálogo.
> - Todas as máquinas no catálogo são colocadas no modo de manutenção enquanto as atualizações são implementadas. As atualizações podem levar até 30 minutos para que sejam iniciadas e serão realizadas somente durante o período de tempo especificado.

No nó **Machine Catalogs**, a coluna **VDA Upgrade** fornece informações de atualização de VDA para o catálogo. As seguintes informações podem aparecer:

> **Dica:**
>
> Para exibir a coluna **VDA Upgrade**, selecione **Columns to Display** na barra de ações, selecione **Machine Catalog > VDA Upgrade** e clique em **Save**.

- **Available**: uma nova versão do VDA está disponível.
- **Scheduled**: o upgrade do VDA foi agendado.
- **Not configured**: aparece quando você não habilitou a atualização do VDA para o catálogo.
- **Up to date**: os VDAs do catálogo estão atualizados.
- **Unknown**: não é possível obter as informações necessárias para a atualização do VDA. Há vários motivos possíveis:
  - O VDA estava em uso durante a janela de atualização.
  - O número de atualizações em andamento atingiu o limite máximo de 500.
  - O VDA Upgrade Agent parou de responder durante a janela de atualização. Certifique-se de que o agente esteja sendo executado no VDA e possa se comunicar com o Citrix DaaS.
  - Não é possível realizar verificações de validação de atualização. Consulte Requisito para atualização do VDA.

Você também pode visualizar o status das atualizações do VDA para um catálogo. Para fazer isso, clique no catálogo e, em seguida, verifique as informações do **VDA Upgrade State** na guia **Details**. As seguintes informações podem aparecer:

- **Not scheduled**: você ativou a atualização do VDA para o catálogo, mas não configurou uma programação de atualização.
- **Scheduled**: você criou um cronograma de atualização para o catálogo. Por exemplo, se você definir a programação para começar em `09:00 PM, December 14, 2030`, as informações aparecerão da seguinte forma: Scheduled for `December 14, 2030 09:00 PM UTC`.
- **In progress**: as atualizações do VDA foram iniciadas.
- **Canceled**: você cancelou o upgrade agendado.
- **Failed**: O catálogo contém uma ou mais máquinas cujas atualizações do VDA não foram bem-sucedidas.
- **Successful**: todos os VDAs no catálogo foram atualizados com sucesso.

Você também pode solucionar problemas de atualização do VDA com ações recomendadas para um catálogo. Para fazer isso, clique no catálogo e vá para a guia **Troubleshoot**.

Para detalhar rapidamente os catálogos que têm um estado específico de atualização do VDA, você pode usar filtros. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration.

Esteja ciente das seguintes considerações:

- O filtro **VDA Upgrade** ou **VDA Upgrade State** está disponível para uso somente com os seguintes filtros: **Name** e **Machine Catalog**.
- Quando você usa o filtro **VDA Upgrade** ou **VDA Upgrade State**, **Errors** e **Warnings** no canto superior direito ficam indisponíveis.

Editar ou cancelar um upgrade de VDA agendado

Depois de programar as atualizações para um catálogo, talvez você queira editar ou cancelar a atualização agendada. Para isso, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs**.
2. Selecione o catálogo e, em seguida, **Edit Scheduled VDA Upgrade** na barra de ações. A janela Editar atualização do VDA é exibida, mostrando informações sobre a versão instalada do VDA e a versão do VDA para a qual atualizar.
3. Escolha se deseja editar ou cancelar o upgrade agendado.
   - Para cancelar o upgrade, clique em **Cancel scheduled upgrade**. Lembre-se: O cancelamento da atualização agendada não força a interrupção da atualização em andamento.
4. Clique em **Done** para sair da janela.

Definir as configurações de upgrade do VDA editando um catálogo

Após a criação do catálogo, você pode definir as configurações de atualização do VDA editando o catálogo. Antes de começar a editar, considere o seguinte:

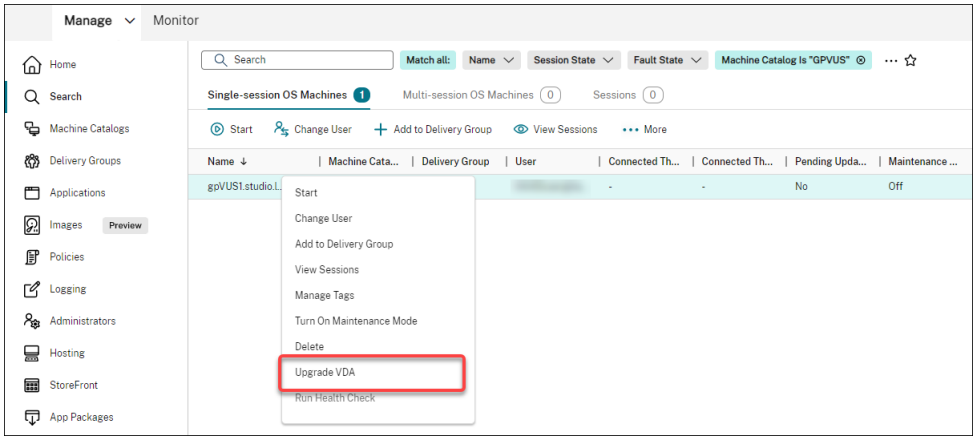
- Verifique se todas as máquinas no catálogo estão na mesma trilha VDA (CR ou LTSR). Caso contrário, alguns upgrades do VDA não serão realizadas. Por exemplo, se você selecionar **Latest LTSR VDA**, os upgrades CR VDA não serão realizados.
- As atualizações em algumas das máquinas do catálogo podem ter começado. Você não pode modificar upgrades que já estão em andamento. Os upgrades em andamento continuam. Aqueles que ainda não iniciaram serão atualizados para a versão especificada.

Fazer upgrade de VDAs por máquina

Depois de habilitar a atualização do VDA para um catálogo, você pode atualizar os VDAs do catálogo um por um ou em lotes. Para isso, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Search**.

2. Selecione uma ou mais máquinas e, em seguida, use **Upgrade VDA** no menu contextual ou na barra de ações. (Clique com o botão direito do mouse para exibir o menu contextual.)



> **Nota:**
>
> - Para que a opção **Upgrade VDA** esteja disponível, verifique se você ativou a atualização do VDA para o catálogo em que as máquinas selecionadas residem e que essas máquinas têm o VDA Upgrade Agent instalado. Para habilitar o upgrade do VDA para ele, edite o catálogo.
> - As máquinas serão colocadas no modo de manutenção enquanto os upgrades forem implementados. Os upgrades podem levar até 30 minutos para serem iniciados.
> - Se sua seleção contiver máquinas para as quais os upgrades do VDA não estão disponíveis ou cujas atualizações estão pendentes (programadas, em andamento ou aguardando atualizações), os upgrades para essas máquinas serão desconsiderados.

No nó **Search**, você pode adicionar a coluna **VDA Upgrade**. Para obter informações sobre como adicionar uma coluna personalizada, consulte Customize columns to display. A coluna é útil. Ele fornece informações de upgrade do VDA para a máquina. As seguintes informações podem aparecer:

- **Available**: uma nova versão do VDA está disponível.
- **Scheduled**: o upgrade do VDA foi agendado.
- **Not configured**: aparece quando você não habilitou o upgrade do VDA para a máquina.
- **Up to date**: O VDA está atualizado.
- **Unknown**: as informações sobre o upgrade do VDA ainda não estão disponíveis.

Você também pode visualizar o status do upgrade do VDA para uma máquina. Para fazer isso, clique na máquina e, em seguida, verifique as informações do **VDA Upgrade State** na guia **Details**. As seguintes informações podem aparecer:

- **Unknown**: não é possível obter as informações necessárias para a atualização do VDA. Há vários motivos possíveis:
  - O VDA estava em uso durante a janela de atualização.

  - O número de atualizações em andamento atingiu o limite máximo de 500.
  - O VDA Upgrade Agent parou de responder durante a janela de atualização. Certifique-se de que o agente esteja sendo executado no VDA e possa se comunicar com o Citrix DaaS.
  - Não é possível realizar verificações de validação de atualização. Consulte Requisito para atualização do VDA.

- **Scheduled**: você configurou um cronograma de upgrade. Por exemplo, se você definir a programação para começar em `09:00 PM, December 14, 2030`, as informações aparecerão da seguinte forma: Scheduled for `December 14, 2030 09:00 PM UTC`.
- **Awaiting upgrade**: a máquina é colocada no modo de manutenção, aguardando o upgrade. (Os usuários deverão ter saído da sessão para que o upgrade possa continuar.)
- **In progress**: o upgrade do VDA foi iniciado.
- **Upgrade failed**: as tentativas de fazer o upgrade o VDA foram malsucedidas.
- **Validation failed**: as tentativas de validar as configurações de upgrade do VDA foram malsucedidas.
- **Canceled**: o upgrade da máquina foi cancelado.
- **Successful**: o upgrade do VDA foi feito com sucesso.

Você também pode solucionar problemas de upgrade do VDA com ações recomendadas para uma máquina. Para fazer isso, clique na máquina e vá para a guia **Troubleshoot**.

Para detalhar rapidamente as máquinas que têm um estado específico de atualização do VDA, você pode usar filtros. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento Full Configuration. Esteja ciente das seguintes considerações:

- O filtro **VDA Upgrade** ou **VDA Upgrade State** está disponível para uso somente com os seguintes filtros: **Name** e **Machine Catalog**.
- Quando você usa o filtro **VDA Upgrade** ou **VDA Upgrade State**, **Errors** e **Warnings** no canto superior direito ficam indisponíveis.

Usar PowerShell para verificar o status do upgrade do VDA e a versão do VDA

Use o comando `Get-VusCatalog` do PowerShell para verificar o status do upgrade do VDA. Suponhamos que o nome do catálogo seja `wuhanTestMC1`. Você pode digitar o seguinte no prompt de comando:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`


```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades            : 0
DurationInHours              : 8
FailedUpgrades               : 0
InProgressUpgrades           : 0
LastStateChangeInUtc         : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades        : 100
Name                         : wuhanTestMC1
ProvisioningType             : MCS
ScheduledTimeInUtc           : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades  : 0
SessionSupport               : SingleSession
StateId                      : UpgradeSuccessful
SuccessfulUpgrades           : 1
TotalMachines                : 1
Uid                          : 12
UpgradeState                 : UpgradeAvailable
UpgradeType                  : CR
UpgradeVersion               : 2112.0.0.32068
Uuid                         : 339e7bce-271b-4c37-9a1c-bce287008b65
```

Neste exemplo, `UpgradeState` é `UpgradeAvailable`, o que significa que o upgrade do VDA está habilitado para o catálogo. `StateId` é `UpgradeSuccessful`, o que significa que o catálogo foi atualizado com êxito para 2112.0.0.32068 (`UpgradeVersion`).

Use o comando `Get-BrokerMachine` do PowerShell para obter a versão atual do VDA.


```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Use o comando `Get-VusAvailableVdaVersion` do PowerShell para obter a versão mais recente do VDA.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```


Redefinir disco do sistema operacional

Use o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. Atualmente, esse recurso é aplicável aos ambientes de virtualização do Azure, Citrix Hypervisor, Google Cloud, SCVMM e VMware.

Para executar com êxito o comando PowerShell, certifique-se de que:

- As VMs de destino estão em um catálogo persistente do MCS.
- O catálogo de máquinas MCS está funcionando corretamente. Isso implica que o esquema de provisionamento e o host existem e que o esquema de provisionamento tem entradas corretas.
- O hipervisor não está no modo de manutenção.
- As VMs de destino estão desligadas e no modo de manutenção.

Execute as seguintes etapas para redefinir o disco do sistema operacional:

1. Abra uma janela do **PowerShell**.
2. Execute asnp citrix* para carregar os módulos do PowerShell específicos à Citrix.
3. Execute o comando `Reset-ProvVMDisk` do PowerShell de qualquer uma das seguintes formas:

   - 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
   <!--NeedCopy-->
   ```

   - Especifique a lista de VMs como saída do comando `Get-ProvVM` e execute a redefinição em cada VM:

   ```
   (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
       "abc" -OS
   <!--NeedCopy-->
   ```

   - Especifique uma única VM pelo nome:

   ```
   Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
       -OS
   <!--NeedCopy-->
   ```

   - 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 a verificação da capacidade do hipervisor e verificação de conexão para cada VM.


```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. É exibido um prompt de confirmação que lista as VMs a serem redefinidas juntamente com uma mensagem de aviso de que essa é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma ação é executada.

   Você pode executar o comando do PowerShell `-WhatIf` para imprimir a ação que ele tomaria e sair sem realizar a ação.

   Você também pode ignorar a solicitação de confirmação usando um dos seguintes métodos:

   - Forneça o parâmetro `-Force`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     <!--NeedCopy-->
     ```

   - Forneça o parâmetro `-Confirm:$false`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Confirm:$false
     <!--NeedCopy-->
     ```

   - Antes de executar o `Reset-ProvVMDisk`, mude `$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
     <!--NeedCopy-->
     ```

> **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`.

Alterar a configuração de rede de um esquema de provisionamento existente

Você pode alterar a configuração de rede de 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.

Para alterar a configuração de rede de 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 chegar ao caminho de rede que deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Execute `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar a nova configuração de rede do esquema de provisionamento existente.

Gerenciar o conjunto de configurações para um catálogo

Antes de começar, verifique se você configurou a implantação do serviço WEM. Para obter mais informações, consulte Primeiros passos com o serviço Workspace Environment Management.

> **Nota:**
>
> Por padrão, se você tiver a função Cloud Administrator, Full Access Administrator ou Machine Catalog , poderá gerenciar conjuntos de configurações para catálogos. Se necessário, você pode permitir que as funções gerenciem conjuntos de configurações concedendo a elas a permissão **Manage configuration sets**.

Vincular um catálogo a um conjunto de configurações

> **Importante:**
>
> Se o Citrix DaaS e as instâncias do serviço WEM não residirem na mesma região, você não poderá vincular um catálogo a um conjunto de configurações. Nesse caso, migre seu serviço WEM para a mesma região que o Citrix DaaS.

Para vincular um catálogo a um conjunto de configurações, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs**.
2. Selecione o catálogo de máquinas e, em seguida, **Manage configuration set** na barra de ações. É exibida a janela **Manage configuration set**.

3. Selecione um conjunto de configurações do WEM ao qual você deseja vincular o catálogo.

> **Nota:**
>
> Se o conjunto de configurações selecionado não contiver configurações relacionadas à configuração básica do WEM, a opção **Apply basic settings to configuration set** será exibida. Recomendamos que você selecione a opção para aplicar as configurações básicas ao conjunto de configurações.

4. Clique em **Save** para salvar sua alteração.

Mudar para um conjunto de configurações diferente

Para alternar para um conjunto de configurações diferente para um catálogo, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs**.
2. Selecione o catálogo de máquinas e, em seguida, **Manage configuration set** na barra de ações. É exibida a janela **Manage configuration set**.
3. Selecione um conjunto de configurações do WEM diferente ao qual você deseja vincular o catálogo.
4. Clique em **Save** para salvar sua alteração.

Desvincular um catálogo do conjunto de configurações

Para desvincular um catálogo do conjunto de configurações, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs**.
2. Selecione o catálogo de máquinas e, em seguida, **Manage configuration set** na barra de ações. É exibida a janela **Manage configuration set**.
3. Clique no ícone X no lado direito do conjunto de configurações selecionado.
4. Clique em **Save** para salvar sua alteração.

Adicionar descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagens 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, o *Office 365 instalado*. Use os seguintes comandos para adicionar ou exibir descrições de imagens:

- `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"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Use esse 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"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Exibir 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

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
<!--NeedCopy-->
```

Repetir a criação do catálogo

> **Nota:**
>
> Esse recurso se aplica somente aos catálogos MCS.

Catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, acesse a guia **Troubleshoot** de cada catálogo. Antes de tentar novamente criar o 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.
- Não é possível alterar as configurações associadas ao sistema operacional e ao gerenciamento da máquina. O catálogo herda essas configurações do original.

- A criação pode levar algum tempo para ser concluída. Se necessário, selecione **Hide progress** para executar a criação em segundo plano.

Para tentar criar um catálogo novamente, faça o seguinte:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo e, em seguida, vá para a sua guia **Troubleshoot**.
3. Clique no hiperlink de nova tentativa para tentar criar o catálogo novamente.
4. No assistente exibido, altere as configurações onde necessário. Se não houver necessidade de fazer alterações, você pode ir diretamente para a página **Summary**.
5. Quando terminar, selecione **Finish** para iniciar a criação.

Converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina

Você pode usar uma VM, uma especificação de modelo (no caso do Azure) ou um modelo de inicialização (no caso da AWS) como entrada de perfil de máquina para converter um catálogo de máquina não baseado em perfil de máquina em um catálogo de máquina baseado em perfil de máquina. As novas VMs adicionadas ao catálogo obtêm os valores de propriedades do perfil da máquina.

> **Nota:**
>
> Um catálogo de máquinas existente baseado no perfil da máquina não pode ser alterado para um catálogo de máquinas que não baseado no perfil da máquina.

Para isso:

1. Crie um catálogo de máquinas persistente ou não persistente com VMs e sem um perfil de máquina.
2. Abra uma janela do **PowerShell**.
3. Execute o comando `Set-ProvScheme` para aplicar os valores das propriedades do perfil da máquina às novas VMs adicionadas ao catálogo de máquinas. Por exemplo:
   - No caso do Azure:

     ```
     Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
        -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
        machineprofile.folder<ResourceGroupName><TemplateSpecName
        ><VersionName>
     <!--NeedCopy-->
     ```

   - No caso da AWS:


```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
<!--NeedCopy-->
```

Reparar as informações de identidade de contas de computador ativas

Você pode redefinir as informações de identidade de contas de computador ativas que tenham problemas relacionados à identidade. Você pode optar por redefinir somente a senha da máquina e as chaves confiáveis ou redefinir todas as configurações do disco de identidade. A implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

> **Nota:**
>
> Atualmente, o recurso é suportado somente para ambientes de virtualização do Azure e VMware.

Condições

Certifique-se do seguinte para redefinir com êxito o disco de identidade:

- Desligue e defina a VM para o modo de manutenção
- Não inclua o parâmetro -OS no comando PowerShell

Redefinir disco de identidade

Para redefinir o disco de identidade:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Redefina as informações de identidade.
   - Para redefinir somente a senha da máquina e as chaves confiáveis, execute os seguintes comandos na seguinte ordem:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
         PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
         $password -Target IdentityInfo
     <!--NeedCopy-->
     ```

     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 AzureAD).
- `PrivilegedUserPassword`: senha para PrivilegedUserName.
- `Target`: destino da ação de reparo. Pode ser IdentityInfo, para reparar a senha/chave confiável da conta, e UserCertificate, para reparar os atributos do certificado do usuário das identidades de máquinas ingressadas no Hybrid AzureAD.

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
    > -Identity -ResetIdentityInfo
<!--NeedCopy-->
```

O parâmetro `ResetIdentityInfo` redefine o seguinte:

- Senha e chaves confiáveis: se a VM estiver ingressada no domínio AD (somente para Citrix DaaS)
- Somente chaves confiáveis: se a VM não estiver ingressada no domínio AD (somente para Citrix DaaS)
- Somente senha: se a VM estiver ingressada no domínio AD (somente para Citrix Virtual Apps and Desktops)

- Para redefinir todas as configurações do disco de identidade, execute os seguintes comandos na seguinte ordem:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Digite **y** para confirmar a ação. Você também pode ignorar o prompt de confirmação usando o parâmetro `-Force`. Por exemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--NeedCopy-->
```

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. `StorageId` e `IdentityDiskIndex` não devem mudar.

Alterar a configuração do cache em 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

Atualmente, esse recurso é aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO habilitado

Requisitos

Os requisitos para modificar a configuração do cache são:

- Atualize para a versão mais recente do VDA (2308 ou posterior).
- Ative o parâmetro `UseWriteBackCache` para o catálogo de máquinas existente. Use `New-ProvScheme` para criar um catálogo de máquinas com `UseWriteBackCache` ativado. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

Alterar a configuração do cache

Execute o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDisk32 -
   WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Nota:**
>
> - O valor de `WriteBackCacheDiskSize` deve ser maior que zero porque 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 só afetam as novas VMs adicionadas ao catálogo depois que a alteração foi feita. As VMs existentes não são afetadas por essas mudanças.

Solucionar problemas

- Para máquinas com status `Power State Unknown`, consulte CTX131267 para obter orientação.
- Para corrigir VMs que mostram continuamente um estado de energia desconhecido, consulte How to fix VMs that continuously show an unknown power state.
- Se um Cloud Connector não estiver funcionando corretamente, as operações de provisionamento do MCS (como atualizações de catálogo) demoram muito mais do que o normal e o desempenho do console de gerenciamento diminui significativamente.

O que fazer a seguir

Para obter informações sobre o gerenciamento de catálogos de hipervisores específicos, consulte:

- Gerenciar um catálogo da AWS
- Gerenciar um catálogo do Citrix Hypervisor
- 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 da VMware

Gerenciar um catálogo da AWS

December 20, 2023

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem da AWS.

> **Nota:**
>
> Antes de gerenciar um catálogo da AWS, você precisa concluir a criação de um catálogo da AWS. Consulte Criar um catálogo da AWS.

Remover tags

Quando você cria um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Máquina virtual
- Volume do disco raiz
- Volume do disco de identidade
- NIC
- Imagem de disco raiz (AMI)
- Modelo de execução
- Captura instantânea da AMI ou do disco raiz

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix e remover tags. Você pode usar:

- O parâmetro `Remove-ProvVM` com `ForgetVM` para remover VMs e tags de uma única VM ou uma lista de VMs de um catálogo de máquinas.
- O parâmetro `Remove-ProvScheme` com `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e recursos de um catálogo de máquinas.

Esse recurso é aplicável somente a VMs persistentes.

Para isso:

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Desbloqueie a máquina virtual antes de remover as VMs. Por exemplo:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Execute um dos comandos a seguir para remover VMs, catálogo de máquinas e tags dos recursos.

   - Execute `Remove-ProvVM` com `ForgetVM` para remover VMs do banco de dados Citrix e tags das VMs. Por exemplo:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
    >" -ForgetVM
<!--NeedCopy-->
```

   - Execute `Remove-ProvScheme` para remover o catálogo de máquinas do banco de dados Citrix e os recursos de um catálogo de máquinas. Por exemplo:


```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
<!--NeedCopy-->
```

5. Confirme que 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 da AWS EC2. Você deve ver as VMs, no entanto, as tags agora foram removidas. As tags dos seguintes recursos são removidas:

      - Máquina virtual
      - Volume do disco raiz
      - Volume do disco de identidade
      - NIC

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 da AWS EC2 se os seguintes recursos foram removidos.

      - Imagem de disco raiz (AMI)
      - Modelo de execução
      - Captura instantânea 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 “key”:”value”.

Nome do recurso	Marca
Disco de identificação	“Name”: “VMName_IdentityDisk” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Imagem	“XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

Nome do recurso	Marca
NIC	“Description”: “XD Nic” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disco do sistema operacional	“Name”: “VMName_rootDisk” “XdConfig”: “XdProvisioned=True” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
PrepVM	“Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
Instantâneo publicado	“XdConfig”: “XdProvisioned=true” Se não for um instantâneo da AMI do Volume Worker, “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true]
Template	“XdConfig”: “XdProvisioned=true” [quando AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “”

Nome do recurso	Marca
VM in catalog	[quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n”
Volume worker AMI	[quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
Volume worker bootstraper	“Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “”
Volume worker instance	“Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true”

Mais informações

- Conexões e recursos
- Conexão com a AWS
- Criar catálogos de máquinas
- Criar um catálogo da AWS
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Citrix Hypervisor

December 21, 2022

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

Gerenciar um catálogo do Google Cloud Platform

July 4, 2023

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Google.

> **Nota:**
>
> Antes de gerenciar um catálogo do Google Cloud Platform, você precisa concluir a criação de 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. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo de máquinas ao qual deseja adicionar máquinas.
3. Selecione **Add Machines** na barra de ações.
4. Na página **Virtual Machines**, especifique o número de máquinas que deseja adicionar e selecione **Next**.
5. Na página **Machine Identities**, selecione uma conta do Active Directory e, em seguida, selecione **Next**.
6. Na página **Domain Credentials**, selecione **Enter credentials**, digite o nome de usuário e a senha, selecione **Save** e selecione **Next**.
7. Na página **Summary**, confirme as informações e selecione **Finish**.

Atualizar máquinas

Um recurso que pode ser útil nos casos em que você deseja atualizar a imagem mestre ou o nível funcional mínimo.

Para atualizar as máquinas, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo de máquinas que contém as máquinas que você deseja atualizar.
3. Selecione **Change Master Image** na barra de ações.
4. Na página **Master Image**, selecione uma VM e o nível funcional mínimo para o catálogo e, em seguida, selecione **Next**.
5. Na página **Rollout Strategy**, especifique quando deseja atualizar as máquinas e selecione **Next**.
6. Na página **Summary**, confirme as informações e selecione **Finish**.

Para reverter uma atualização de máquina, siga estas etapas:

> **Importante:**
>
> Não renomeie, exclua ou mova imagens mestre. Caso contrário, você não poderá reverter a atualização.

1. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
2. Selecione o catálogo de máquinas no qual deseja reverter a atualização da máquina.
3. Selecione **Roll Back Master Image** na barra de ações.
4. Na página **Overview**, confirme as informações e selecione **Next**.
5. Na página **Rollout Strategy**, configure a estratégia de implantação e selecione **Next**.
6. Na página **Summary**, confirme as informações e selecione **Finish**.

Gerenciamento de energia

O Citrix DaaS permite o gerenciamento de energia das máquinas do Google Cloud. Use o nó **Search** no painel de navegação para localizar a máquina cuja energia você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Delete
- Start
- Restart
- Force Restart
- Shut Down
- Force Shutdown
- Add to Delivery Group
- Manage Tags
- Turn On Maintenance Mode

Você também pode gerenciar as máquinas do Google Cloud usando Autoscale. Para isso, adicione as máquinas do Google Cloud a um grupo de entrega e ative Autoscale para o grupo de entrega. Para obter mais informações sobre Autoscale, consulte Autoscale.

Atualizar máquinas provisionadas usando o PowerShell

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, isso não afeta as máquinas existentes. Usando o comando `Set-ProvVMUpdateTimeWindow` do PowerShell, agora você pode aplicar o esquema de provisionamento atual a uma máquina persistente ou não persistente existente ou a um conjunto de máquinas. Atualmente, no GCP, a atualização de propriedade suportada por esse recurso é o perfil da 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

Para atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Atualize o esquema de provisionamento. Por exemplo,

```
`Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```


4. Atualize as máquinas existentes.

   - Para atualizar todas as máquinas existentes:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   - Para atualizar uma lista de máquinas específicas:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

   - Para atualizar máquinas com base na saída de `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Nota:**
>
> - `StartsNow` indica que a hora de início programada é a hora atual.
> - `DurationInMinutes` com um número negativo (por exemplo, —1) indica que não há limite superior na janela de tempo do cronograma.

5. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Reinicialize as máquinas. Na próxima vez que forem ligadas, as alterações às propriedades serão aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

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 das VMs existentes do catálogo:

- `PersistOSDisk`

- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Nota:**
>
> - A propriedade `StorageType` é para o disco do sistema operacional
> - A propriedade `PersistOsDisk` pode ser definida somente para catálogo não persistente com cache de write-back ativado

Essa implementação ajuda você a selecionar diferentes tipos de armazenamento para discos diferentes mesmo depois de criar um catálogo, e, assim, equilibrar os preços associados aos diferentes tipos de armazenamento.

Para fazer isso, use os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow` do PowerShell:

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 cadeia de caracteres das propriedades personalizadas:
   a) Copie as propriedades personalizadas para o 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>'
<!--NeedCopy-->
```

5. Atualize o catálogo existente. Por exemplo:


```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. Atualize as VMs existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Reinicie as VMs. Na próxima vez que forem ligadas, as alterações às propriedades personalizadas serão aplicadas às máquinas virtuais existentes.

Proteger a exclusão acidental da 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 do Google Cloud ou MCS 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` habilitado.

Se você tentar excluir uma instância de VM para a qual definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você receber a permissão `compute.instances.setDeletionProtection` ou a atribuição da função **Compute Admin** do IAM, poderá 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 “key”:”value”.

Nome do recurso	Marca
Disco de identificação	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Imagem	“CitrixResource”: “internal”

Nome do recurso	Marca
Disco do sistema operacional	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
Instantâneo publicado	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
Storage bucket	“CitrixResource”: “internal”
Template	“CitrixResource”: “internal”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “internal”
Disco WBC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. O plug-in também adiciona esse rótulo para VMs provisionadas pelo MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. Você pode usar esse rótulo para filtrar por catálogo no console do GCP. “CitrixResource”: “internal” CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

> **Nota:**
>
> Uma VM não fica visível no inventário da 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

- 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 do HPE Moonshot (prévia)

December 6, 2023

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos do catálogo do HPE Moonshot.

> **Nota:**
>
> Antes de gerenciar um catálogo do HPE Moonshot, você precisa terminar de criar um catálogo do HPE Moonshot.

Gerenciamento de energia

O Citrix DaaS permite que você faça o gerenciamento de energia das máquinas do HPE Moonshot. Use o nó **Search** no painel de navegação para localizar a máquina cuja energia você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Start
- Shut Down
- Force Shutdown
- Restart
- Reset

> **Nota:**
>
> As ações de energia **Suspend** e **Resume** não são aceitas.

Mais informações

- Criar e gerenciar conexões
- Conexão com o HPE Moonshot
- Criar catálogos de máquinas
- Criar um catálogo de máquinas do HPE Moonshot
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Microsoft Azure

December 20, 2023

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir abrangem 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 nos custos de armazenamento mudando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade `StorageTypeAtShutdown` personalizada.

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 `StorageType` personalizada ou na propriedade `WBCDiskStorageType` personalizada).

> **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.
> - A máquina virtual pode demorar um pouco mais para começar depois que você alterar o tipo de armazenamento para um nível inferior.

Requisitos

- Aplicável a um disco gerenciado. Isso implica que você defina a propriedade personalizada `UseManagedDisks` como true.
- Aplicável a um catálogo persistente e não persistente com um disco de sistema operacional permanente. Isso implica que você defina a propriedade personalizada `persistOsDisk` como true.
- Aplicável a um catálogo não persistente com um disco WBC persistente. Isso implica que você defina 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 de `StorageType` acontece sempre que há uma ação de Iniciar ou Desalocar para a VM. Portanto, limite o número de ações de energia por VM a duas vezes por dia. Por exemplo, uma ação de energia pela manhã para iniciar a VM e outra 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`. Para obter informações sobre como criar um catálogo usando o PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Se `StorageTypeAtShutdown` tiver qualquer valor diferente de vazio ou Standard_LRS (HDD), a operação falhará.

   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> ’
<!--NeedCopy-->
```

   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> '
<!--NeedCopy-->
```

> **Nota:**
>
> Quando você usa 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 `StorageTypeAtShutdown` personalizada.
3. Ligue a VM. O tipo de armazenamento do disco volta para o tipo de armazenamento mencionado em:
   - Propriedade personalizada `StorageType` para disco do sistema operacional
   - Propriedade personalizada `WBCDiskStorageType` para o disco WBC somente se você especificar 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 configuração de 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
<!--NeedCopy-->
```

Alterar o tipo de armazenamento das 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 das VMs existentes para um nível inferior quando as VMs são desligadas.

Para alterar o tipo de armazenamento das máquinas existentes em um catálogo para um nível inferior quando as VMs são desligadas:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Altere a cadeia de caracteres das 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>'
<!--NeedCopy-->
```

5. Atualize o esquema de provisionamento do catálogo existente. A atualização se aplica às novas VMs adicionadas após a execução de `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Atualize as VMs existentes para habilitar `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Quando você ligar as máquinas na próxima vez, a propriedade `StorageTypeAtShutdown` das máquinas será atualizada. O tipo de armazenamento muda no próximo desligamento.
8. Execute o comando a seguir para visualizar o valor `StorageTypeAtShutdown` de 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  }
   }

<!--NeedCopy-->
```

Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, isso não afeta as máquinas existentes. Usando o comando `Set-ProvVMUpdateTimeWindow` do PowerShell, você pode aplicar o esquema de provisionamento atual a uma máquina persistente ou não persistente existente ou a um conjunto de máquinas. Você também pode agendar um horário para as atualizações de configuração das máquinas provisionadas pelo MCS existentes. Qualquer ativação ou reinicialização durante o horário programado aplica uma atualização programada do esquema de provisionamento a uma máquina. Atualmente, no Azure, você pode atualizar `ServiceOffering`, `MachineProfile` e as seguintes propriedades personalizadas:

- `StorageType`

- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> - Você só pode atualizar as propriedades personalizadas `StorageType`, `WBCDiskStorageType` e `IdentityDiskStorageType` de um catálogo usando o disco gerenciado em ambientes do Azure.
> - Se você executar `Set-ProvVMUpdateTimeWindow` duas vezes, o comando mais recente entrará em vigor.

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 de VM é recriada para catálogos persistentes no Azure:

- Altere o `MachineProfile`
- Remova `LicenseType`
- Remova `DedicatedHostGroupId`

> **Nota:**
>
> O disco do sistema operacional 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
<!--NeedCopy-->
```

2. Atualize o esquema de provisionamento. Por exemplo,

- Com a VM como entrada do perfil da máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
<!--NeedCopy-->
```

- Com a especificação do modelo como entrada do perfil da 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"
<!--NeedCopy-->
```

- Com apenas a oferta do serviço:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

Para solicitar que atualizações sejam aplicadas na próxima reinicialização das máquinas existentes:

1. Execute os comandos a seguir 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
<!--NeedCopy-->
```

- Para atualizar uma lista de máquinas específicas. Por exemplo,


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

> **Nota:**
>
> - `StartsNow` indica que a hora de início programada é a hora atual.
> - `DurationInMinutes` com um número negativo (por exemplo, —1) indica que não há limite superior na janela de tempo do cronograma.

2. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Reinicialize as máquinas. Na próxima vez que forem ligadas, as alterações às propriedades serão aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

Para programar a atualização de uma VM com as configurações de provisionamento mais recentes na próxima vez que ela for iniciada na janela do horário agendado.

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
<!--NeedCopy-->
```

   - 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
<!--NeedCopy-->
```


> **Nota:**
>
> - `VMName` é opcional. Se não for especificada, a atualização será 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 na janela de tempo do cronograma.

2. Verifique o status da atualização.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Ligue a VM. Se você ligar a máquina após o horário programado, a atualização da configuração não será aplicada. Se você ligar a máquina dentro do horário programado,

   - Se a máquina estiver desligada, e
     - você não ligar a máquina, a atualização de configuração não é aplicada
     - você ligar a máquina, a atualização de configuração é aplicada
   - Se a máquina estiver ligada, e
     - você não reiniciar a máquina, a atualização de configuração não é aplicada
     - você reiniciar a máquina, a atualização de configuração é aplicada

Para cancelar a atualização de 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 de uma única VM:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-
    catalog “ -VMName “ vm1 ”
<!--NeedCopy-->
```

   - Para cancelar a atualização de configuração agendada de várias VMs:

```
 Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```


> **Nota:**
>
> As VMs devem ser do mesmo catálogo.

Atualizar propriedades de VMs individuais

Você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistentes usando o comando `Set-ProvVM` do PowerShell. No entanto, as atualizações não são aplicadas imediatamente. Você deve definir a janela de tempo usando o comando `Set-ProvVMUpdateTimeWindow` do PowerShell para que as atualizações sejam aplicadas.

Essa implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, esse recurso é aplicável somente ao ambiente do Azure.

Atualmente, as propriedades que você pode atualizar são:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Usando esse 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 o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Verifique a configuração do catálogo de máquinas existente. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Verifique a configuração da VM na qual você deseja aplicar as atualizações. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Atualizar propriedades de uma VM

Faça o seguinte para atualizar as propriedades em uma VM:

1. Desative 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 AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

   Você pode atualizar as propriedades de duas VMs em um catálogo de máquinas simultaneamente. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

   > **Nota:**
   >
   > As atualizações não são aplicadas imediatamente.

3. Obtenha a lista de propriedades especificadas para serem atualizadas e a versão da configuração. Por exemplo:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

   Verifique o valor da propriedade `Version` e as propriedades a serem atualizadas (nesse caso, `StorageType`).

4. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização ainda não foi aplicada. A VM ainda está na configuração antiga.

5. Solicite uma atualização agendada. Por exemplo:

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
     StartsNow -DurationInMinutes -1
 <!--NeedCopy-->
```


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
<!--NeedCopy-->
```

7. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização agora está aplicada. A VM agora tem a nova configuração.

8. Para aplicar mais atualizações de configuração na VM, desligue-a e repita as etapas.

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. Desative 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 AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Obtenha os detalhes de configuração do catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

   Agora, `ProvisioningSchemeVersion` 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 AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```


> **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
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Nota:**
>
> Qualquer atualização na VM substituirá as atualizações feitas no catálogo de máquinas.

6. Solicite uma atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

A VM mantém seu tamanho de VM atualizado conforme derivado do perfil da máquina. Os valores da tag, conforme especificado 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 AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Agora, `ProvisioningSchemeVersion` e `ProvVMConfigurationVersion` mostram a versão mais recente.

Reverter as atualizações de configuração aplicadas a uma VM

1. Depois de aplicar as atualizações a uma VM, desligue-a.
2. Execute o comando a seguir para remover as atualizações aplicadas à VM. Por exemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```


3. Solicite uma atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Verifique a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   Agora, o valor `ProvVMConfigurationVersion` é a versão de configuração do catálogo de máquinas.

Recuperar informações para VMs do Azure, instantâneos, disco de SO e definição de imagem da galeria

Você pode exibir informações para uma VM do Azure, incluindo disco de SO e tipo, 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 exibir e selecionar uma imagem do Linux ou do Windows. Uma propriedade do PowerShell, `TemplateIsWindowsTemplate`, foi adicionada ao parâmetro `AdditionDatafield`. Esse campo contém informações específicas do Azure: tipo de VM, disco de SO, informações da imagem da galeria e informações do tipo do sistema operacional. Se `TemplateIsWindowsTemplate` for definido como **True**, isso indica que o tipo de sistema operacional é Windows; se `TemplateIsWindowsTemplat` for definido como **False**, isso indica que o tipo de sistema operacional é Linux.

> **Dica:**
>
> As informações exibidas pela propriedade do `TemplateIsWindowsTemplate` PowerShell são derivadas da API do Azure. Às vezes, esse campo pode estar vazio. Por exemplo, um instantâneo de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de sistema operacional não pode ser recuperado de um instantâneo.

Por exemplo, defina o parâmetro `AdditionData` da VM do Azure como **True** para o tipo de sistema operacional 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
<!--NeedCopy-->
```

Recupere informações de nome de região de VMs do Azure, discos gerenciados, instantâneos, VHD do Azure e modelos ARM

Você pode exibir informações de nome de região de uma VM do Azure, discos gerenciados, instantâneos, VHD do Azure e modelos ARM. Essas informações são exibidas para 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 do 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
<!--NeedCopy-->
```

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 “key”:”value”.

Nome do recurso	Marca
Disco de identificação	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Imagem	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Disco do sistema operacional	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Instantâneo publicado	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Resource group	“CitrixResource”: “Internal”
Storage account	CitrixSchemaVersion: 2.0 “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
VM in catalog	“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 da 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

Quando você cria um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Resource group
- Máquina virtual
- Disco do sistema operacional
- Disco de identidade
- Interface de rede
- Storage account

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix e remover tags. Você pode usar:

- O parâmetro `Remove-ProvVM` com `ForgetVM` para remover VMs e tags de uma única VM ou uma lista de VMs de um catálogo de máquinas.
- O parâmetro `Remove-ProvScheme` com `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e tags de um catálogo de máquinas inteiro.

Esse recurso é aplicável somente a VMs persistentes.

Para isso:

1. Abra uma janela do **PowerShell**.
2. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
3. Execute `Remove-ProvVM` para excluir VMs do banco de dados Citrix e tags de VMs.
   Por exemplo:

   ```
   1 Remove-ProvVM -ProvisioningSchemeName " ProvisioningSchemeName " -
       VMName " vmname " -ForgetVM
   2 <!--NeedCopy-->
   ```

4. Execute `Remove-ProvScheme` para excluir o catálogo de máquinas do banco de dados Citrix e tags dos catálogos de máquinas. Por exemplo:

   ```
   1 Remove-ProvScheme -ProvisioningSchemeName " ProvisioningSchemeName
       " -ForgetVM
   2 <!--NeedCopy-->
   ```

   > **Nota:**
   >
   > Depois de usar o parâmetro `ForgetVM` em `Remove-ProvScheme`, o MCS exclui todos

> os instantâneos, inclusive o instantâneo do disco básico, se o esquema de provisionamento estiver presente no BYORG (traga o seu próprio grupo de recursos) ou no grupo de recursos gerenciados Citrix.

Mais informações

- 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 System Center Virtual Machine Manager

December 21, 2022

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 Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de gerenciar um catálogo do VMM, você precisa concluir a criação de um catálogo do 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 “key”:”value”.

Nome do recurso	Marca
Prep VM	Cadeia de caracteres da marca: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Entrada de propriedade personalizada: “XdConfig:”XdProvisioned=True”

Nome do recurso	Marca
VM in catalog	Cadeia de caracteres da marca: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Entrada de propriedade personalizada: “XdConfig:”XdProvisioned=True”

Mais informações

- 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 do VMware

December 21, 2022

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 VMware.

> **Nota:**
>
> Antes de gerenciar um catálogo do VMware, você precisa concluir a criação de um catálogo do VMware. Consulte Criar um catálogo do VMware.

Atualizar o ID da pasta de um catálogo de máquinas

Você pode atualizar o ID da pasta de um catálogo de máquinas MCS especificando o `FolderId` nas propriedades personalizadas do comando `Set-ProvScheme`. As VMs criadas após a atualização do ID da pasta são criadas com esse novo ID de pasta. Se essa propriedade não for especificada no `CustomProperties`, as VMs serão criadas na pasta em que a imagem mestre está localizada.

Execute as etapas a seguir para atualizar o ID da pasta de um catálogo de máquinas.

1. Abra um navegador da Web e insira a URL do **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 do PowerShell específicos à Citrix.
6. Especifique `FolderID` em `CustomProperties` de `Set-ProvScheme`. Neste exemplo, o valor do ID da pasta é `group-v2406`.

```
Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -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>"
<!--NeedCopy-->
```

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 no vSphere

Acesse o MOB em qualquer sistema de servidor ESXi ou vCenter para encontrar o ID da pasta das VMs.

O MOB (Managed Object Browser) é um aplicativo de servidor baseado na Web, disponível em todos os sistemas de servidor ESX/ESXi e vCenter. Esse utilitário do vSphere permite que você visualize informações detalhadas sobre objetos como VMs, armazenamentos de dados 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 o host ESX/ESXi. Por exemplo, https://10.60.4.70/mob.
2. Na **página inicial** 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	Marca
Prep VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”

Mais informações

- Conexões e recursos
- Conexão com o VMware
- Criar catálogos de máquinas
- Crie um catálogo do VMware
- Gerenciar catálogos de máquinas

Gerenciamento de energia

December 6, 2023

Com o Citrix DaaS, você pode gerenciar a energia das VMs provisionadas pelo MCS em vários hipervisores e serviços de nuvem compatíveis. A operação de gerenciamento de energia fornece:

- Ótima experiência ao usuário
- Gerenciamento de custos e economia de energia

As ações disponíveis de energia são:

- Start
- Shut down
- Restart
- Suspend
- Resume
- Force restart
- Force shutdown

> **Nota:**
>
> - Para uma VM não persistente, o ciclo de alimentação de energia (desligar/iniciar e reiniciar) faz com que o disco do sistema operacional seja reiniciado.
> - Os recursos e comportamentos da ação de energia variam dependendo dos hipervisores ou dos serviços de nuvem.

O artigo aborda os principais recursos de gerenciamento de energia associados a determinados hipervisores compatíveis.

- Gerenciamento de energia de VMs da AWS
- Gerenciamento de energia de VMs do Azure

Gerenciamento de energia de VMs da AWS

December 6, 2023

Para obter informações sobre as permissões necessárias, consulte Sobre as permissões da AWS.

Hibernação de instâncias

O processo de hibernação armazena o estado na memória da instância, junto com seus endereços Elastic IP e privado, permitindo que ela continue exatamente de onde parou.

Quando uma instância é instruída a hibernar, ela grava o estado na memória em um arquivo no volume raiz do EBS e depois se desliga. Um volume do Amazon EBS é um dispositivo de armazenamento durável em nível de bloco que você pode conectar às suas instâncias. Depois de anexar um volume a uma instância, você pode usá-lo da mesma forma que usaria um disco rígido físico. Criptografe o volume raiz do EBS da instância. A criptografia garante a proteção adequada dos dados confidenciais quando eles são copiados da memória para o volume do EBS. Para obter informações sobre a criptografia do EBS, consulte Criptografia do Amazon EBS.

A seguir estão as limitações de hibernação da instância suportada:

- Memória (RAM) da instância com apenas até 150 GB é suportada
- Modo de inicialização UEFI não é suportado
- SSD de uso geral e SSD IOPS provisionado só são suportados como tipos de volume do EBS.

A seguir está o recurso de conexão do host no nível do hipervisor.

- Hipervisores com capacidade de suspensão: VMware, Citrix Hypervisor, Hyper-V e GCP
- Hipervisores sem capacidade de suspensão: Nutanix, Azure e AWS

> **Nota:**
>
> - Todos os recursos de suspensão e hibernação são chamados de suspensão.
> - Para a AWS, a capacidade de suspensão é suportada no nível da máquina, mas não no nível do hipervisor.

Criar VMs compatíveis com hibernação

Para criar VMs compatíveis com hibernação:

1. Crie uma conexão de host. Consulte Conexão com a AWS.
2. Inicie uma instância com a raiz do EBS criptografada e a propriedade **Stop-Hibernate** ativada. Para obter mais informações sobre como iniciar a instância, criptografar o volume raiz do EBS e ativar a hibernação, consulte https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Use essa instância como uma imagem mestre para criar uma AMI.
3. Prepare a imagem mestre:
   a) Instale um VDA na imagem mestre. A Citrix recomenda a instalação da versão mais recente para permitir o acesso aos recursos 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) Associe a imagem mestre ao domínio onde aplicativos e áreas de trabalho são membros. Assegure-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas.
4. 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.
5. Crie um catálogo de máquinas usando o comando `New-ProvScheme`. Defina a propriedade personalizada `AwsCaptureInstanceProperties` como **True**. Para obter informações sobre como habilitar as propriedades da instância da AWS na interface Full Configuration, consulte Aplicação de propriedades de instância da AWS e marcação de recursos operacionais na interface Full Configuration.

```
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"
<!--NeedCopy-->
```

Para obter informações sobre como criar um catálogo de máquinas usando comandos do 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 tem a propriedade **Stop-Hibernate** ativada.
- A VM mestre for ingressada no domínio e tiver o VDA instalado.
- Você selecionar o tamanho correto da VM (oferta do serviço) que pode lidar com a hibernação.

O comando **New-ProvScheme** falhará com uma mensagem de erro apropriada se:

- A VM mestre estiver habilitada para hibernação, mas a oferta do serviço não for capaz de lidar com a hibernação.
- Se a VM mestre não for ingressada no domínio e não tiver nenhum VDA instalado.

Status de hibernação das ofertas do serviço e da AMI

Para obter o status de hibernação das ofertas do serviço e da 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 a oferta do serviço de um esquema de provisionamento existente suportado por hibernação

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
<!--NeedCopy-->
```

O sistema exibirá uma mensagem de exceção se a oferta do serviço não for compatível.

Criar um catálogo de máquinas com suporte a hibernação

Ao criar catálogos de máquinas, você pode usar um perfil de máquina que suporte a hibernação.

1. No assistente de criação de catálogo, siga as instruções até a seleção do perfil da máquina.
2. Na página **Machine Template**, clique em **Select a machine profile** e selecione um perfil de máquina.
3. Na página **Virtual Machine**, clique no ícone **Edit** e selecione uma VM.

   > **Nota:**
   >
   > Se o perfil da máquina estiver habilitado para hibernação, o sistema exibirá somente as VMs que podem ser hibernadas.

4. Siga as instruções na tela para concluir todas as configurações. A página **Summary** exibe o status de hibernação do catálogo.

   > **Nota:**
   >
   > Ao editar um catálogo de máquinas, quando você altera o perfil da máquina para um perfil habilitado para hibernação, você é solicitado para reconfigurar suas VMs de acordo.

Atualizar o catálogo de máquinas que oferece suporte à hibernação

Se você tentar atualizar um catálogo de máquinas existente com um catálogo de máquinas que não oferece suporte à hibernação, a atualização falhará com uma mensagem de erro apropriada.

Gerenciamento de energia de máquinas virtuais em hibernação

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 de suspensão.
3. Reiniciar a VM do estado de suspensão.

Para ver as opções de gerenciamento de energia, na interface **Manage > Full Configuration**, clique com o botão direito do mouse nas VMs hibernadas.

Você também pode ver o estado de energia como **Suspending** e **Suspended** para cada máquina virtual, de acordo com as operações de energia que você executa nas VMs.

Gerenciamento de energia de VMs do Azure

December 6, 2023

Para obter informações sobre as permissões necessárias, consulte Permissões necessárias do Azure.

Provisionamento sob demanda do Azure

Com o provisionamento sob demanda do Azure, as VMs são criadas somente quando o Citrix Virtual Apps and Desktops inicia uma ação de inicialização, após a conclusão do provisionamento.

Quando você usa o MCS para criar catálogos de máquina no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz os custos de armazenamento
- Oferece criação de catálogos mais rápida

Quando você cria um catálogo MCS, o portal do Azure exibe os grupos de segurança de rede, as interfaces de rede, as imagens base e os discos de identidade nos grupos de recursos.

O portal do Azure não mostra uma VM até que o Citrix Virtual Apps and Desktops inicie uma ação de inicialização para ela. Em seguida, o status da VM na interface Full Configuration muda para **On**. Existem dois tipos de máquinas com as seguintes diferenças:

- No caso de uma máquina em pool, o disco do sistema operacional e o cache de write-back existem somente quando a VM existe. Quando você desliga uma máquina em pool no console, a VM não fica visível no portal do Azure. Há uma economia significativa nos 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 armazenada até que a identidade da máquina seja excluída. Quando você encerra uma máquina dedicada no console, a VM ainda fica visível no portal do Azure.

Preservação de uma máquina virtual provisionada durante o ciclo de energia

Escolha se deseja preservar uma máquina virtual provisionada durante o ciclo de energia. Use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. Esse parâmetro oferece suporte a uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provisionada persiste quando a energia é desligada. 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` só se aplica 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 serão 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>
<!--NeedCopy-->
```

No exemplo a seguir, o `New-ProvScheme CustomProperties` parâmetro preserva o cache de gravação `PersistVM` definindo 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
 <!--NeedCopy-->
```

> **Dica:**
>
> A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco de SO deve ser mantido. Para preservar uma máquina virtual provisionada, primeiro preserve o disco de SO. Você não pode excluir o disco de SO sem primeiro excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem usar a especificação do parâmetro `PersistVm`.

Personalizar o comportamento de ativação em caso de falha na alteração do tipo de armazenamento

Ao ligar, o tipo de armazenamento de um disco gerenciado pode apresentar falha ao mudar para o tipo desejado devido a uma falha no Azure. Nesses cenários, a VM permanece desligada e uma mensagem de falha é enviada a você. No entanto, você pode optar por ligar a VM, mesmo quando o armazenamento não pode 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`:
  - Na ativação, a VM é ligada com o tipo de armazenamento incorreto.
  - Na desativação, 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`:
  - Na ativação, a VM permanece desligada com o tipo de armazenamento incorreto.
  - Na desativação, a VM permanece desligada com o tipo de armazenamento incorreto.

Para criar um catálogo de máquinas:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do 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>"
<!--NeedCopy-->
```

5. Crie o catálogo de máquinas. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Para atualizar um catálogo de máquinas existente que inclua a propriedade personalizada `FailSafeStorageType`. Essa 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>"
<!--NeedCopy-->
```

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>
<!--NeedCopy-->
```

2. Reinicie as VMs.

Criar VMs com capacidade de hibernação (prévia)

Em ambientes Azure, você pode criar um catálogo de máquinas MCS que aceite a hibernação. Usando esse recurso, você pode suspender uma VM e depois se reconectar ao estado anterior da VM quando um usuário fizer login novamente.

> **Nota:**
>
> O recurso de hibernação se aplica somente a catálogos de máquinas de SO de sessão única (persistentes e não persistentes).

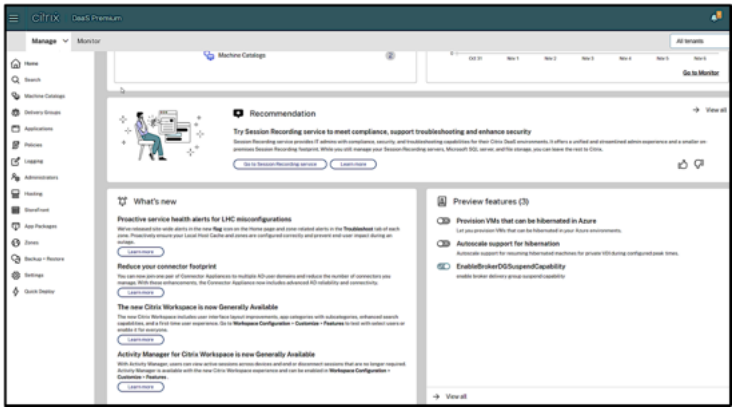
Nesta seção, consulte o seguinte:

- 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
- Habilitar a hibernação em VMs provisionadas por MCS existentes
- 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:

- Ative o recurso para sua assinatura do Azure. Consulte Habilitando o recurso de hibernação para sua assinatura.
- Ative as seguintes opções em **DaaS > Home > Preview features**:
  - **Provision VMs that can be hibernated in Azure**
  - **Autoscale support for hibernation**



- Instale o Azure VM Agent na imagem mestre para Windows e Linux. O arquivo de paginação da imagem do Windows pode estar no disco temporário. O MCS define a localização do arquivo de página como a unidade C: no disco base quando a hibernação está habilitada no catálogo de máquinas.
- O MCS define automaticamente a propriedade de hibernação para os recursos gerados. Você não precisa configurar as propriedades dos recursos principais para dar suporte à hibernação.
- Use um tamanho de VM em sua assinatura que ofereça suporte à hibernação.
- Crie um perfil de máquina com capacidade de hibernação (especificação de modelo ou VM) 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 habilitadas para hibernação a partir de um disco do sistema operacional. Atualmente, esse recurso é compatível com determinadas regiões e estará disponível para todas as regiões em breve. Para obter mais informações, consulte Implantar as VMs habilitadas para hibernação de um disco do sistema operacional.

Para criar a especificação do modelo, faça o seguinte:

1. Abra o Portal do Azure. Escolha uma VM cuja configuração você deseja usar no modelo. Selecione **Export template** no painel esquerdo.
2. Desmarque a caixa de seleção **Include parameters**. Copie o contexto e salve-o como um arquivo JSON, por exemplo, `VMExportTemplate.json`.
3. Certifique-se de que o parâmetro `hibernationEnabled` seja **`true`** no modelo. Se o parâmetro não for **`true`**, verifique a configuração da VM que você usou. Você pode especificar um tamanho de VM compatível no arquivo de modelo. No entanto, você também pode especificar o tamanho da máquina ao criar o catálogo.
4. Adicione o modelo para o recurso da interface de rede ao arquivo JSON `VMExportTemplate.json`. Como resultado, você tem um arquivo de modelo ARM com duas funções.

5. Selecione **Azure Portal > Template specs > Import template > Choose local template file** para importar esse arquivo de modelo como uma especificação de modelo ARM.
6. Depois que a especificação do modelo ARM for criada, você poderá usá-la como um perfil de máquina.

> **Nota:**
>
> Pode levar alguns minutos para sincronizar com o Citrix Studio.

Para obter mais informações, consulte o documento da Microsoft Pré-requisitos para usar hibernação.

Limitações

- Somente catálogos de máquinas de SO de sessão única (persistentes e não persistentes) são suportados.
- Os discos de SO efêmero e os recursos MCS I/O não oferecem suporte à hibernação do Azure.
- A hibernação pode falhar durante as atualizações automáticas do Windows.

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:

- Interface Full Configuration, ou
- Comandos do PowerShell

Criar um catálogo usando a interface Full Configuration

1. Faça login no Citrix Cloud. No menu superior esquerdo, selecione **My Services > DaaS**.
2. Em **Manage > Full Configuration**, selecione **Machine Catalogs** no painel esquerdo.
3. Selecione **Create Machine Catalog**. O assistente de criação de catálogo é aberto.
4. Na página **Machine Type** selecione o tipo de máquina **Single-session OS** para esse catálogo.
5. Na página **Machine Management**, selecione as configurações da seguinte forma:
   a) Selecione **Machines that are power managed (for example, virtual machines or blade PCs)**.
   b) Selecione **Citrix Machine Creation Services (MCS)**.

6. Na página **Desktop Experience**, selecione a experiência de área de trabalho aleatória ou estática, conforme necessário.
7. Na página **Image**, selecione uma imagem mestre. Marque a caixa de seleção **Use a machine profile** e selecione um perfil de máquina que suporte a hibernação. Clique na dica de ferramenta para saber se um perfil de máquina suporta hibernação.
8. Na página **Storage and License Types**, selecione o armazenamento e a licença a serem usados neste catálogo.
9. Na página **Virtual Machines**, selecione a contagem de VMs, o tamanho da VM e a zona de disponibilidade.

   > **Nota:**
   >
   > Os tamanhos de máquinas que suportam a hibernação são exibidos somente para a sua seleção.

10. Na página **NICs**, adicione as NICs que você deseja que as VMs usem.
11. Na página **Disk Settings**, selecione o tipo de armazenamento e o tamanho do disco de cache de write-back.
12. Na página **Resource Group**, selecione o grupo de recursos para provisionar VMs.
13. Na página **Machine Identities**, selecione **Create new Active Directory accounts**. Em seguida, especifique um esquema de nomenclatura de conta.
14. Na página **Domain Credentials**, clique em **Enter credentials**. Insira suas credenciais de domínio para realizar a criação da conta no domínio do Active Directory de destino.
15. Na página **Summary**, insira um nome para o catálogo de máquinas e clique em **Finish**.

Quando a criação do catálogo de máquinas MCS estiver concluída, localize o catálogo na lista de catálogos e clique na guia **Template Properties**. O valor do parâmetro **Hibernation** deve ser **Supported**.

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar a hibernação, você não pode:
  - Alterar o tamanho da VM para um que não tenha capacidade de hibernar.
  - Mudar o perfil da máquina para um que não tenha capacidade de hibernar.
- Se o catálogo de máquinas atual não oferecer suporte à hibernação, você não pode:
  - atualmente, alterar o perfil da máquina para um com capacidade de hibernação usando a interface Full Configuration. No entanto, você pode fazer isso usando os comandos do PowerShell. Consulte Habilitar a hibernação em VMs provisionadas por MCS existentes.

Criar um catálogo de máquinas para gerenciar VMs existentes com capacidade de hibernação
Se você já tem VMs com capacidade de hibernação e deseja suspendê-las e retomá-las, crie um catálogo de máquinas para importar essas VMs para o gerenciamento de energia.

> **Nota:**
>
> Você pode criar um catálogo de máquinas contendo VMs com capacidade e sem capacidade de hibernação. No entanto, se você quiser funcionalidades relacionadas à hibernação, deverá criar o catálogo de máquinas somente com VMs com capacidade de hibernação.

Para criar um catálogo de VMs existentes com capacidade de hibernação usando a interface Full Configuration, siga as instruções na tela para concluir as etapas e preste atenção especial às seguintes configurações:

1. Na página **Machine Management**, selecione **Machines that are power managed** e **Other service or technology** como a forma de implantar máquinas.
2. Na página **Virtual Machines**, adicione ou importe somente as VMs com capacidade de hibernação.

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 Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Ao criar o catálogo, você pode verificar se o tamanho da VM e o perfil da máquina suportam ou não a hibernação usando os seguintes comandos do PowerShell:

- Para o tamanho da VM, execute o comando a seguir e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @("
    XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder"
    ) | select Name, AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- Para o perfil da máquina, execute o comando a seguir e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @("
    XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder\
    abc.resourcegroup")|select Name, AdditionalData|ConvertTo-Json
<!--NeedCopy-->
```

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar a hibernação, você não pode:
  - Alterar o tamanho da VM para um que não tenha capacidade de hibernar
  - Mudar o perfil da máquina para um que não tenha capacidade de hibernar
- Se o catálogo de máquinas atual não oferecer suporte à hibernação, você não pode:
  - atualmente, alterar o perfil da máquina para um com capacidade de hibernação usando a interface Full Configuration. No entanto, você pode fazer isso usando os comandos do PowerShell. Consulte Habilitar a hibernação em VMs provisionadas por MCS existentes.

Para obter informações sobre como modificar o tamanho da VM e o perfil da máquina de um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Habilite a hibernação em VMs provisionadas por MCS existentes

Você pode habilitar a hibernação do Azure em:

- VMs provisionadas pelo Windows MCS de um catálogo de máquinas criado sem um disco temporário.
- VMs provisionadas pelo Linux MCS de um catálogo de máquinas criado com e sem um disco temporário.

> **Nota:**
>
> - As VMs provisionadas pelo MCS existentes devem ter um agente de VM do Azure instalado.
> - Atualmente, você só pode usar o comando PowerShell para ativar esse recurso.

Para isso:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Verifique a configuração das máquinas existentes. Por exemplo:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Ative a hibernação neste catálogo de máquinas usando o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
```



```
<!--NeedCopy-->
```

5. Solicite a atualização das VMs existentes em um catálogo de máquinas.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```

6. Reinicie as VMs para disparar atualizações nas VMs existentes. Por exemplo:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

Verificar propriedade de hibernação

Você pode verificar a propriedade de hibernação de um catálogo de máquinas, uma VM e uma máquina intermediária 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
<!--NeedCopy-->
```

- Para verificar a propriedade de hibernação de uma VM de provisionamento, execute os seguintes comandos do PowerShell. O parâmetro `SupportsHibernation` deve ser `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Para verificar a capacidade de hibernação de uma máquina intermediária, execute os seguintes comandos do PowerShell. As ações de energia **Suspend** e **Resume** indicam a capacidade de hibernação.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
    SupportedPowerActions
<!--NeedCopy-->
```

Gerenciamento de energia de VMs com capacidade de hibernação

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs com capacidade de hibernar:

- **Suspender** a VM do estado em execução

- **Retomar** a VM do estado de suspensão
- **Forçar o desligamento** da VM do estado de suspensão
- **Forçar a reinicialização** da VM do estado de suspensão

Consulte o seguinte para obter mais informações:

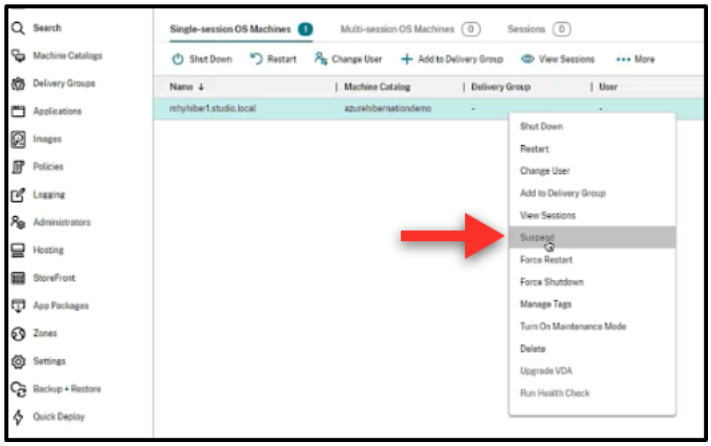
- Suspend
- Resume

Suspend Você pode suspender uma VM de uma das seguintes formas:

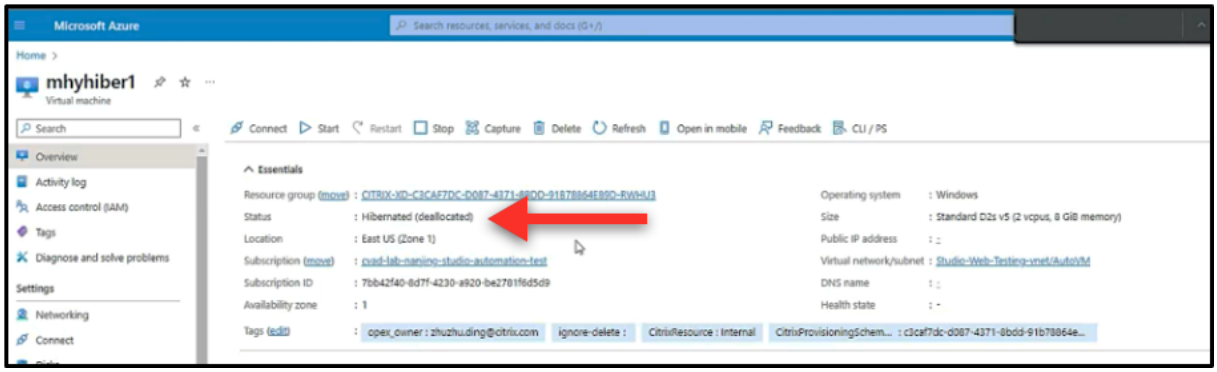
- **Manualmente**, usando a interface Full Configuration
- **Automaticamente**, usando a política de tempo limite: para obter mais informações, consulte Configurações diversas.

Para suspender manualmente uma VM:

1. Clique com o botão direito na VM e selecione **Suspend**. Clique em **Yes** para confirmar a ação. **Power State** muda de **Suspending** para **Suspended**.

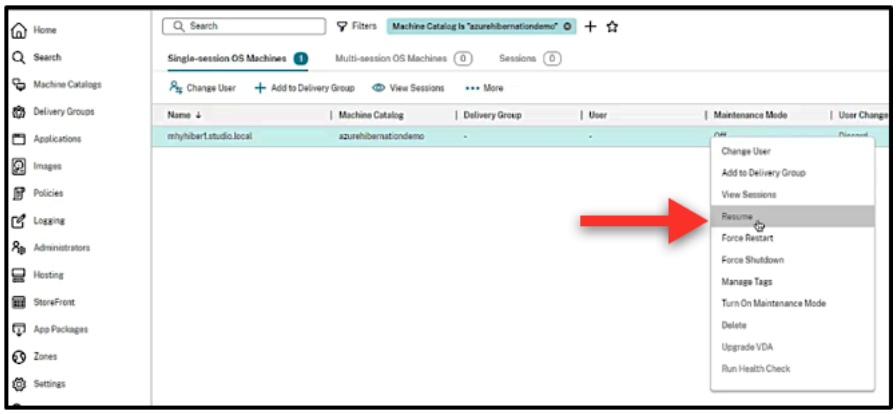


Você pode verificar o status da VM no portal do Azure.

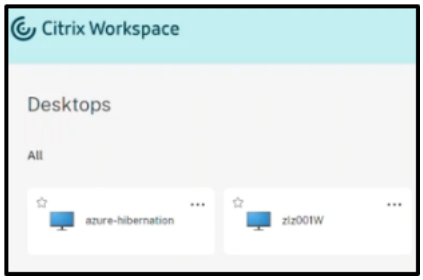


Resume Para retomar uma VM em hibernação, você pode fazê-lo:

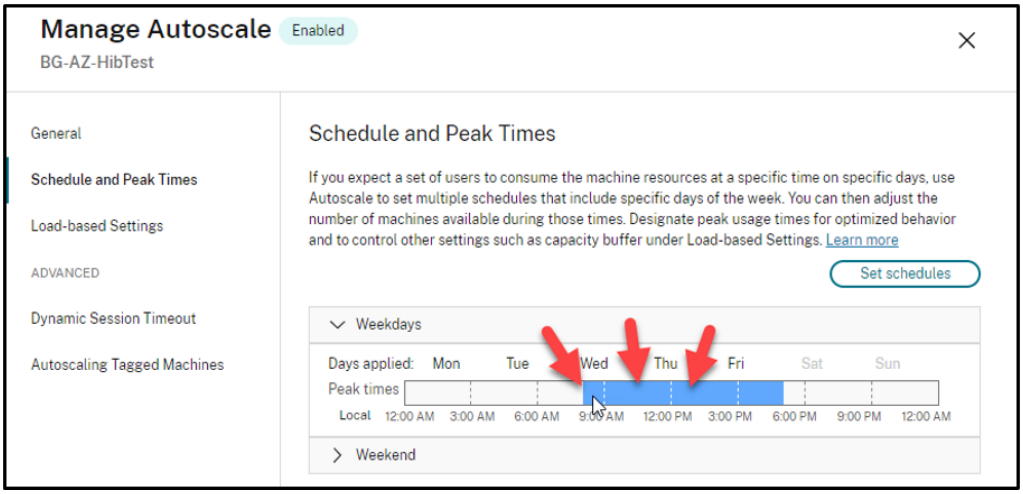
- **Manualmente**:
  - Os administradores podem retomar a VM usando a interface Full Configuration.



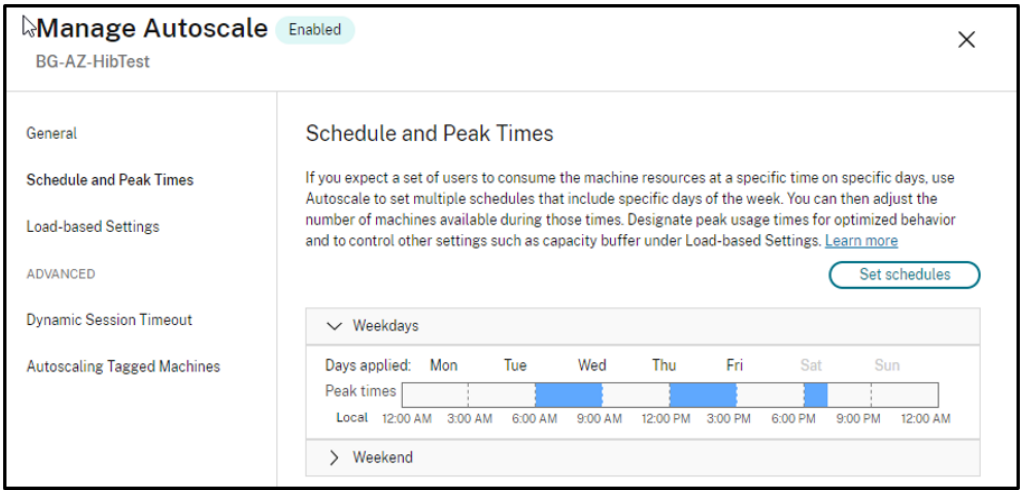
  - Os usuários finais podem iniciar a VM usando o menu Citrix Workspace depois de clicarem no ícone da área de trabalho.



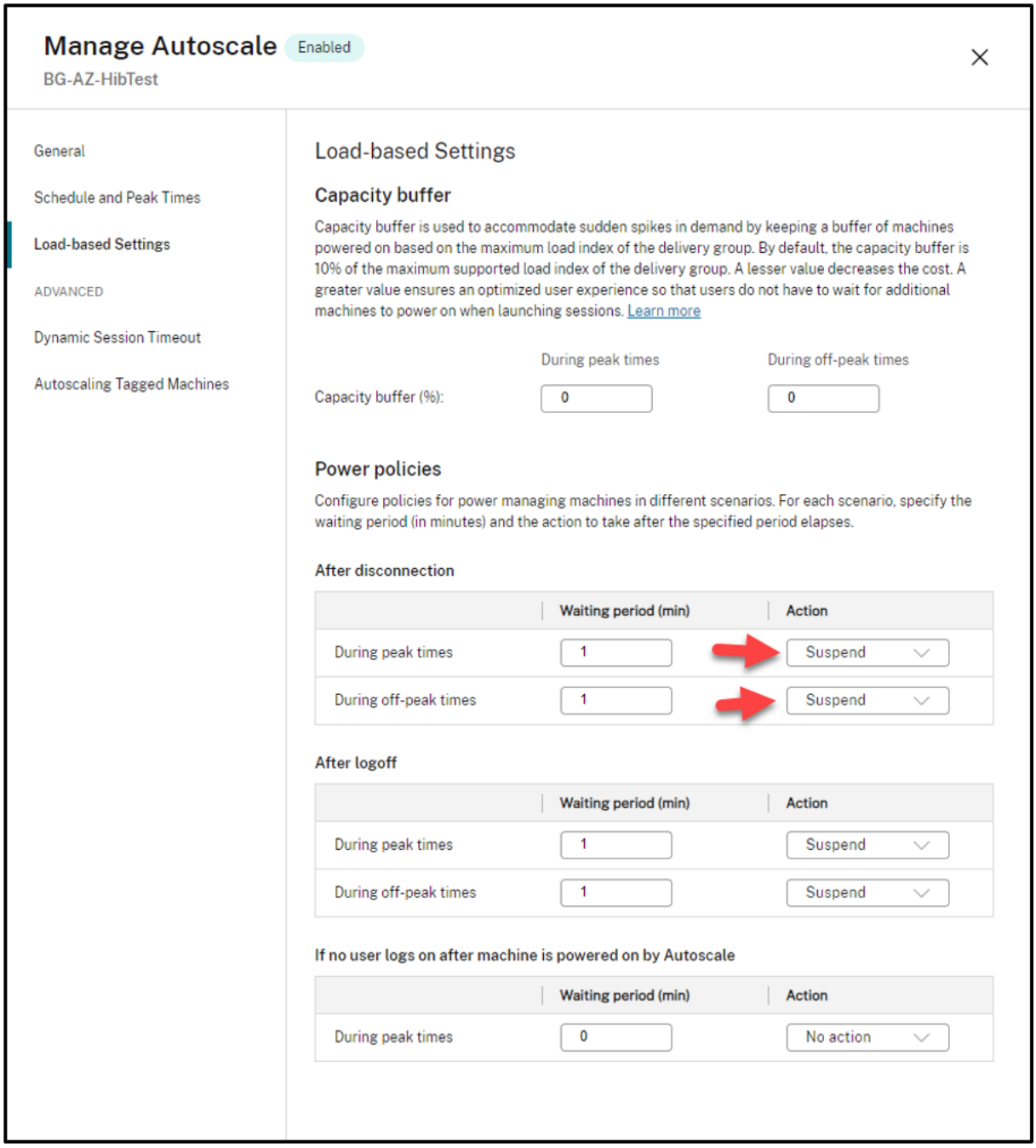
- **Automaticamente**:
  - O AutoScale pode ligar automaticamente as máquinas hibernadas se você configurar os horários de pico corretamente. Você pode definir os horários de pico em intervalos de 30 minutos clicando no cronograma. Cada moldura azul representa um intervalo de tempo marcado como horário de pico. Os horários de pico podem ter intervalos de tempo consecutivos e não consecutivos.
    - Intervalos de tempo consecutivos



* Intervalos de tempo não consecutivos



> **Nota:**
>
> Em **Manage Autoscale > Load-based Settings**, se **Action** estiver configurado como **Suspend**, certifique-se de que todas as VMs dentro desse grupo de entrega tenham capacidade de hibernação. Caso contrário, as VMs que não podem hibernar continuam em execução.



Mais informações

Para obter mais informações sobre a hibernação do Citrix Azure, consulte o artigo da Citrix Tech Zone.

Políticas de segurança

April 14, 2023

Este artigo descreve os recursos de segurança em vários hipervisores compatíveis. Os recursos de segurança incluem:

- Grupo de segurança
- Inicialização segura
- Recursos de criptografia

Grupo de segurança

April 14, 2023

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 entrada na rede, ou o tráfego de saída da rede, a vários tipos de recursos. Cada regra especifica as seguintes propriedades:

- Nome: um nome exclusivo dentro do grupo de segurança da rede
- Prioridade: as regras são processadas em ordem de prioridade, sendo os números mais baixos processados antes dos números mais altos, porque números mais baixos têm maior prioridade
- Origem ou destino: um endereço IP individual ou qualquer bloco de roteamento entre domínios sem classe (CIDR) (10.0.0.0/24, por exemplo), marca de serviço ou grupo de segurança de aplicativos
- 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 os hipervisores compatíveis:

- Grupo de segurança na AWS
- Grupo de segurança no Microsoft Azure
- Grupo de segurança no Google Cloud Platform

Grupo de segurança na AWS

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 pode associar esses grupos de segurança a cada instância na sua VPC. As regras de entrada controlam o tráfego de entrada na sua instância, e as regras de saída controlam o tráfego de saída da sua instância.

Para obter 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 às 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 o disco do sistema de imagem mestre para o catálogo. Quando esse processo ocorre, o disco é conectado temporariamente a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e de saída. Isso é feito por meio de um par de regras de firewall deny-all. Para obter mais informações, consulte Regras de firewall.

Inicialização segura

June 6, 2023

A inicialização segura foi projetada para garantir que somente softwares confiáveis sejam usados para inicializar o sistema. O firmware tem um banco de dados de certificados confiáveis e verifica se a imagem que ele carrega está assinada por um dos certificados confiáveis. Se a imagem carregar mais imagens, essa imagem também deverá ser verificada da mesma forma.

O vTPM é uma instância de software virtualizado de um módulo TPM físico tradicional. O vTPM permite o atestado medindo toda a cadeia de inicialização da sua VM (UEFI, sistema operacional, sistema e drivers).

Consulte o seguinte para obter mais informações sobre os hipervisores compatíveis:

- Inicialização segura no Google Cloud Platform
- Inicialização segura no Microsoft Azure
- Inicialização segura no VMware

Inicialização segura no Google Cloud Platform

Você pode provisionar máquinas virtuais protegidas no GCP. Uma máquina virtual protegida é reforçada usando um conjunto de controles de segurança que fornecem integridade verificável das instâncias do Compute Engine usando recursos avançados de segurança de plataforma, como reinicialização segura, Trusted Platform Module virtual, firmware UEFI e monitoramento de integridade.

Para obter mais informações sobre como usar o PowerShell para criar um catálogo com VM protegida, consulte Usar o PowerShell para criar um catálogo com VM protegida.

Inicialização segura no Microsoft Azure

Em ambientes Azure, você pode criar catálogos de máquinas habilitados com o Início confiável. O Azure oferece o início confiável como uma excelente maneira de melhorar a segurança das VMs de 2ª geração. O início confiável protege contra técnicas de ataque avançadas e persistentes. Na raiz do início confiável está a inicialização segura da sua VM. O início confiável também usa o vTPM para realizar o 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 o início confiável, consulte Catálogos de máquinas com início confiável.

Inicialização segura no VMware

O MCS suporta a criação de um catálogo de máquinas com o modelo VMware anexado ao vTPM como fonte para entrada do perfil da máquina. Se o Windows 11 estiver instalado na imagem mestre, é necessário ter o vTPM ativado para a imagem mestre. Portanto, o modelo VMware, que é uma fonte do perfil da máquina, deve ter o vTPM anexado a ele. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Recursos de criptografia

June 6, 2023

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 os hipervisores compatíveis:

- 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 nos ambientes de virtualização da AWS.

Criptografia automática

Você pode ativar a criptografia automática de novos volumes do Amazon EBS e cópias instantâneas 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 nos ambientes de virtualização do Google Cloud Platform (GCP).

Se você precisar de mais controle sobre as operações de chaves do que as chaves de criptografia gerenciadas pelo Google permitem, você pode usar chaves de criptografia gerenciadas pelo cliente. Quando usa 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 o objeto é entregue 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 do MCS. Para obter mais informações, consulte Usar chaves de criptografia gerenciadas pelo cliente (CMEK).

Recursos de criptografia no Microsoft Azure

Esta seção descreve os recursos de criptografia nos ambientes de virtualização do Azure.

Criptografia do servidor do Azure

A maioria dos discos gerenciados do Azure é criptografada com a criptografia do Azure Storage, 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 servidor do Azure.

Criptografia dupla do Azure

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 algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, instantâneos e imagens são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla no disco gerenciado.

Quick Deploy

November 21, 2023

Introdução

No Citrix DaaS, a interface **Manage > Quick Deploy** oferece implantação rápida de aplicativos e áreas de trabalho quando você usa o Microsoft Azure para hospedar suas áreas de trabalho e aplicativos. Essa interface oferece configuração básica, sem recursos avançados.

Use Quick Deploy para:

- Provisione máquinas virtuais e catálogos que fornecem áreas de trabalho e aplicativos hospedados no Microsoft Azure.
- Crie catálogos de acesso remoto a PC para máquinas existentes.

Com o Quick Deploy, você pode usar uma assinatura do Citrix Managed Azure ou sua própria assinatura do Azure.

(Embora os nomes sejam semelhantes, o Quick Deploy não é o mesmo que o método Quick Create de criação de catálogos na interface Quick Deploy.)

Como alternativa ao Quick Deploy, a interface de **Full Configuration** oferece recursos de configuração avançados. Para obter informações sobre as opções da guia **Manage**, consulte Management interfaces.

Diferenças entre interfaces de gerenciamento

A tabela a seguir compara as interfaces Full Configuration e Quick Deploy.

Recurso	Quick Deploy	Full Configuration
Implantar usando o Azure	Sim	Sim *
Implantar usando outros serviços de nuvem	Não	Sim
Implantar usando hipervisores locais	Não	Sim
Imagens preparadas pela Citrix disponíveis	Sim	Não
Experiência de usuário simplificada	Sim	Não

* Ao usar uma assinatura do Citrix Managed Azure, você deve usar o Quick Deploy ao criar uma imagem ou catálogo.

Se você estiver familiarizado com o uso de Full Configuration para criar e gerenciar catálogos, o Quick Deploy tem as seguintes diferenças.

- Terminologia diferente.
  - No Quick Deploy, você cria um catálogo.
  - Em Full Configuration, você cria um catálogo de máquinas. Na prática, muitas vezes é chamado simplesmente de catálogo.
- Localização de recursos e Cloud Connectors.
  - O Quick Deploy cria automaticamente um local de recurso contendo dois Cloud Connectors quando você cria seu primeiro catálogo.
  - Na Full Configuration, criar um local de recurso e adicionar conectores de nuvem 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 e usar imagens de suas próprias assinaturas do Azure.

  - Em Full Configuration, você personaliza imagens do host suportado que está usando. As imagens preparadas pela Citrix não estão disponíveis.

- O catálogo exibe:
  - Os catálogos criados no Quick Deploy são visíveis nos modos de exibição Quick Deploy e Full Configuration.
  - Os catálogos criados em Full Configuration não são visíveis no modo de exibição Quick Deploy.

- Grupos de entrega:
  - Você não cria grupos de entrega no Quick Deploy. Em Quick Deploy, você especifica as máquinas, os aplicativos, as áreas de trabalho e os usuários (assinantes) no catálogo.

    A Citrix cria automaticamente um grupo de entrega para cada catálogo de 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 somente na interface Full Configuration, não no Quick Deploy.
  - Em Full Configuration, você cria um grupo de entrega e indica quais máquinas ele contém. Opcionalmente, você também especifica aplicativos, áreas de trabalho e usuários. Você também pode criar grupos de aplicativos.

- Layout e interface de usuário.
  - A interface Quick Deploy tem um layout e estilo diferentes da Full Configuration. 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 a Full Configuration para criar outros catálogos.

Gerenciar catálogos criados na interface Quick Deploy

Depois de criar um catálogo na interface Quick Deploy, você pode continuar a gerenciar esse catálogo nessa interface. Para obter detalhes, consulte Gerenciar catálogos no Quick Deploy. Você também pode usar a interface Full Configuration.

Quando você cria um catálogo no Quick Deploy, o catálogo (mais o grupo de entrega e a conexão de hospedagem que são criados automaticamente nos bastidores) recebem um escopo de `Citrix managed object`. Os escopos são usados na administração delegada para objetos de grupo.

Catálogos, grupos de entrega e conexões com o escopo `Citrix managed object` são proibidos de determinadas ações na interface Full Configuration. (Permitir essas ações na Full Configuration pode afetar adversamente a capacidade do sistema de oferecer suporte à Quick Deploy e à Full Configuration, portanto, essas ações são desativadas.) Na interface Full Configuration:

- **Catálogo:** a maioria das ações de gerenciamento de catálogos não está disponível. Você não pode excluir um catálogo.
- **Grupo de entrega:** a maioria das ações de gerenciamento do grupo de entrega está disponível. Você não pode excluir o grupo de entrega.
- **Conexão:** A maioria das ações de gerenciamento de conexão não está disponível. Você não pode excluir uma conexão. Você não pode criar uma conexão baseada em uma conexão que tenha o escopo `Citrix managed object`.

Se você criar um catálogo na Quick Deploy usando sua própria assinatura do Azure (adicionada à Quick Deploy) e quiser gerenciar o catálogo (e seu grupo de entrega e conexão) inteiramente na Full Configuration, poderá *converter* o catálogo.

- A conversão de um catálogo restringe seu gerenciamento somente à interface Full Configuration. Depois que um catálogo é convertido, você não pode mais usar a interface de Quick Deploy para gerenciar esse catálogo.
- Depois que um catálogo é convertido, as ações que estavam anteriormente indisponíveis na Full Configuration podem ser selecionadas. (O escopo `Citrix managed object` é removido do catálogo convertido, do grupo de entrega e da conexão de hospedagem.)
- Para converter um catálogo:

  No painel **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo. Na guia **Details**, em **Advanced settings**, selecione **Convert Catalog**. Quando solicitado, confirme a conversão.
- Você não pode converter um catálogo que foi criado no Quick Deploy usando uma assinatura do Citrix Managed Azure.

Substituição da interface anterior do Azure Quick Deploy

O Quick Deploy substitui uma interface anterior chamada Azure Quick Deploy. A tela Quick Deploy inclui todos os catálogos que você criou usando o Azure Quick Deploy.

Se você começou a criar um catálogo no Azure Quick Deploy, mas não o concluiu, esse catálogo aparece na lista de catálogos do Quick Deploy. No entanto, a única ação disponível no Quick Deploy é excluí-lo.

Requisitos

- O Quick Deploy dá suporte apenas a cargas de trabalho do Azure. Ele não está disponível com nenhum outro tipo de host de nuvem, serviços ou hipervisores.
- O Quick Deploy está disponível somente no Citrix DaaS para as edições Azure, Premium e Advanced e Workspace Premium Plus.
- Você deve ter uma conta do Citrix Cloud e uma assinatura do Citrix DaaS.
- Se você solicitou o Citrix Managed Azure Consumption Fund, poderá usar uma assinatura do Citrix Managed Azure ao criar catálogos e imagens.

  Se você não solicitou o Fundo de Consumo (ou prefere usar sua própria assinatura do Azure), você deve ter uma assinatura do Azure.
- Você deve ter a permissão apropriada no Citrix DaaS para ver a guia **Manage**. Para obter detalhes, consulte Administração delegada.

> **Importante:**
>
> Para garantir que você obtenha informações importantes sobre o Citrix Cloud e os serviços Citrix que você assina, procure receber todas as notificações por e-mail. Por exemplo, a Citrix envia emails de notificação informativos mensais detalhando seu consumo (uso) do Azure.
>
> No canto superior direito do console do Citrix Cloud, expanda o menu à direita do nome do cliente e dos campos OrgID. Selecione **Configurações de conta**. Na guia **Meu perfil**, selecione todas as entradas na seção **Notificações por e-mail**.

Consideração sobre o Citrix Gateway

Se você usar seu próprio Citrix Gateway, ele deverá ter acesso à VNet especificada no assistente de criação de catálogo. Uma VPN pode fornecer esse acesso.

O Citrix Gateway Service funciona automaticamente com catálogos Quick Deploy.

O próximo passo

Siga as orientações de configuração do Quick Deploy em Primeiros passos.

Depois de configurar sua implantação usando o Quick Deploy, você pode continuar usando essa interface para as seguintes tarefas de gerenciamento.

- Gerencie o catálogo. O gerenciamento de catálogos inclui adicionar ou excluir máquinas, gerenciar aplicativos e gerenciar agendamentos de gerenciamento de energia.

- Gerenciar imagens. O gerenciamento de imagens inclui preparar ou importar imagens, atualizar catálogos com uma nova imagem, renomear ou excluir imagens e instalar ou atualizar VDAs em uma imagem.
- Adicionar ou remover usuários em um catálogo.
- Gerenciar locais de recursos.

Introdução ao Quick Deploy

May 30, 2023

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.

Criar catálogos usando o Quick Deploy

June 24, 2022

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 de uma imagem preparada ou importada pela Citrix.

Criação rápida	Criação personalizada
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

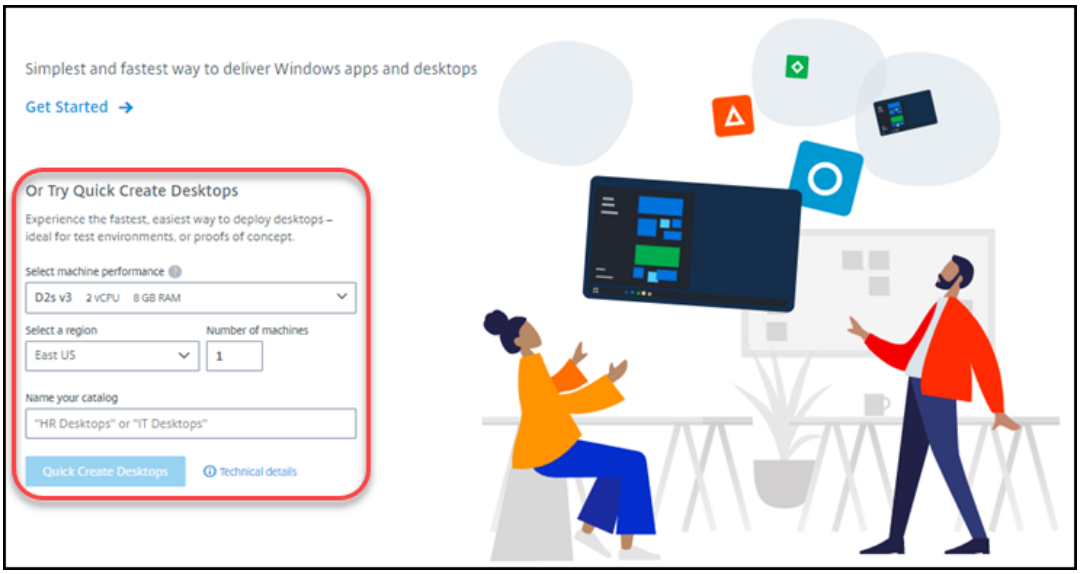
> **Importante:**
>
> Quando você cria um catálogo (ou uma imagem) usando uma assinatura do Citrix Managed Azure pela primeira vez, você é solicitado a reconhecer e consentir com sua responsabilidade pelos valores cobrados. Os lembretes desse consentimento também podem aparecer ao criar mais catálogos 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.

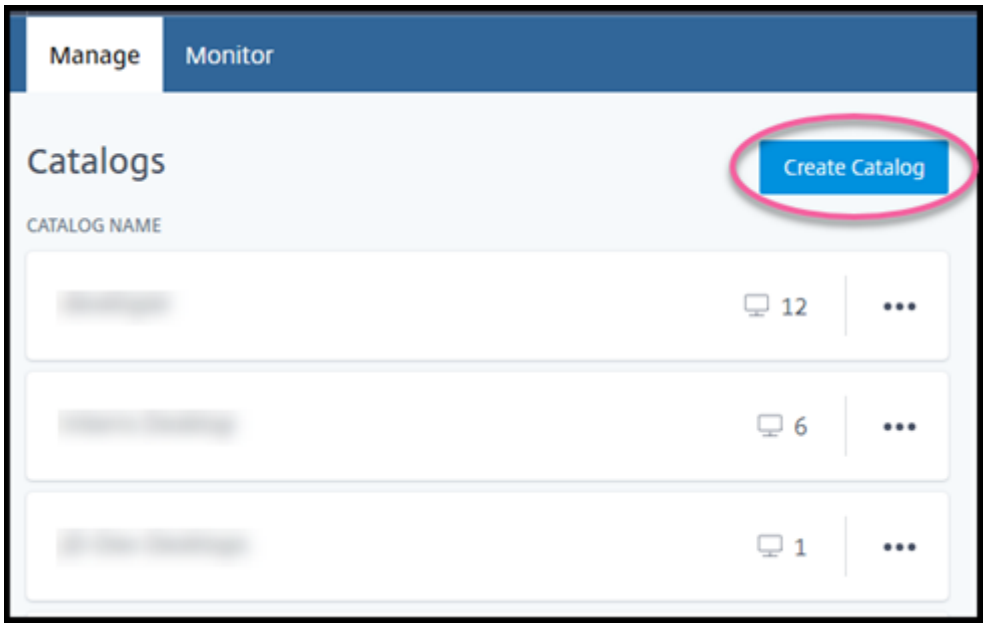
1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Selecione **Manage > Quick Deploy**.
4. Se ainda não tiver sido criado nenhum catálogo, você será direcionado para a página de **boas-vindas**. Escolha uma das seguintes opções:

- Configure o catálogo nesta página. Continue com as etapas de 6 a 10.

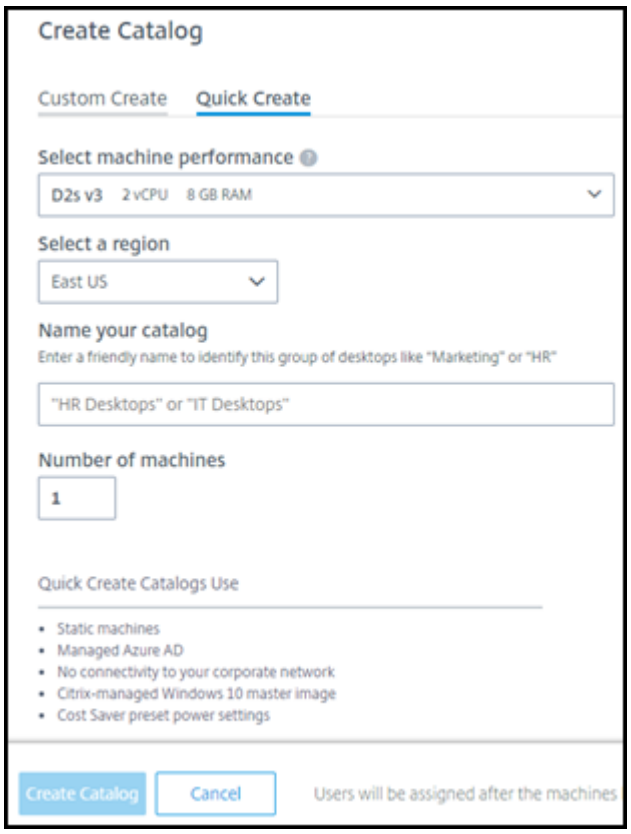


- Selecione **Get Started**. Você será direcionado para o painel **Manage > Quick Deploy**. Selecione **Create Catalog**.

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

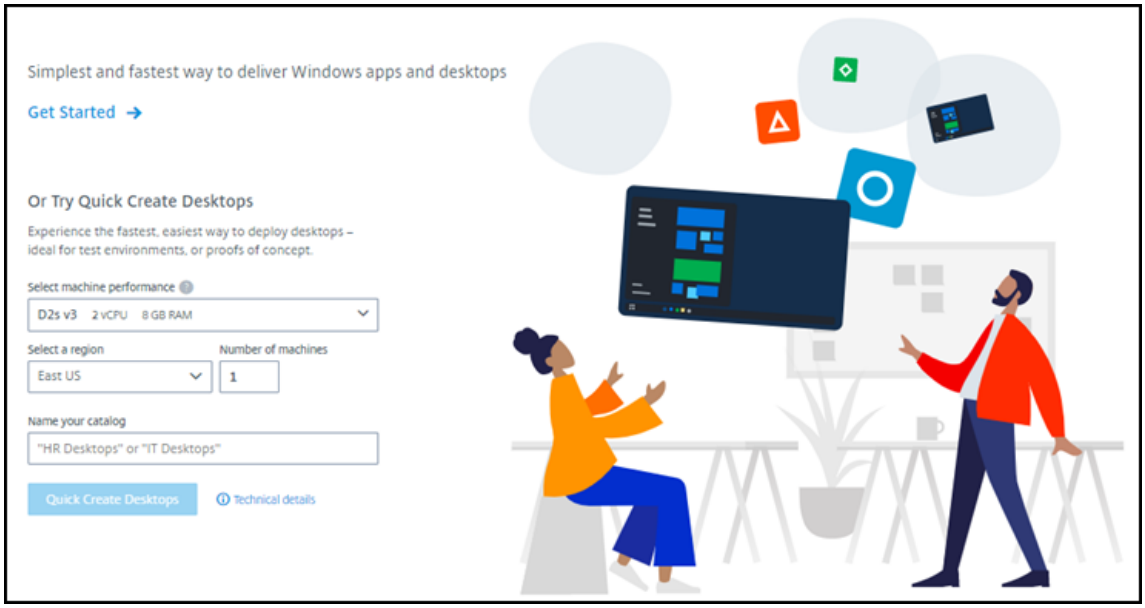
Se você estiver usando uma assinatura do Citrix Managed Azure e planeja usar uma conexão com seus recursos de rede local, crie essa conexão de rede antes de criar o catálogo. Para permitir que seus usuários acessem seus recursos locais ou outros recursos de rede, você também precisa de informações do Active Directory para esse local.

Se você não tiver uma assinatura do Citrix Managed Azure, será possível:

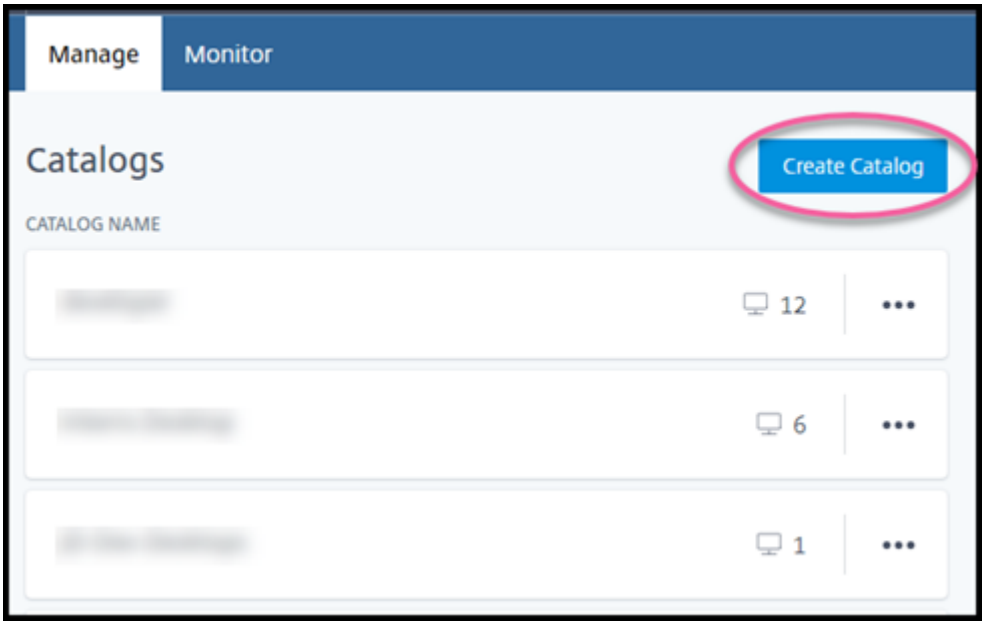
- Solicite o Azure Consumption Fund no Azure Marketplace, que fornece uma assinatura do Citrix Managed Azure.
- Importe (adicione) uma ou mais de suas próprias assinaturas do Azure para o Citrix DaaS antes de criar um catálogo.

Para criar um catálogo:

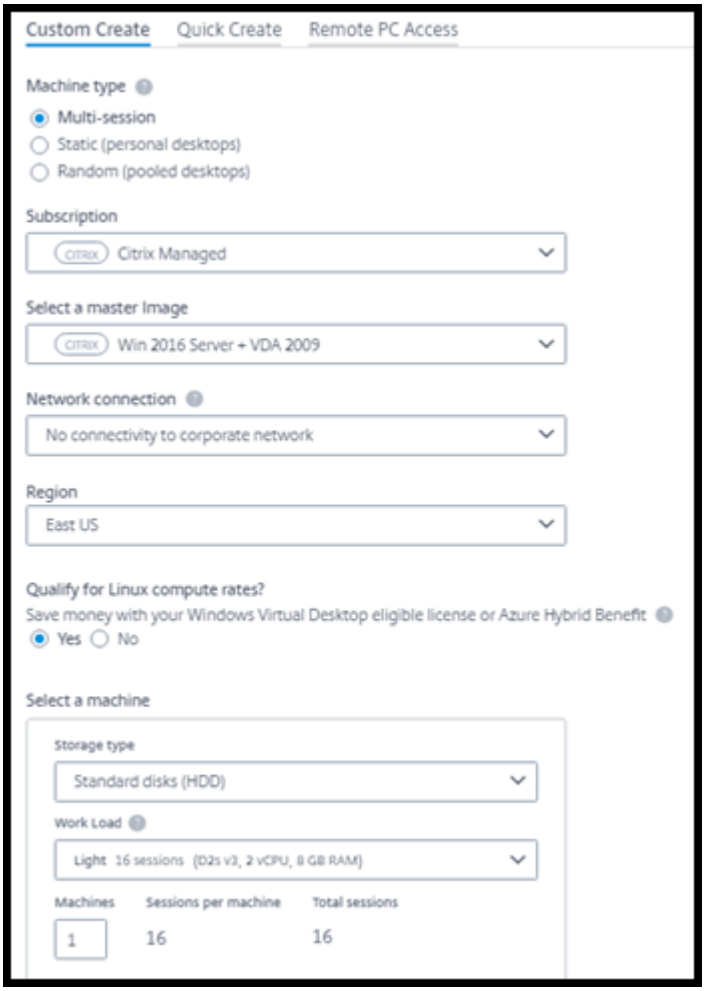
1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Selecione **Manage > Quick Deploy**.
4. Se ainda não tiver sido criado nenhum catálogo, você será direcionado para a página de **boas-vindas**. Selecione **Get Started**. No final da página de introdução, 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

July 1, 2022

Este artigo descreve as tarefas de gerenciamento de catálogo que você pode usar para gerenciar catálogos que foram criados no Quick Deploy.

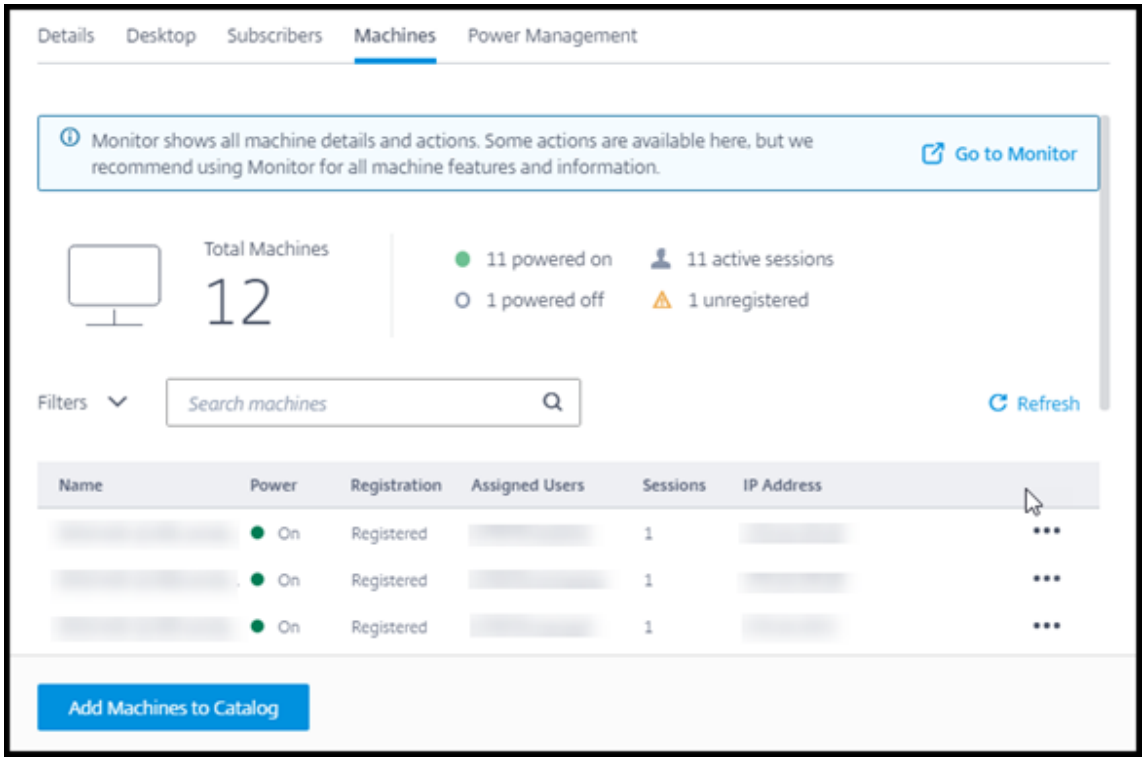
Lembre-se: se você tiver usado o Quick Deploy para criar um catálogo e, em seguida, usar a interface Full Configuration para executar tarefas de gerenciamento nesse catálogo, não será mais possível usar a interface Quick Deploy para esse catálogo.

(Para obter informações sobre o gerenciamento de catálogos na interface de gerenciamento de Full Configuration, consulte Manage machine catalogs.)

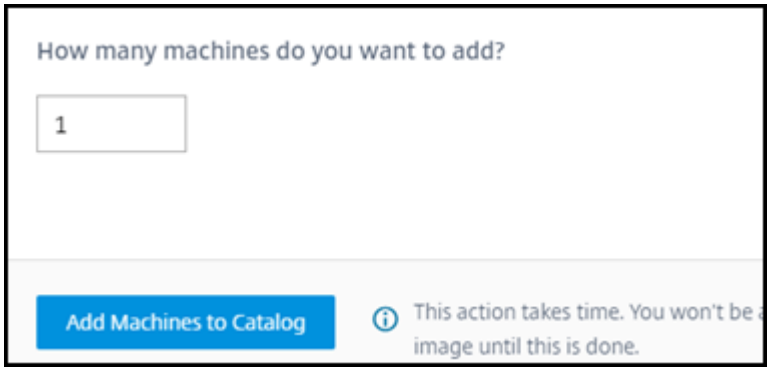
Adicionar máquinas a um catálogo

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.

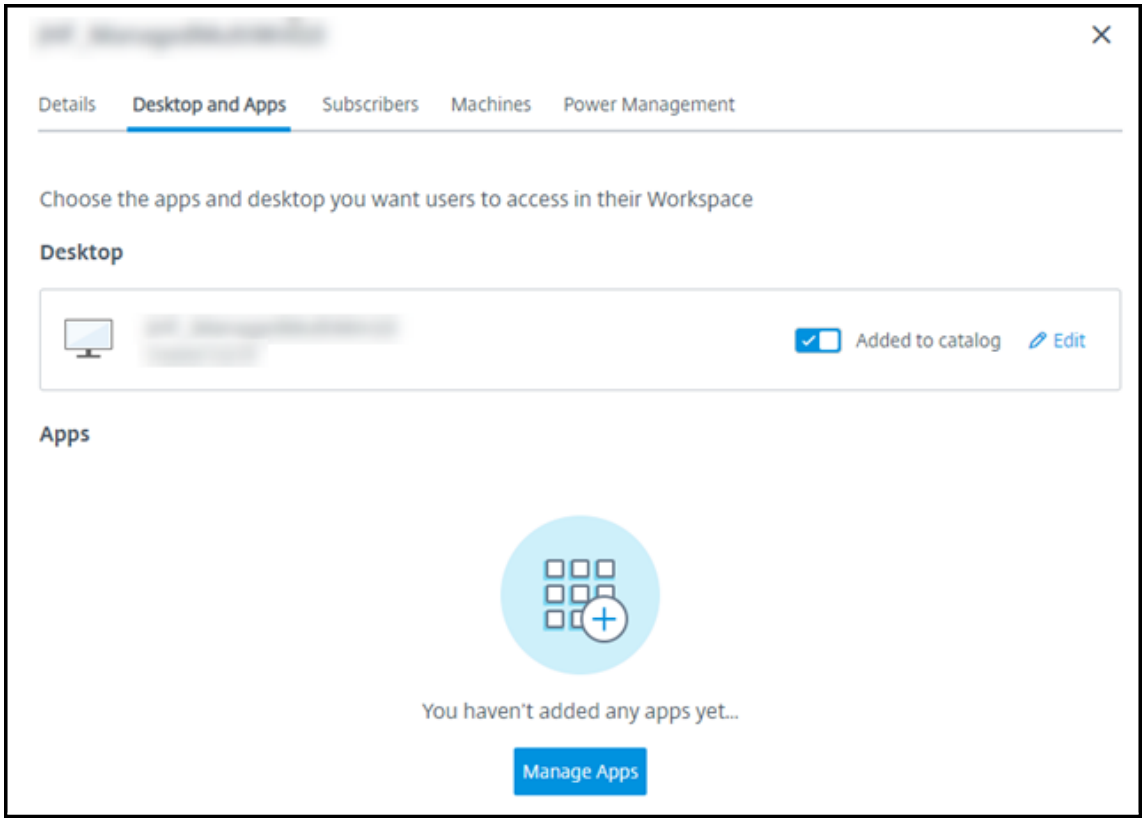
- **Delete:** exclui a máquina selecionada. Essa ação está disponível somente quando a contagem de sessões da máquina é zero. Confirme a exclusão.

  Quando uma máquina é excluída, todos os dados nela contidos são removidos.

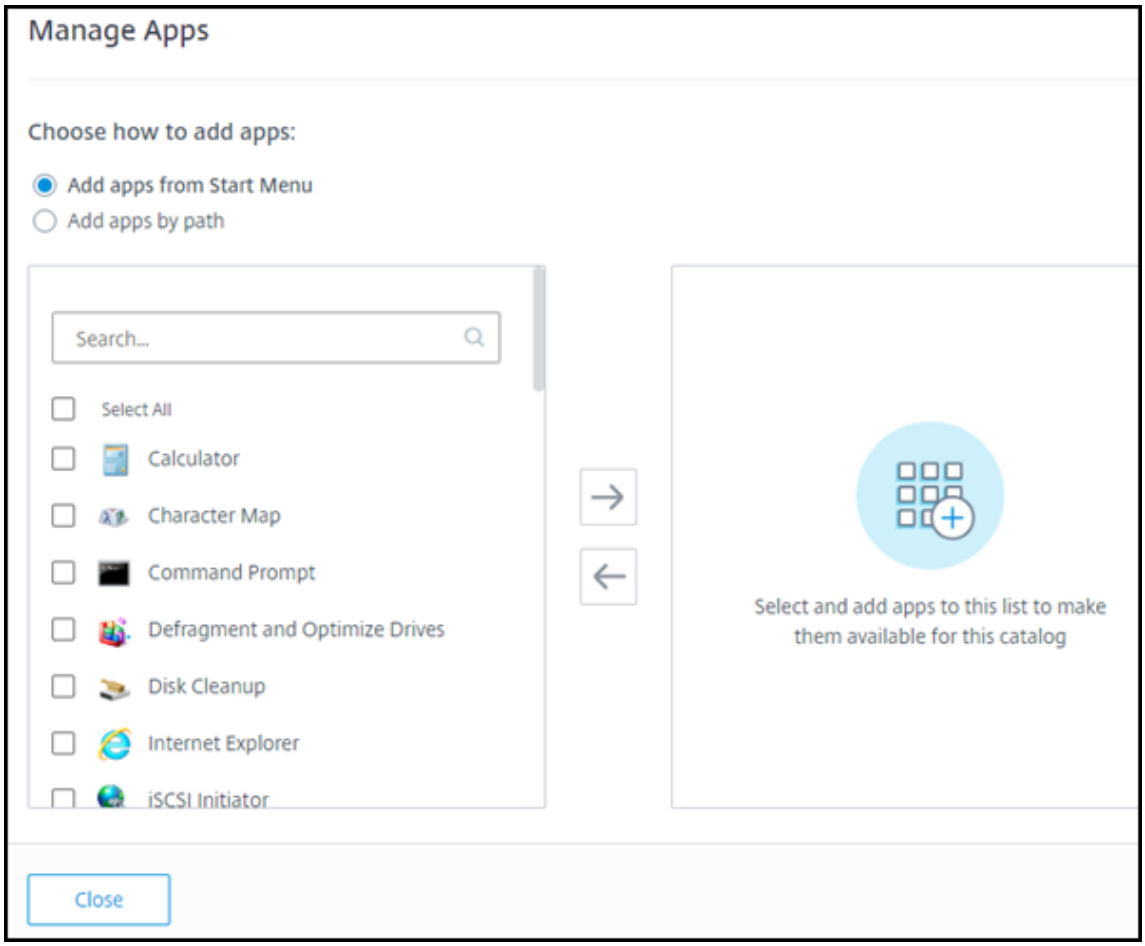
- **Force restart:** força a reinicialização da máquina selecionada. Selecione essa ação somente se uma ação **Restart** não surtir efeito na máquina.

Adicionar aplicativos a um catálogo

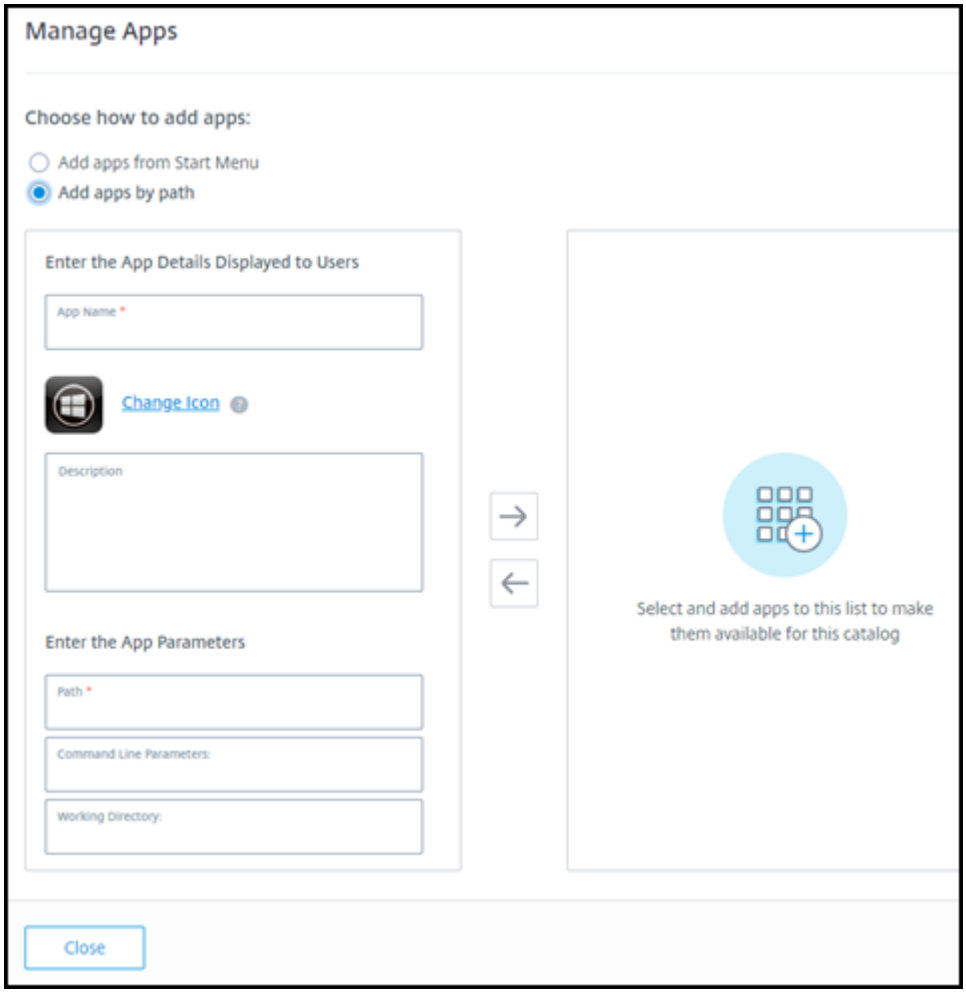
1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, selecione **Manage Apps**.



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:



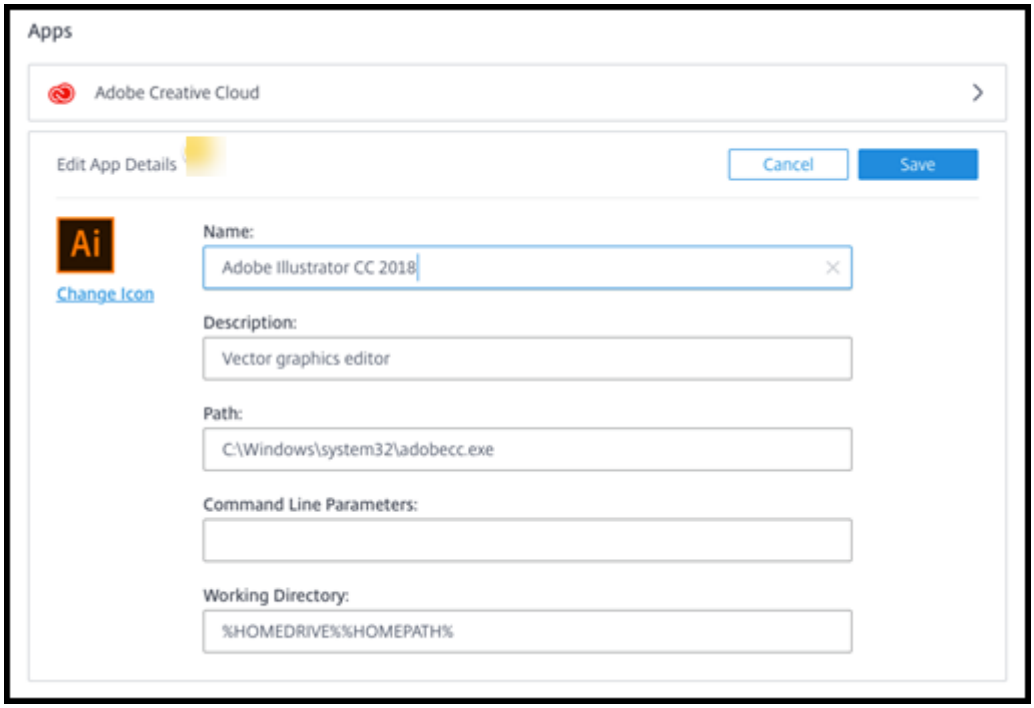
- Insira o nome do aplicativo. Esse é o nome que os usuários veem no Citrix Workspace.
- O ícone mostrado é o ícone que os usuários veem no Citrix Workspace. Para selecionar outro ícone, selecione **Change icon** e navegue até o ícone que deseja exibir.
- (Opcional) Insira uma descrição do aplicativo.
- 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

Assinaturas do Azure no Quick Deploy

August 17, 2023

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**.

Imagens no Quick Deploy

June 24, 2022

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:

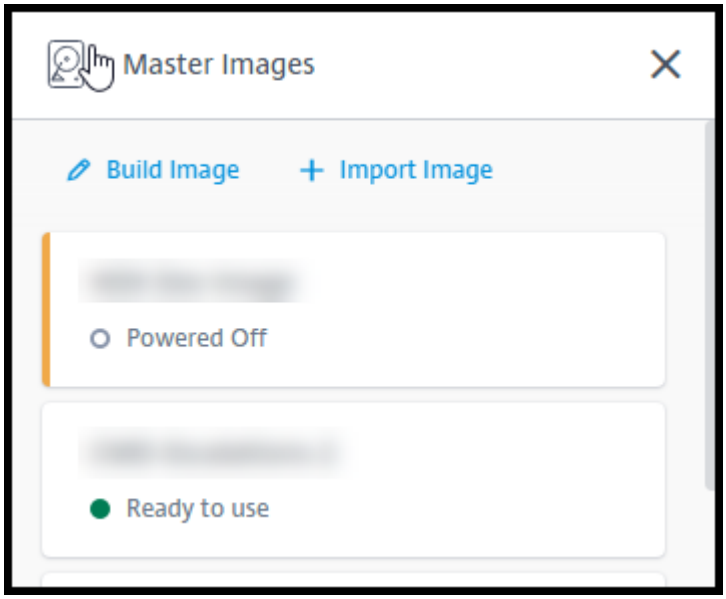
- **Use a Citrix prepared image when creating a catalog.** Essa opção é recomendada somente para implantações de prova de conceito.
- **Use a Citrix prepared image to create another image.** Depois que a nova imagem é criada, você a personaliza adicionando aplicativos e outros softwares de que seus usuários 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.

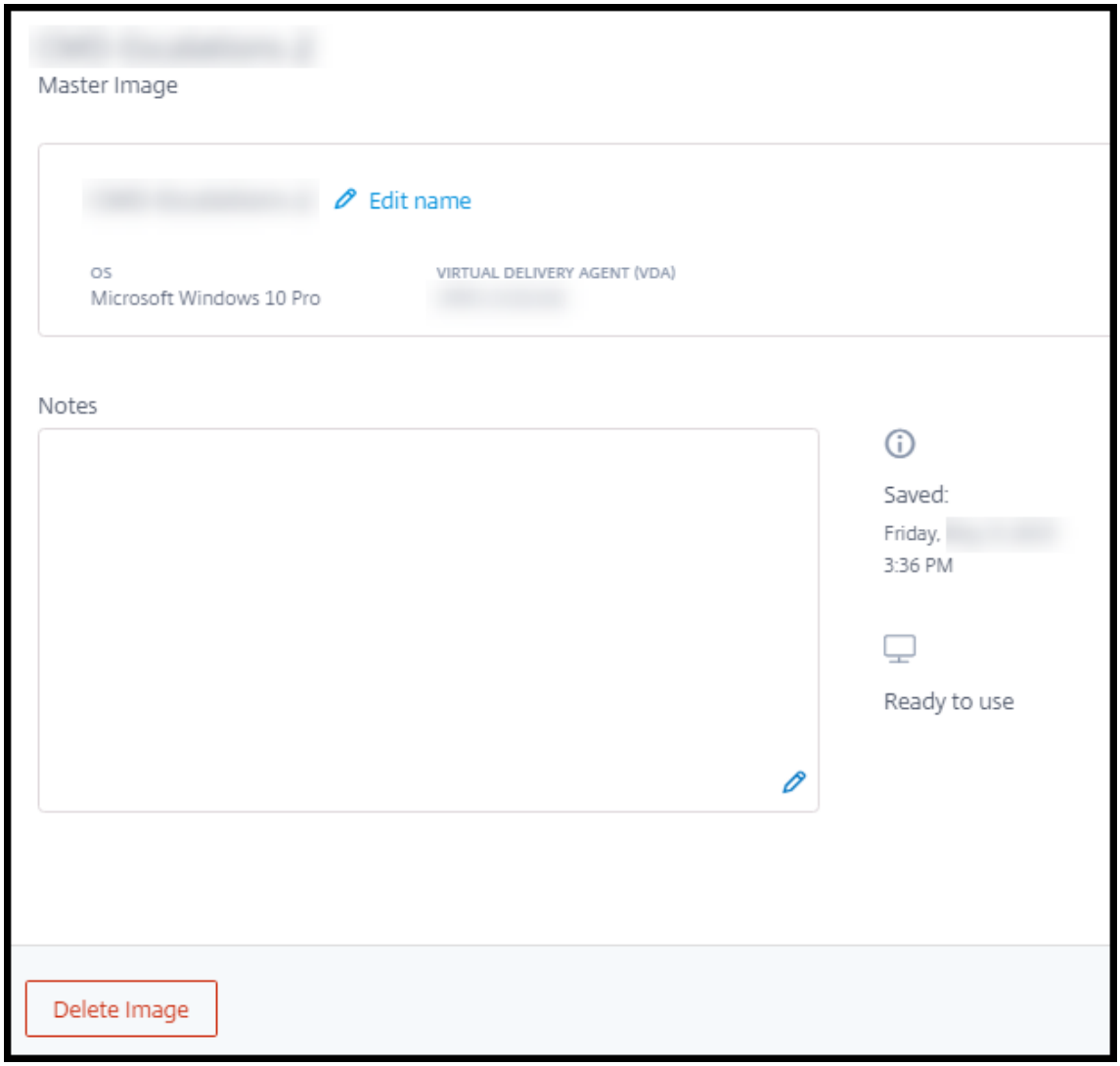
Quando você cria um catálogo, o Citrix DaaS verifica se a imagem usa um sistema operacional válido e tem um Citrix VDA e ferramentas de solução de problemas instaladas (junto com outras verificações).

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 exe-

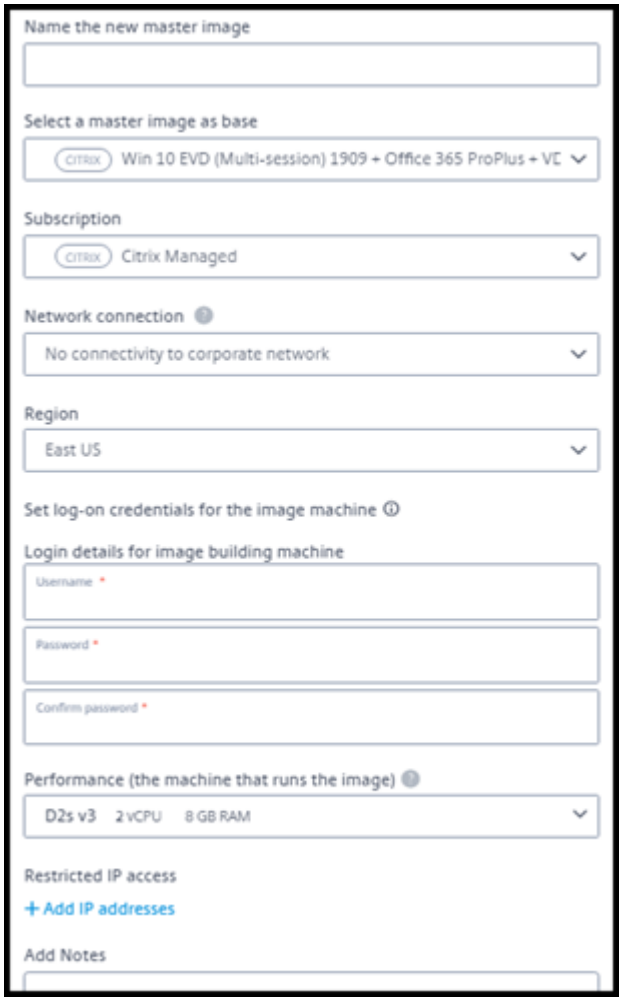
cução de aplicativos CAD pode exigir CPU, RAM e armazenamento diferentes dos outros aplicativos de escritório.
- Se você planeja usar uma conexão com seus recursos locais, configure essa conexão antes de criar a imagem e o catálogo. Para obter detalhes, consulte Network connections.

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.

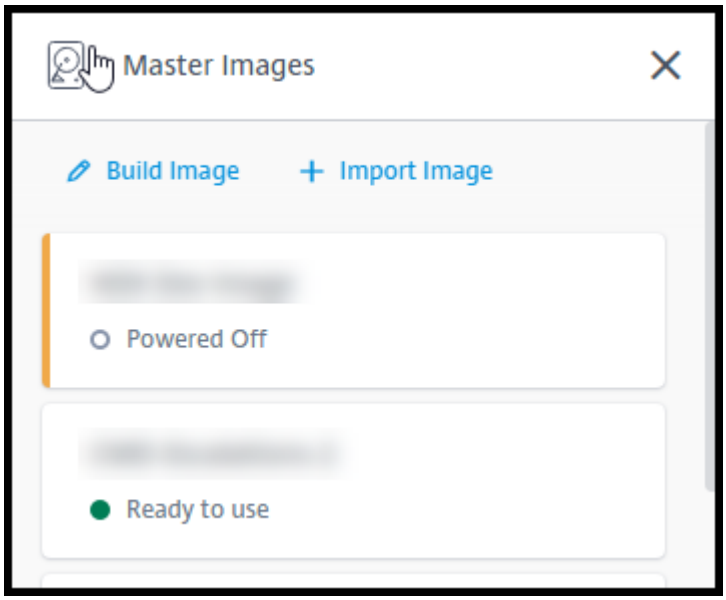
- **Supported OS:** a imagem deve ser um sistema operacional com suporte. Para verificar uma versão do sistema operacional Windows, execute `Get-WmiObject Win32_OperatingSystem`.
- **Supported generation:** somente VMs de geração 1 têm suporte.
- **Not generalized:** a imagem não deve ser generalizada.
- **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`

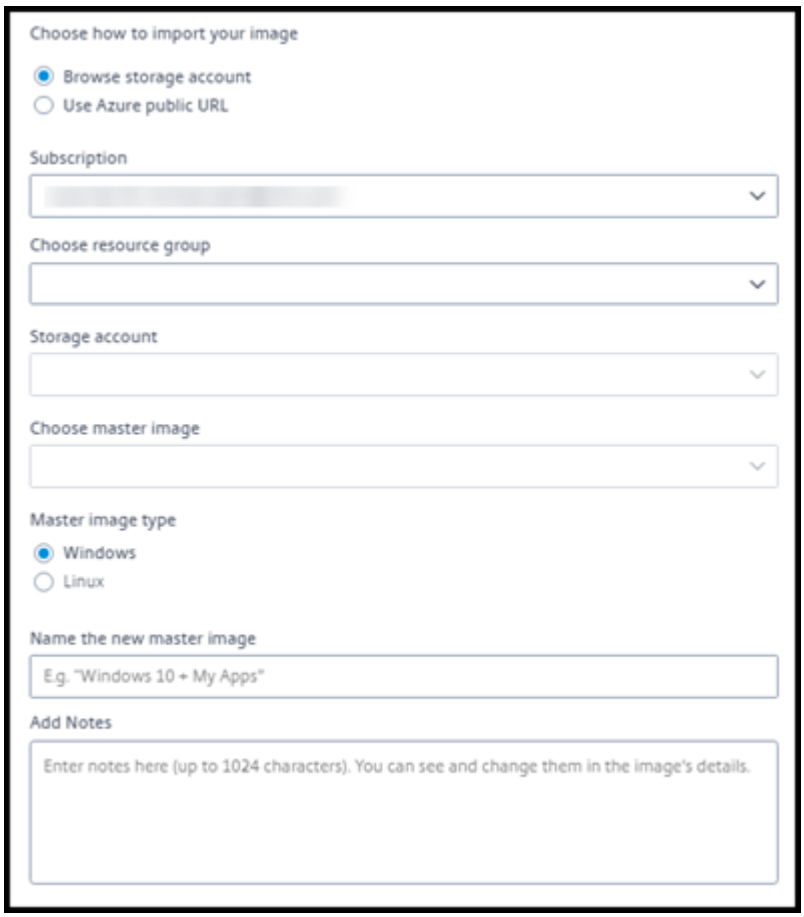
- **Personality.ini file:** o arquivo `personality.ini` deve existir na unidade do sistema.
- **Valid VDA:** a imagem deve ter um Citrix VDA mais recente que 7.11 instalado.
  - Windows: Para verificar, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. 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

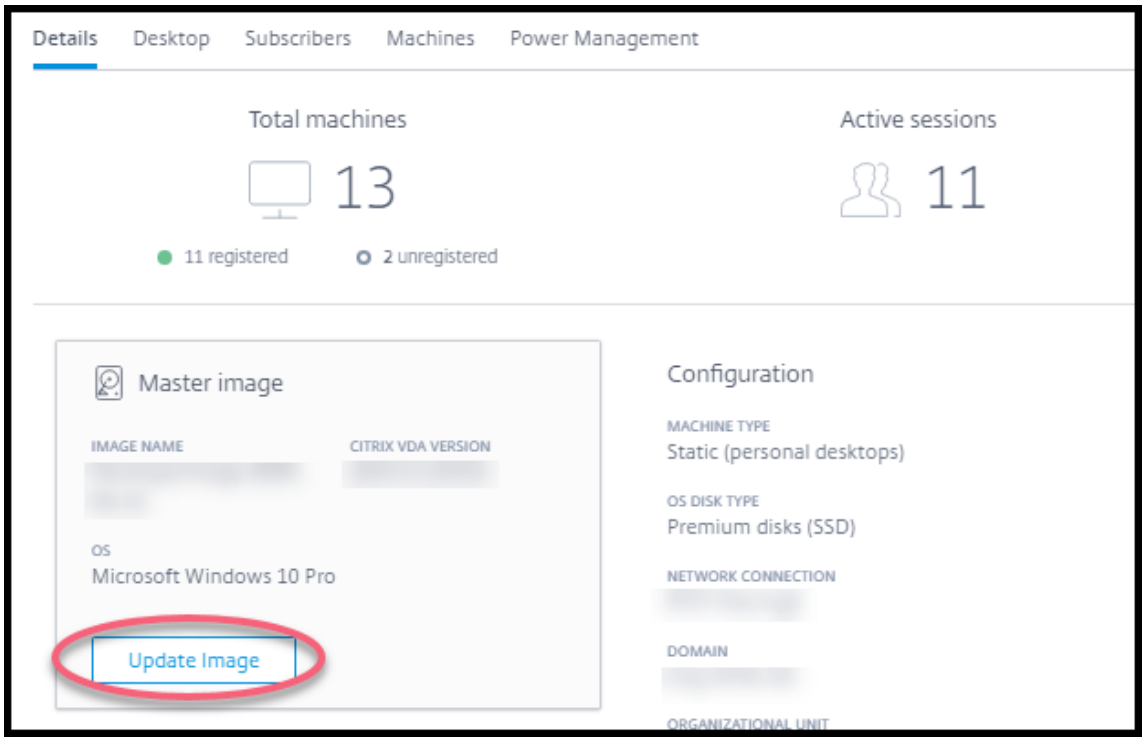
O tipo de catálogo determina quais máquinas são atualizadas quando você atualiza o catálogo.

- 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.

Conexões de rede no Quick Deploy

June 24, 2022

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

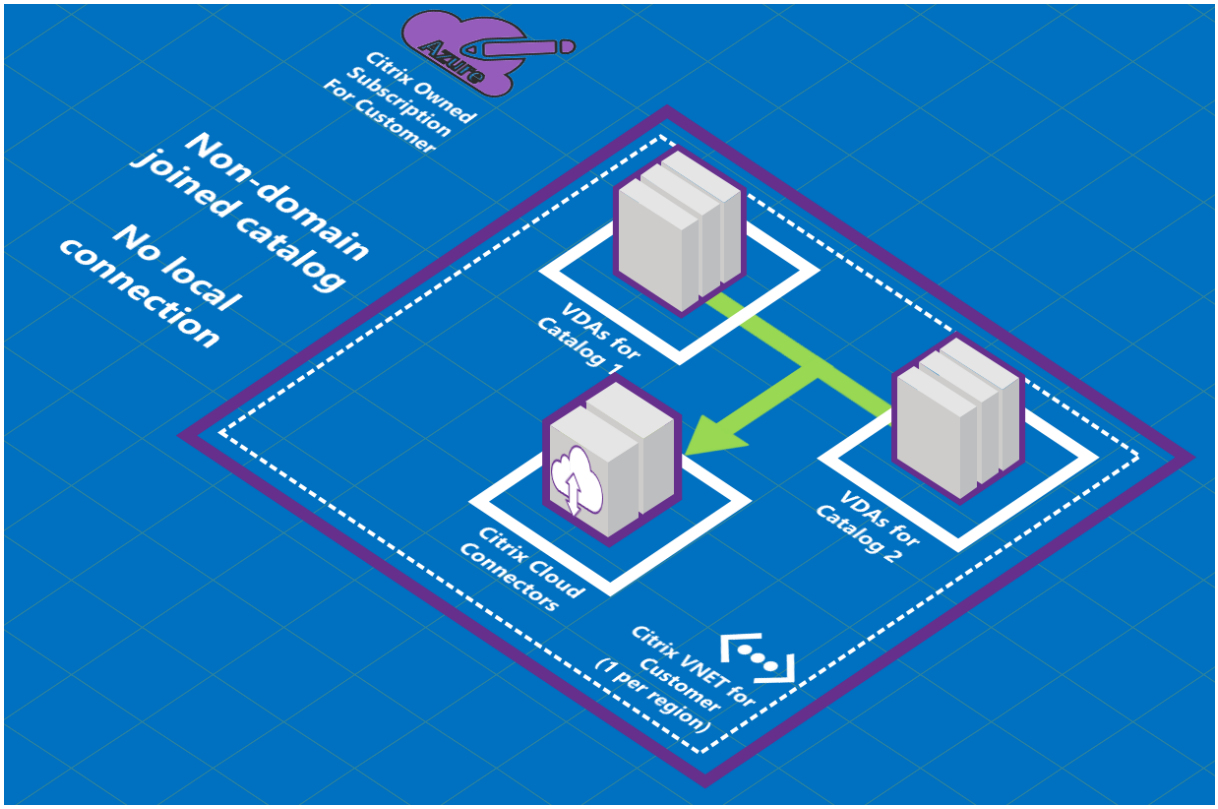
Não é possível alterar o tipo de conexão de um catálogo após a criação desse catálogo.

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

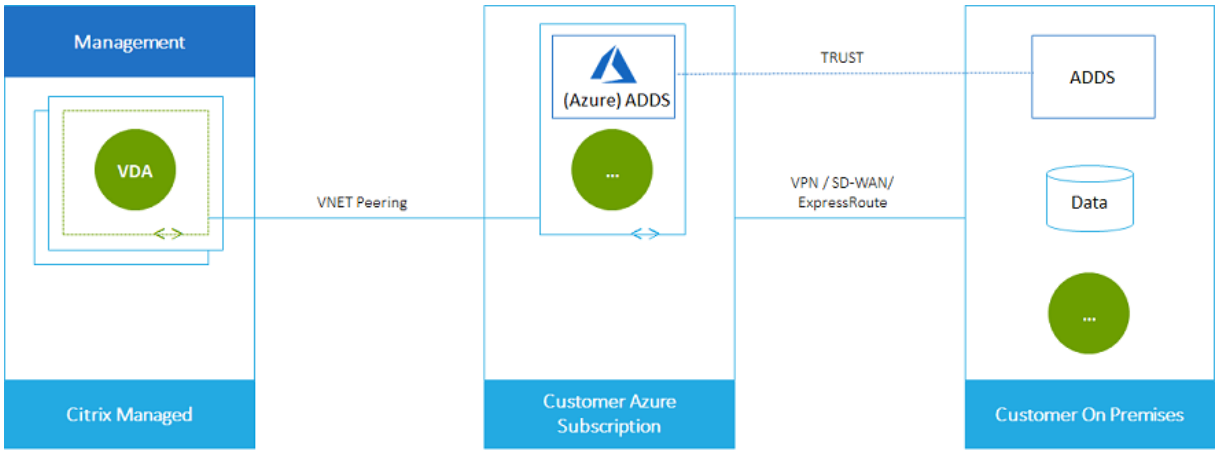
Quando um catálogo é configurado com **Sem conectividade**, os usuários não podem acessar recursos em suas redes locais ou em outras redes. Essa é a única opção ao criar um catálogo usando a criação rápida.



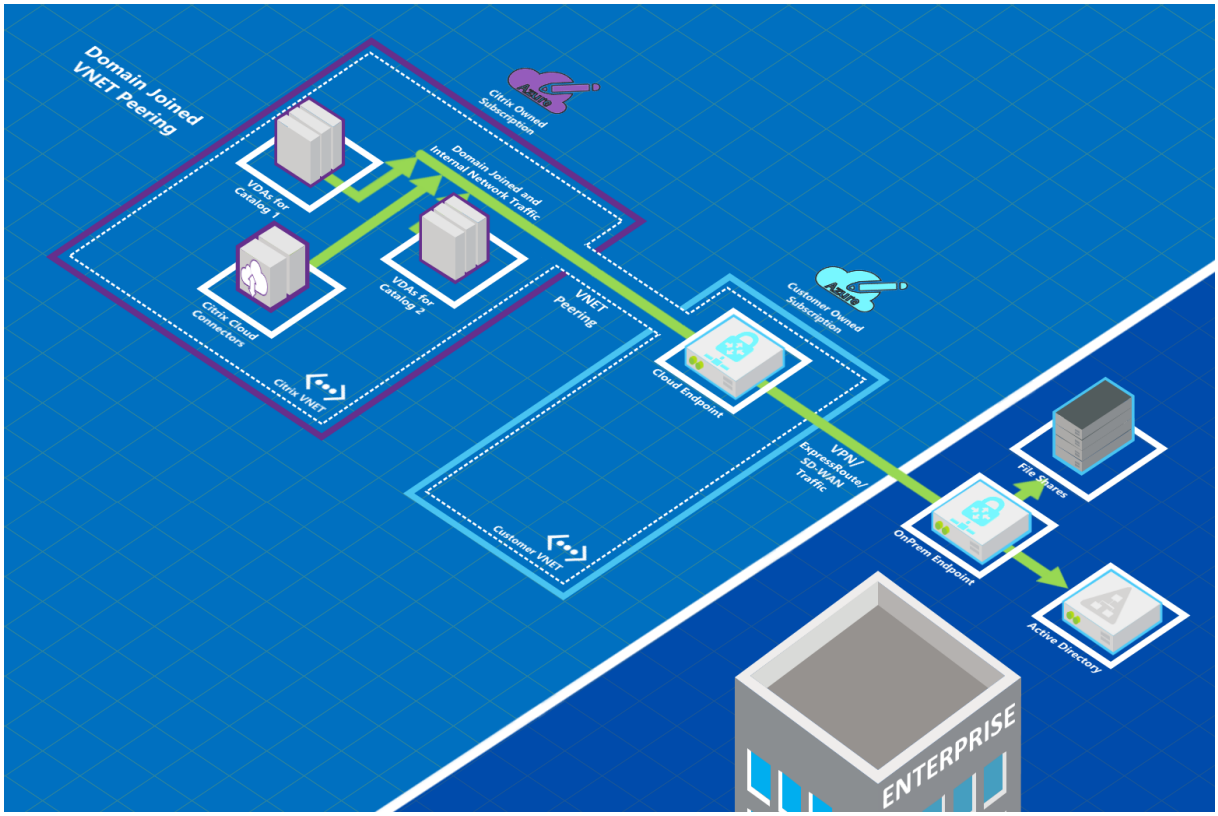
Sobre as conexões emparelhadas do Azure VNet

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.

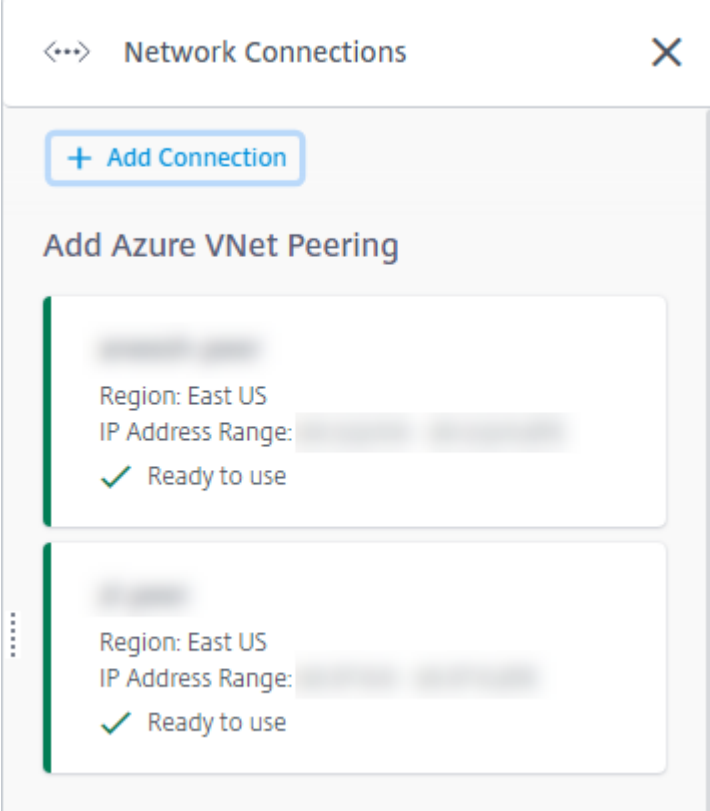
Para saber mais sobre o emparelhamento de VNet, consulte os seguintes artigos da Microsoft.

- Virtual network peering
- Azure VPN Gateway

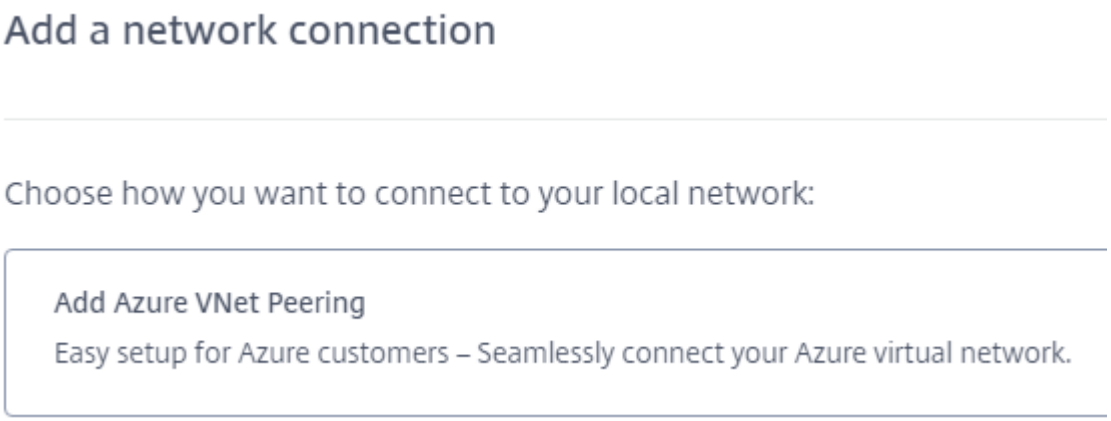
- Create a Site-to-Site connection in the Azure portal
- VPN Gateway FAQ (procure por “overlap”)

Criar uma conexão emparelhada do Azure VNet

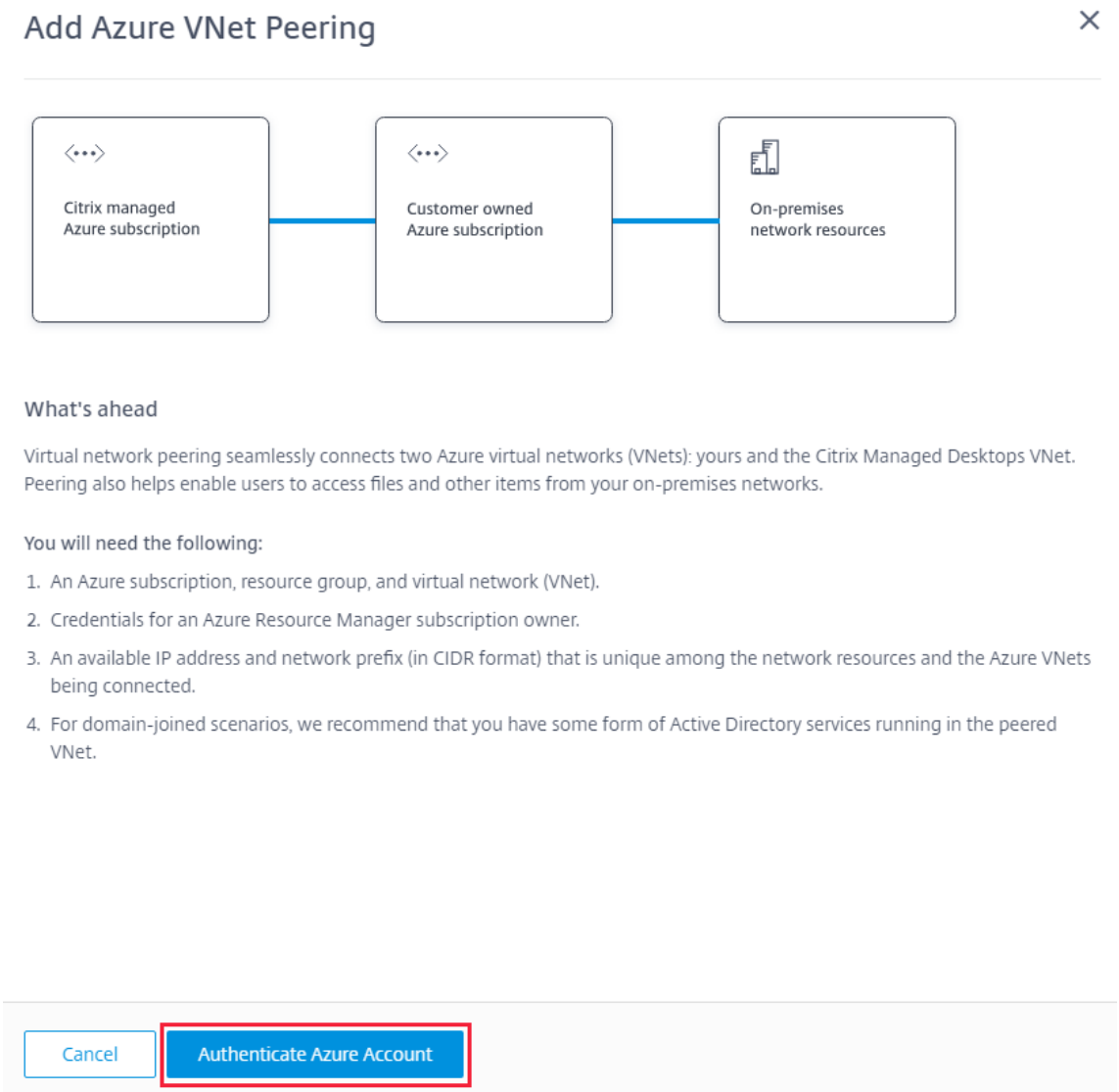
1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita. Se você já tiver configurado conexões, elas estão listadas.



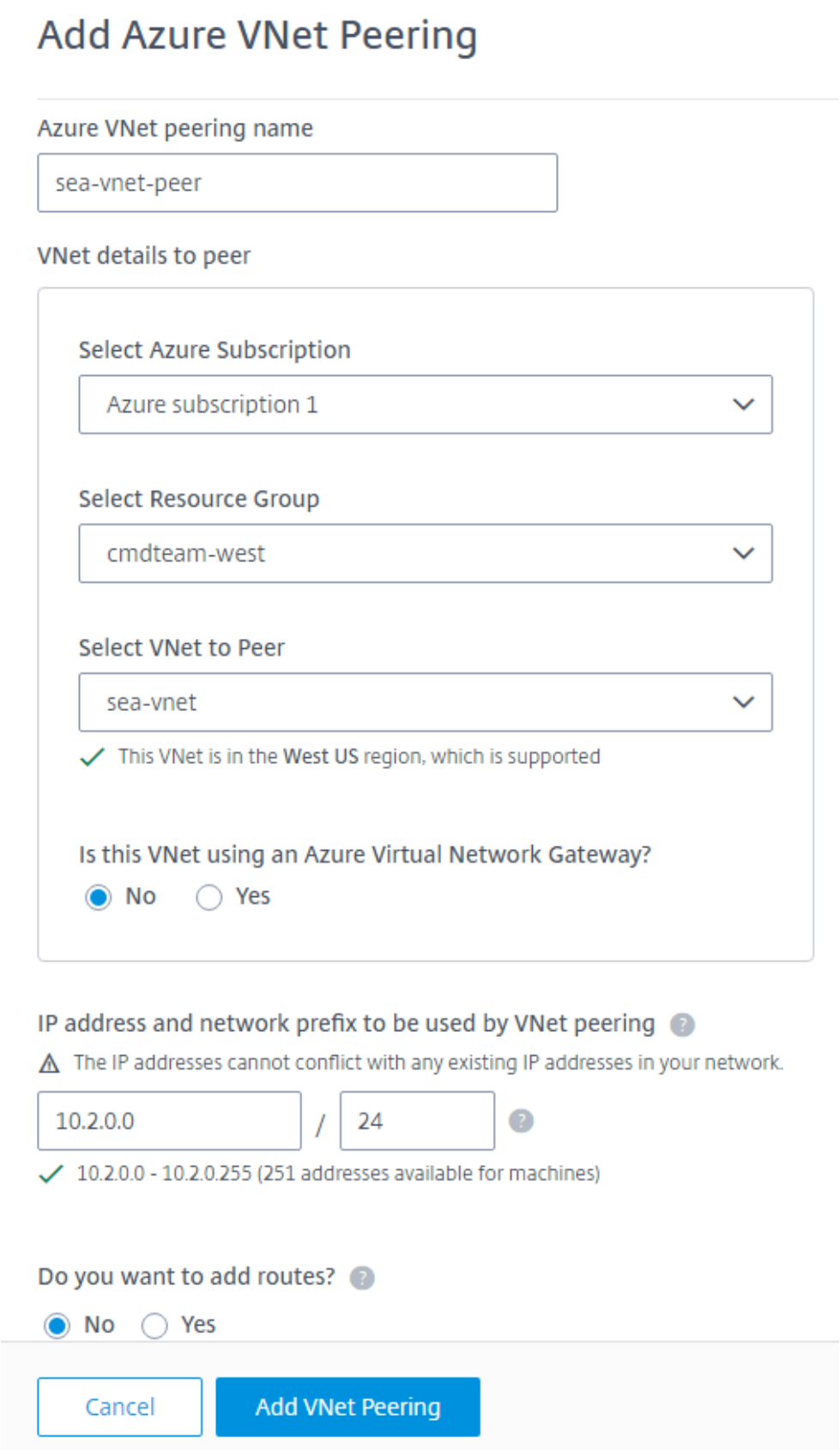
2. Selecione **Add Connection**.
3. Clique em qualquer lugar na caixa **Add Azure VNet Peering** .



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.

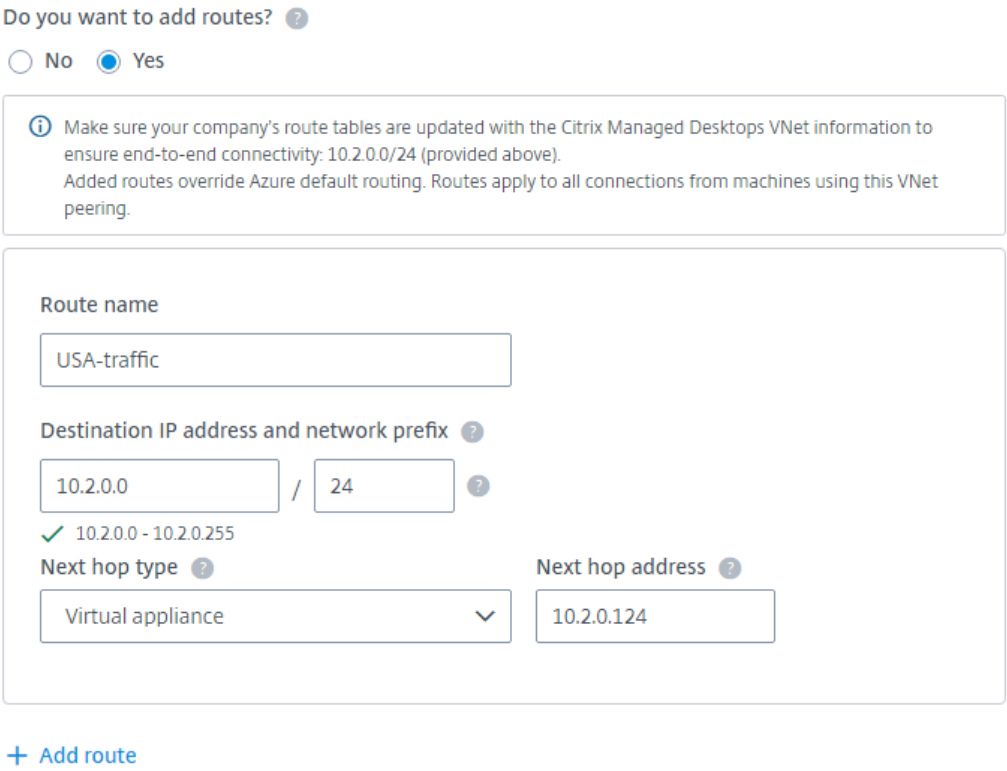
    - Por exemplo, se sua VNet do Azure tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão de emparelhamento VNet no Citrix DaaS como algo como 192.168.0.0 /24.
    - Neste exemplo, a criação de uma conexão de emparelhamento VNet com um intervalo de IP 10.0.0.0 /24 é considerada um intervalo de 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.



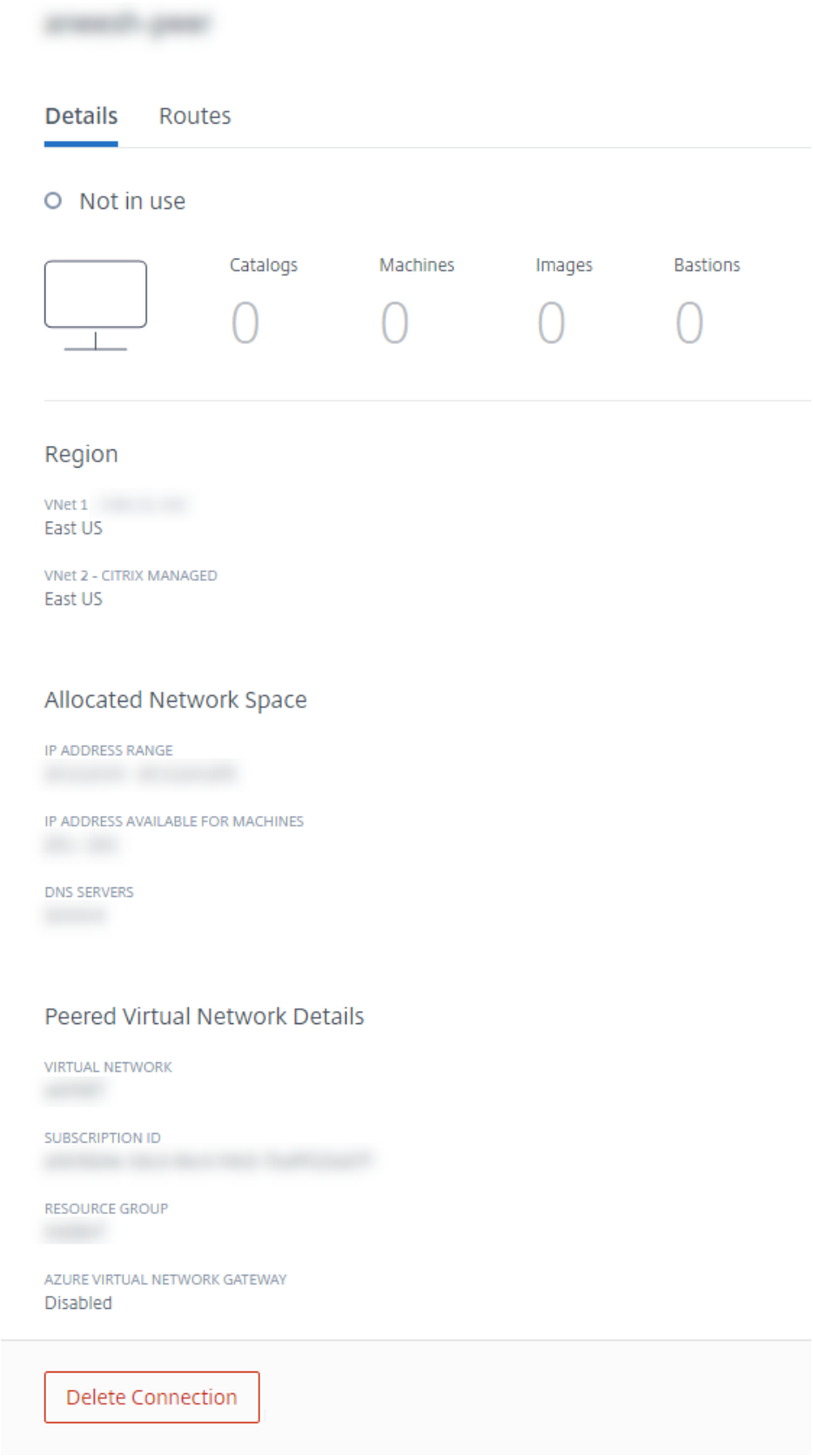
Para obter mais informações sobre os tipos de salto seguinte, consulte a seção Custom routes no artigo da Microsoft *Virtual network traffic routing*.

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.

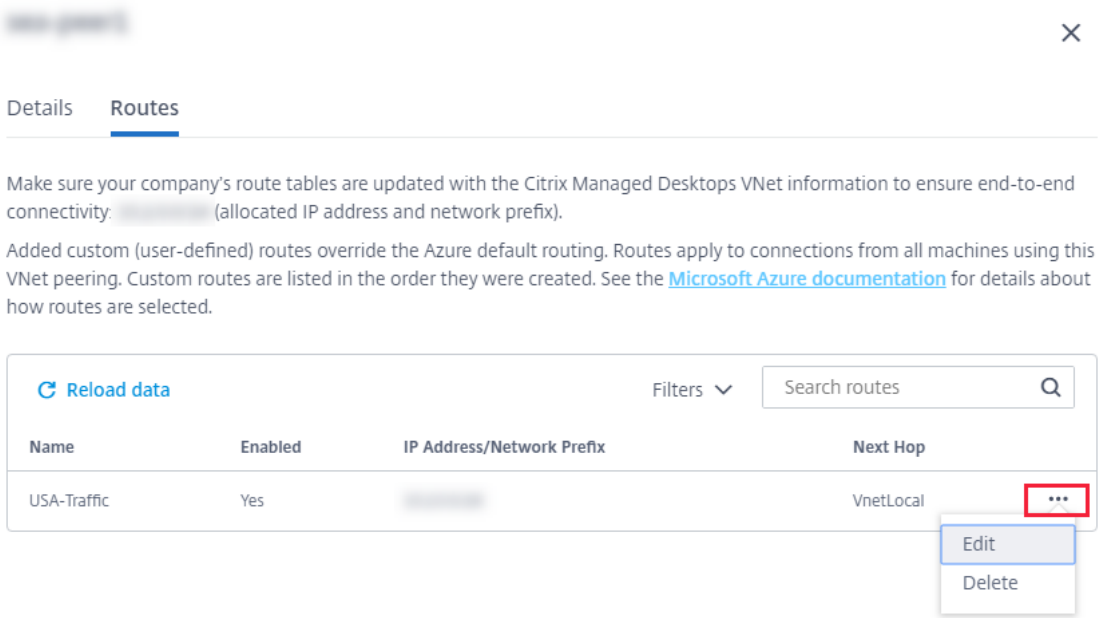
> **Importante:**
>
> A modificação, desativação ou exclusão de rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper qualquer sessão de usuário que possa estar ativa.

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.

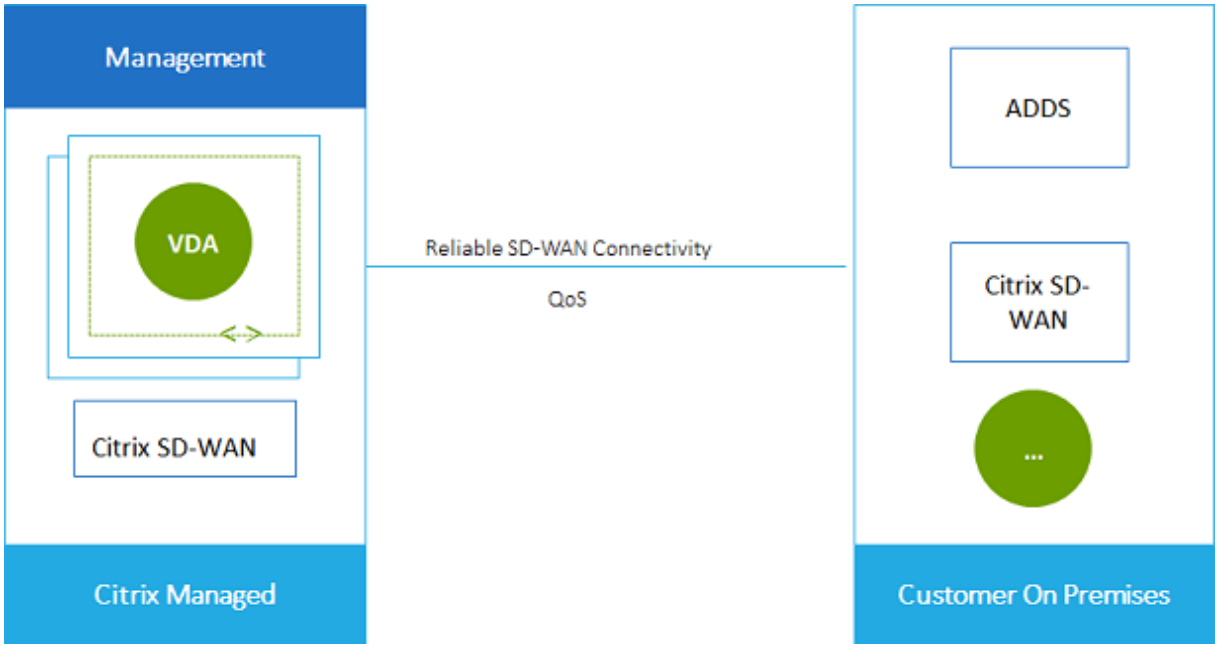
1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, selecione **Delete Connection**.

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.

Usuários e autenticação no Quick Deploy

November 9, 2023

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

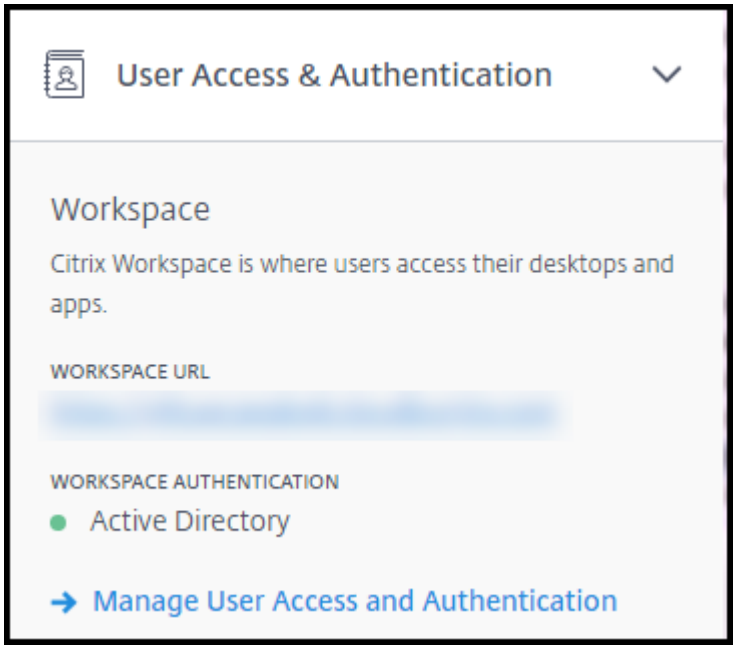
Para configurar a autenticação do usuário no Citrix Cloud:

- 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.

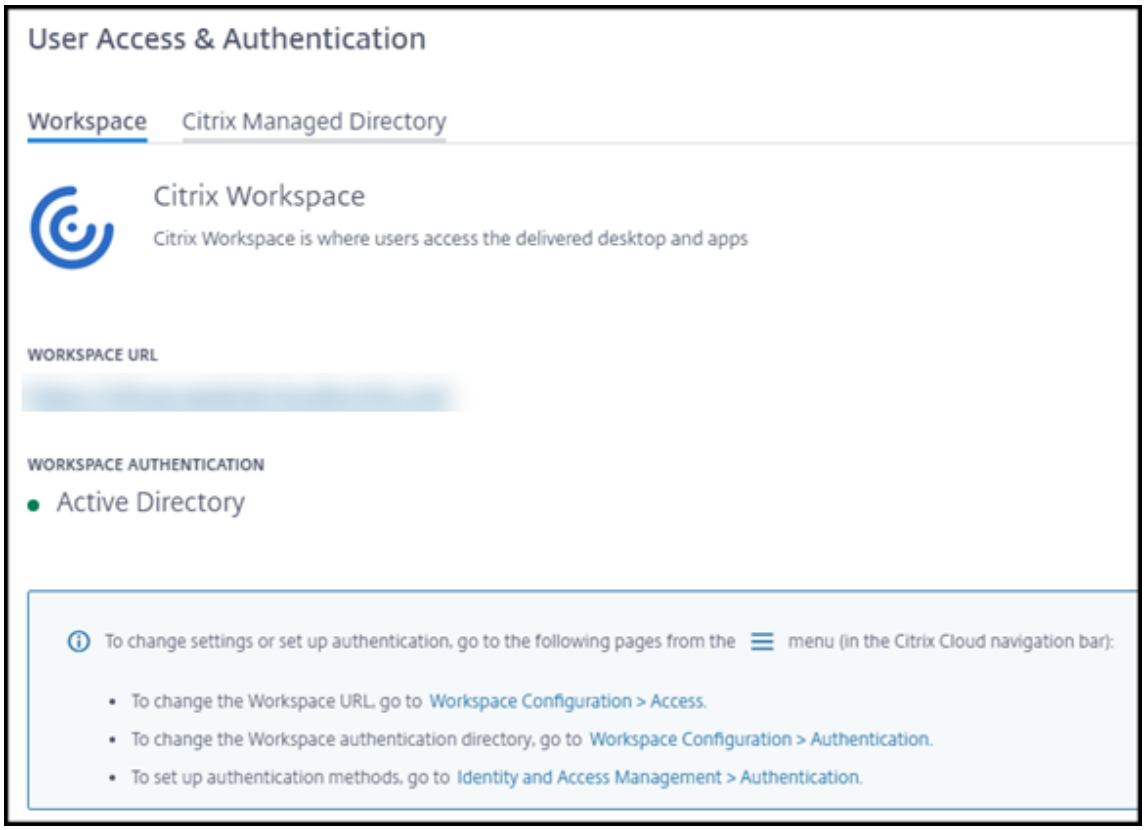
> **Nota:**
>
> O método de autenticação Managed Azure AD é configurado por padrão. Ou seja, ele é conectado automaticamente no Citrix Cloud, e a autenticação do Workspace é definida automaticamente para usar o Managed Azure AD for Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). 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

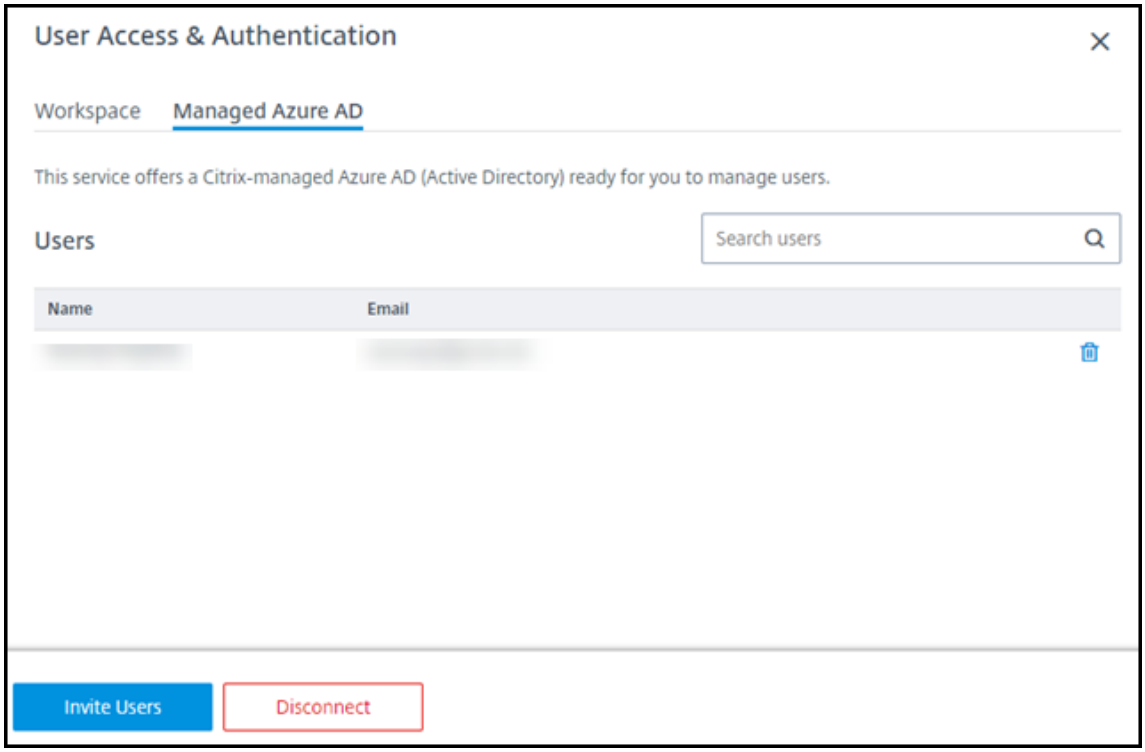
Siga este procedimento somente se estiver usando o Managed Azure AD para autenticação do usuário no Citrix Workspace.

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.

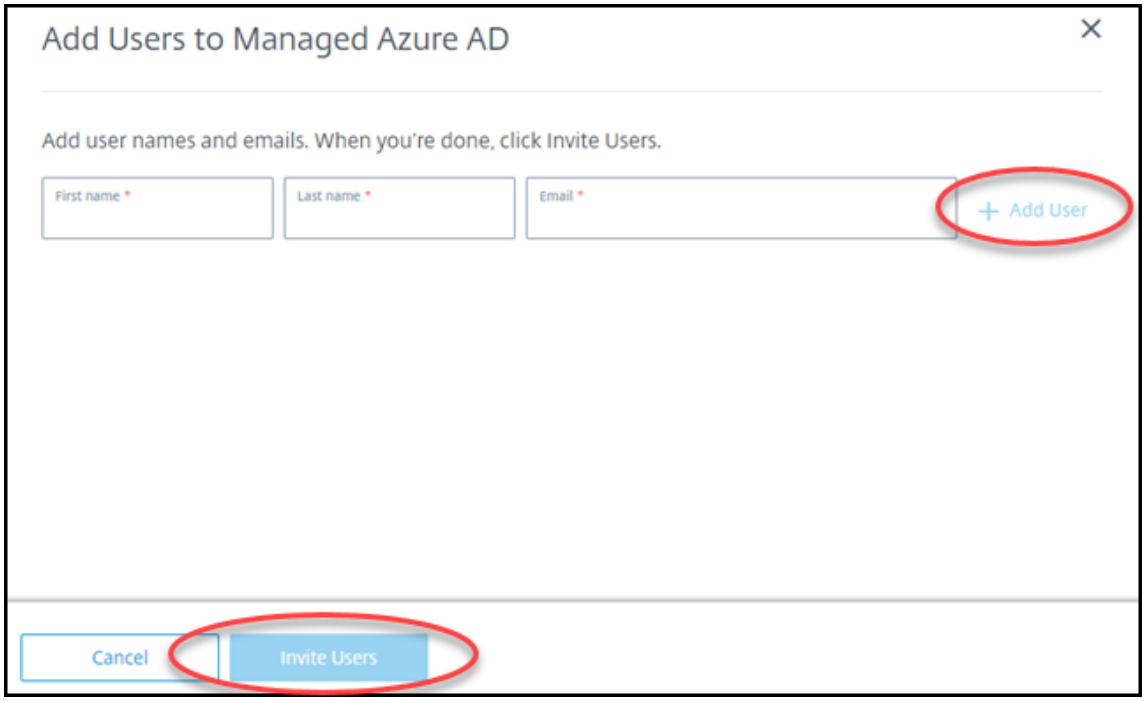
- Se o usuário já tiver uma conta da Microsoft com o endereço de e-mail fornecido, essa conta será usada.
- Se o usuário não tiver uma conta da Microsoft com o endereço de e-mail, a Microsoft criará uma conta.

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.

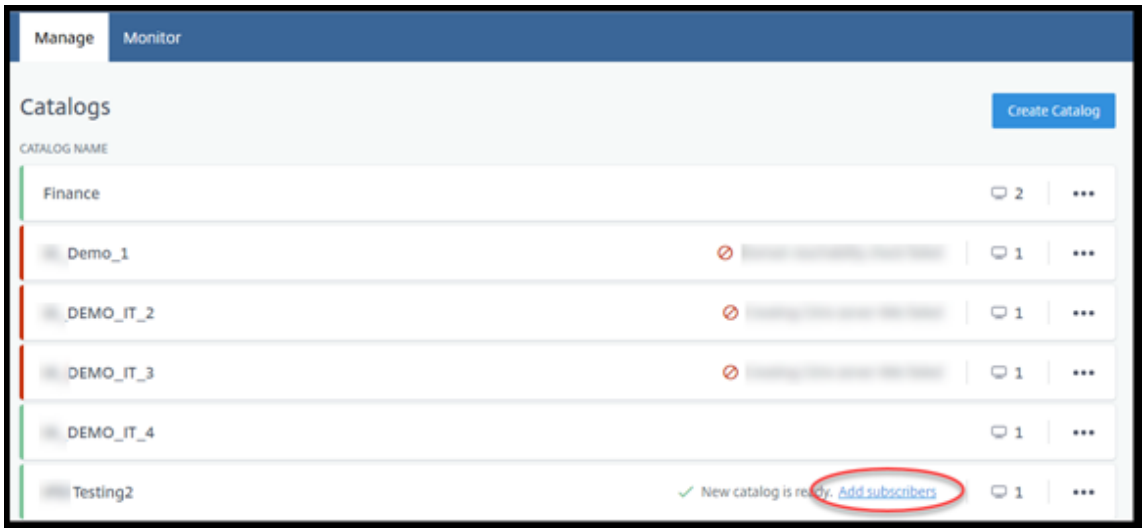
Para excluir um usuário do Managed Azure AD, selecione o ícone de lixeira ao lado do nome do usuário que deseja excluir do diretório. Confirme a exclusão.

O que fazer a seguir: Adicionar usuários ao catálogo

Adicionar ou remover usuários em um catálogo

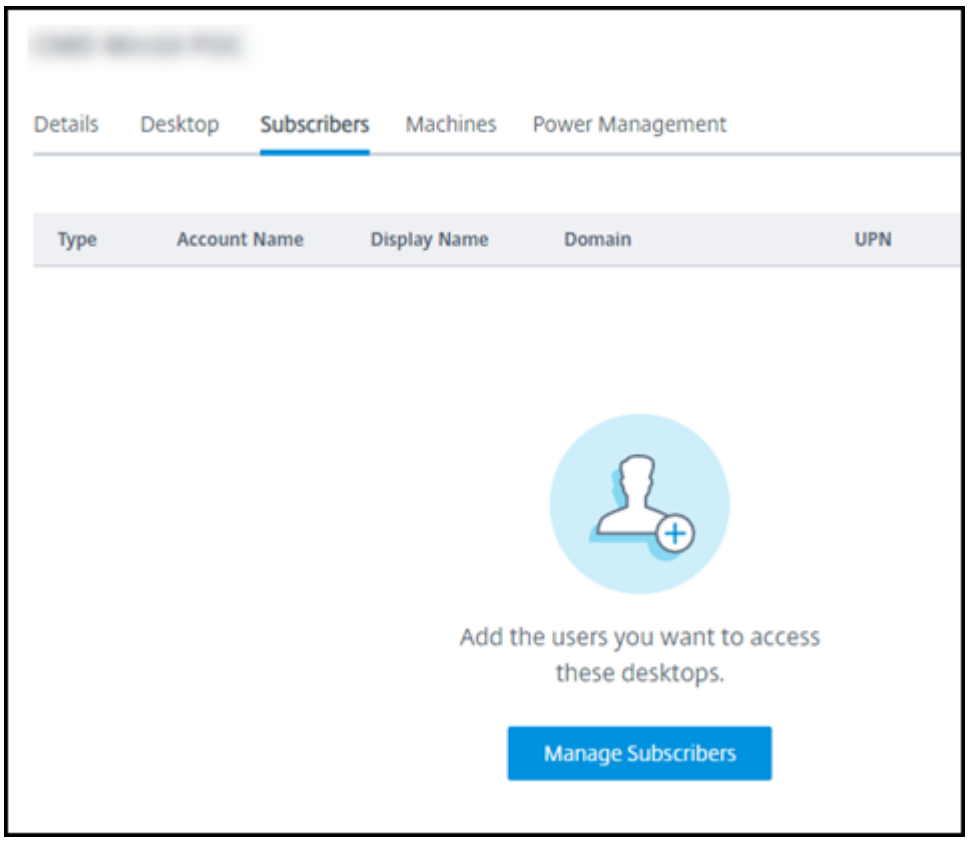
Conclua este procedimento independentemente do método de autenticação usado.

1. Em **Manage > Quick Deploy**, se você não adicionou nenhum usuário a um catálogo, selecione **Add subscribers**.

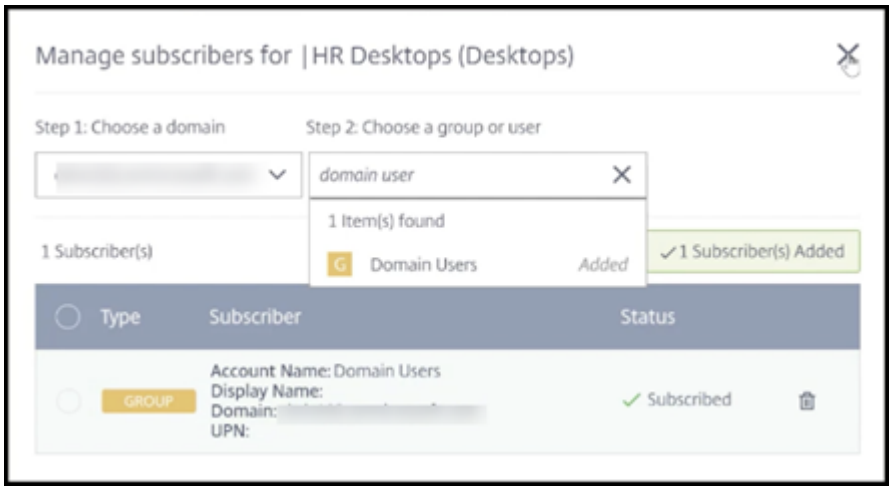


   Para adicionar usuários a um catálogo que já tem usuários, clique em qualquer lugar na entrada do catálogo.

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.

Acesso remoto ao PC no Quick Deploy

February 23, 2023

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:

  1. Usando suas credenciais de conta do Citrix Cloud, navegue até a página de download do Citrix DaaS.
  2. 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.

Monitorar no Quick Deploy

June 24, 2022

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

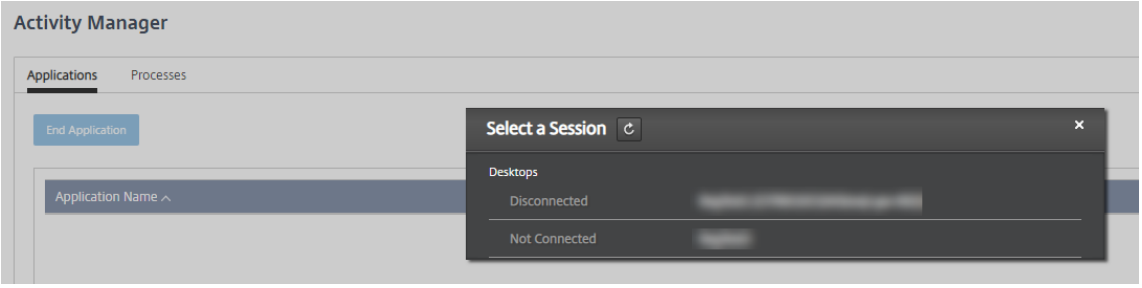
Quando você está monitorando as informações da sessão e da máquina, todas as máquinas ou sessões são exibidas por padrão. Você pode:

- 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

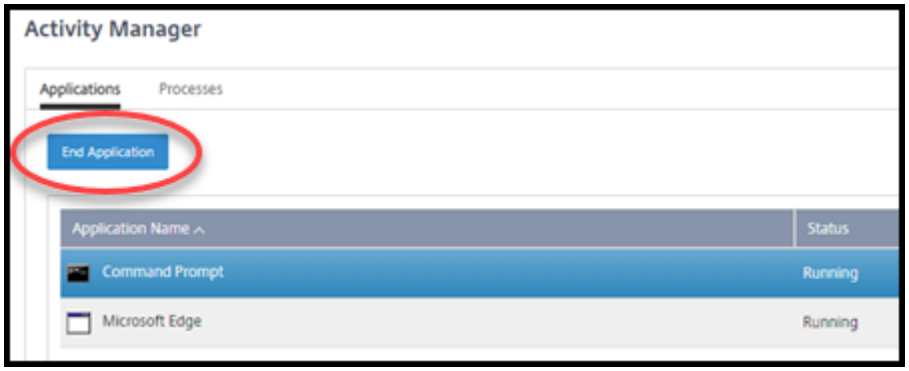
Você pode exibir e gerenciar aplicativos e processos para um usuário que tenha uma sessão em execução ou uma área de trabalho atribuída.

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

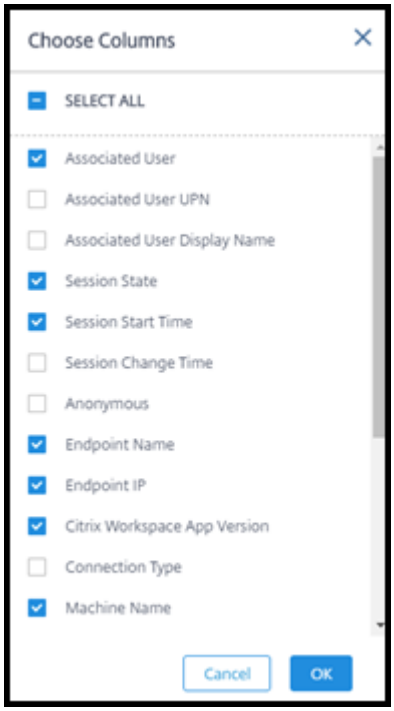
A exibição da sessão são atualizadas a cada minuto.

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.

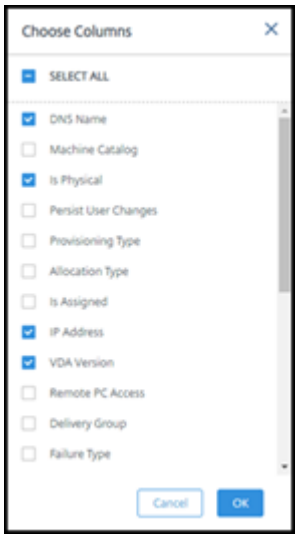
Máquinas de monitoramento e controle de energia

Os visores da máquina são atualizados a cada minuto.

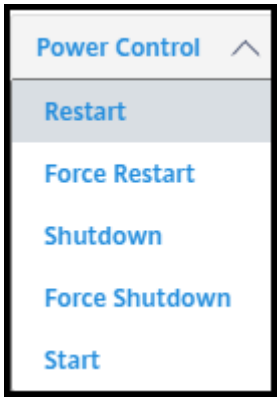
1. Em **Manage > Quick Deploy > Monitor**, selecione **Filters**.
2. Selecione a visualização **Machines** .

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

Solução de problemas no Quick Deploy

June 24, 2022

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.

Referência ao Quick Deploy

August 8, 2022

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.

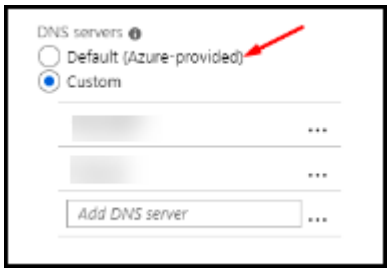
1. Antes de criar um catálogo ingressado no domínio (ou uma conexão, se estiver usando uma assinatura do Citrix Managed Azure), verifique se você tem entradas de servidor DNS que podem resolver nomes de domínios públicos e privados.

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.

Criar grupos de entrega

December 20, 2023

Introdução

Um grupo de entrega é uma coleção de máquinas selecionadas de um ou mais catálogos de máquinas. O grupo de entrega também pode especificar quais usuários podem usar essas máquinas, além dos aplicativos e áreas de trabalho disponíveis para esses usuários.

Criar um grupo de entrega é a próxima etapa na configuração da implantação depois de criar um catálogo de máquinas. Mais tarde, você pode alterar as configurações iniciais no primeiro grupo de entrega e criar outros grupos de entrega. Há também recursos e configurações que você pode definir somente ao editar um grupo de entrega, não ao criá-lo.

Antes de criar um grupo de entrega:

- Revise esta seção para saber mais sobre as escolhas que você faz e as informações que você fornece.
- Certifique-se de ter criado uma conexão com o hipervisor, serviço de nuvem ou outro recurso que hospeda suas máquinas.
- Certifique-se de ter criado um catálogo de máquinas contendo máquinas virtuais ou físicas.

Para iniciar o assistente de criação do grupo de entrega:

1. Faça login no Citrix Cloud. No menu superior esquerdo, selecione **My Services > DaaS**.
2. Selecione **Manage**.
3. Se este for o primeiro grupo de entrega que está sendo criado, o console o orienta para a seleção correta (como "Set up delivery groups to be displayed as services"). O assistente de criação do grupo de entrega é aberto e orienta você pelo processo.
4. Se você já criou um grupo de entrega e deseja criar outro, siga estas etapas:
   a) Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
   b) Para organizar grupos de entrega usando pastas, crie pastas na pasta **Delivery Groups** padrão. Para obter mais informações, consulte Criar uma pasta de grupo.
   c) Selecione a pasta na qual você deseja criar o grupo e clique em **Create Delivery Group**. O assistente de criação de grupos é aberto.

O assistente o leva pelas páginas descritas nas seções a seguir. As páginas do assistente que você vê podem ser diferentes, dependendo das seleções feitas.

Etapa 1. Máquinas

Selecione um catálogo de máquinas e selecione o número de máquinas que deseja usar desse catálogo.

É bom saber:

- Pelo menos uma máquina deve permanecer não utilizada em um catálogo selecionado.
- Um catálogo pode ser especificado em mais de um grupo de entrega. Contudo, uma máquina pode ser usada em apenas um grupo de entrega.
- Um grupo de entrega pode usar máquinas de mais de um catálogo. No entanto, esses catálogos devem conter os mesmos tipos de máquinas (SO multissessão, SO de sessão única ou Remote PC Access). Em outras palavras, você não pode misturar tipos de máquina em um grupo de entrega. Da mesma forma, se a sua implantação tiver catálogos de máquinas Windows e catálogos de máquinas Linux, um grupo de entrega pode conter máquinas de qualquer tipo de sistema operacional, mas não ambos.
- Um grupo de entrega MCS só pode adicionar um catálogo do tipo MCS.
- A Citrix recomenda que você instale ou atualize todos os VDAs com a versão mais recente e, em seguida, realize uma **alteração de nível funcional** dos catálogos de máquinas e os grupos de entrega conforme necessário. Ao criar um grupo de entrega, se você selecionar máquinas com versões VDA diferentes instaladas, o grupo de entrega será compatível com a versão mais antiga do VDA. Por exemplo, se uma das máquinas que você selecionar tiver a versão 7.1 do VDA instalada e outras máquinas tiverem uma versão mais recente, todas as máquinas do grupo

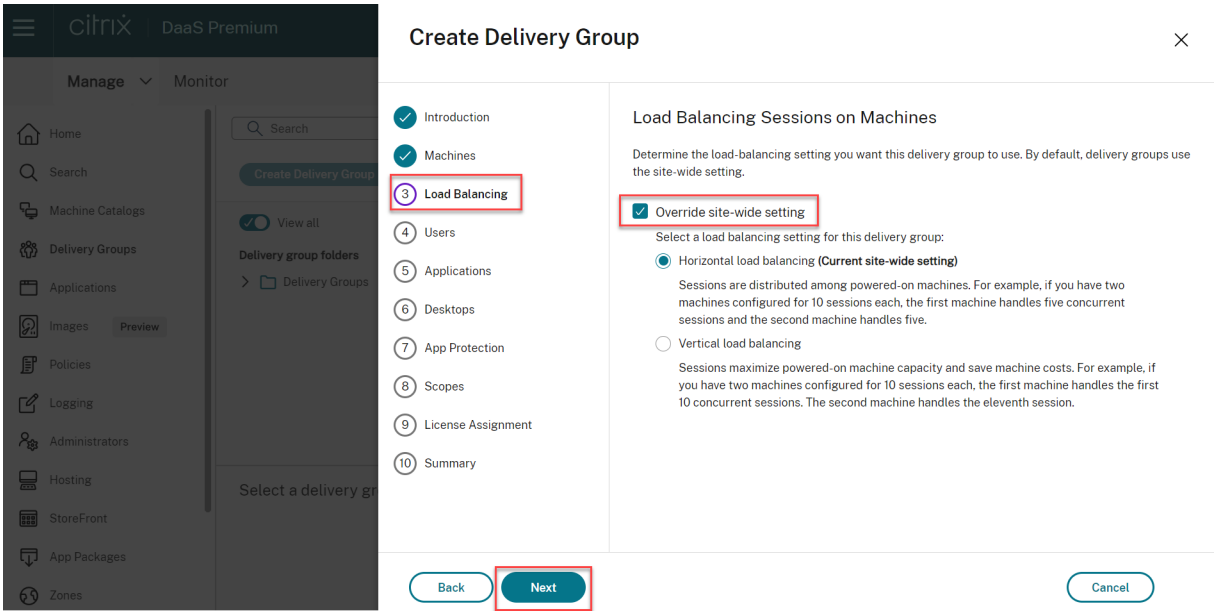
poderão usar somente os recursos compatíveis com o VDA 7.1. Isso significa que alguns recursos que exigem versões mais recentes do VDA não estarão disponíveis nesse grupo de entrega.

- As seguintes verificações de compatibilidade são realizadas:
  - MinimumFunctionalLevel deve ser compatível
  - SessionSupport deve ser compatível
  - AllocationType deve ser compatível com SingleSession
  - ProvisioningType deve ser compatível
  - PersistChanges deve ser compatível com MCS e Citrix Provisioning
  - O catálogo RemotePC só é compatível com o catálogo RemotePC
  - Verificação relacionada ao AppDisk

Etapa 2. Balanceamento de carga (prévia)

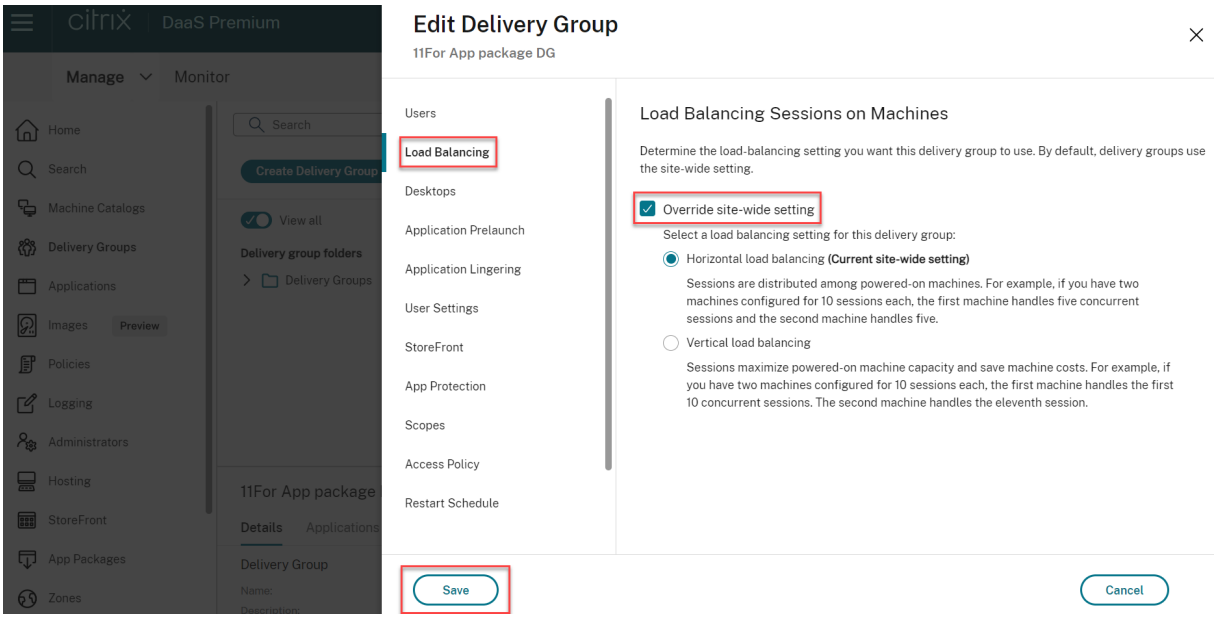
Para definir as configurações de balanceamento de carga ao criar um grupo de entrega:

1. Faça login no DaaS Premium.
2. Na navegação à esquerda, clique em **Delivery Groups**.
3. Na página **Delivery Groups**, clique em **Create Delivery Group**.
4. No assistente **Create Delivery Group**, clique em **Next**. O assistente **Machine** é aberto.
5. No assistente **Machine**, selecione um catálogo de máquinas necessário e clique em **Next**. O assistente **Load Balancing** é aberto.
6. No assistente **Load Balancing**, marque a caixa de seleção **Override site-wide setting**.
7. Selecione a opção **Horizontal load balancing** ou **Vertical load balancing** conforme necessário e clique em **Next**.

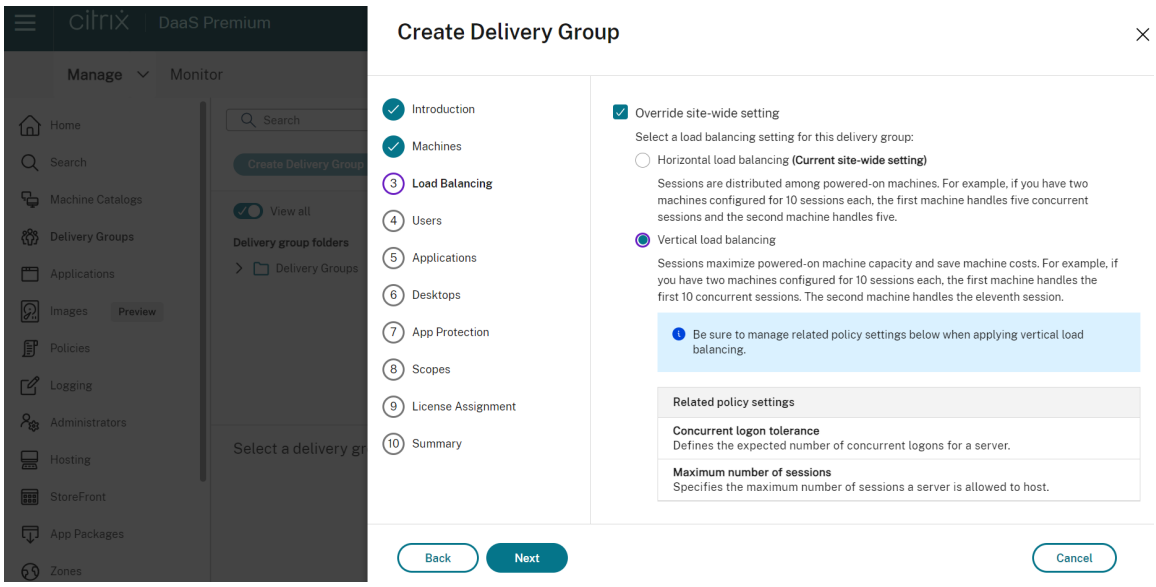


Para definir as configurações de balanceamento de carga ao editar um grupo de entrega existente:

1. Faça login no DaaS Premium.
2. Na navegação à esquerda, clique em **Delivery Groups**.
3. Selecione um **grupo de entrega** na lista e clique em **Edit**. O assistente **Edit Delivery Group** é aberto.
4. Na página **Edit Delivery Group**, clique em **Load Balancing**.
5. Marque a caixa de seleção **Override site-wide setting**.
6. Selecione a opção **Horizontal load balancing** ou **Vertical load balancing** conforme necessário e clique em **Save**.



> **Nota:**
>
> Quando a configuração de balanceamento de carga vertical for aplicada, verifique se as políticas **Concurrent logon tolerance** e **Maximum number of sessions** estão configuradas adequadamente.



Para obter mais informações sobre balanceamento de carga em nível de site e de grupo de entrega, consulte Balanceamento da carga das máquinas.

Etapa 3. Tipo de entrega, em Delivery Type

Esta página é exibida somente se você escolher um catálogo de máquinas contendo máquinas de SO de sessão única estáticas (atribuídas). Escolha **Applications** ou **Desktops.** Você não pode ativar os dois.

Se você selecionou máquinas de um catálogo de SO multissessão ou de SO de sessão única aleatório (em pool), o tipo de entrega será considerado como sendo de aplicativos e áreas de trabalho. Você pode entregar aplicativos, áreas de trabalho ou ambos.

Etapa 4. AppDisks

Ignore esta página. Selecione **Next.**

Etapa 5. Usuários

Especifique os usuários e grupos de usuários que podem usar os aplicativos e áreas de trabalho no grupo de entrega.

Onde as listas de usuários são especificadas

As listas de usuários são especificadas quando você cria ou edita o seguinte:

- A lista de acesso de usuários de uma implantação, que não é configurada por meio deste console. Por padrão, a regra de política de direito ao aplicativo inclui todos. Consulte os cmdlets `BrokerAppEntitlementPolicyRule` do SDK do PowerShell para obter detalhes.
- Grupos de entrega.
- Aplicativos.

> **Nota:**
>
> Ao especificar uma lista de usuários, você pode selecionar contas de usuário de qualquer um dos seguintes provedores de identidade aos quais sua conta do Citrix Cloud está conectada: Active Directory, Azure Active Directory ou Okta.

A lista de usuários que podem acessar um aplicativo é formada pela interseção das listas de usuários acima.

Usuários autenticados e não autenticados

Existem dois tipos de usuários: autenticado e não autenticado (não autenticado também é chamado de anônimo). Você pode configurar um ou os dois tipos em um grupo de entrega.

- **Authenticated:** para acessar aplicativos e áreas de trabalho, os usuários e membros do grupo que você especificar por nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha no aplicativo StoreFront ou Citrix Workspace. (Para grupos de entrega contendo máquinas de SO de sessão única, você pode importar dados do usuário (uma lista de usuários) posteriormente editando o grupo de entrega.)
- **Unauthenticated (anonymous):** para grupos de entrega contendo máquinas de SO multissessão, você pode permitir que os usuários acessem aplicativos e áreas de trabalho sem apresentar credenciais para o aplicativo StoreFront ou Citrix Workspace. Por exemplo, em quiosques, o aplicativo pode exigir credenciais, mas o portal de acesso Citrix e as ferramentas não. Um grupo de usuários anônimos é criado quando você instala o primeiro Delivery Controller.

  Para conceder acesso a usuários não autenticados, cada máquina no grupo de entrega deve ter um VDA com SO multissessão instalado. Quando usuários não autenticados estão habilitados, você deve ter um armazenamento StoreFront não autenticado.

  Contas de usuários não autenticados são criadas sob demanda quando uma sessão é iniciada e são chamadas AnonXYZ, em que XYZ é um valor único de três dígitos.

  As sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desativadas automaticamente quando o cliente se desconecta. Não há suporte para reconexão, roaming entre clientes e controle de espaço de trabalho.

A tabela a seguir descreve as suas escolhas na página **Users**:

Ativar acesso para	Adicionar/atribuir usuários e grupos de usuários?	Ativar a caixa de seleção “Give access to unauthenticated users”?
Somente usuários autenticados	Sim	Não
Somente usuários não autenticados	Não	Sim
Usuários autenticados e não autenticados	Sim	Sim

Restringir o acesso de usuários ou grupos

Você também pode restringir o uso de um grupo de entrega adicionando usuários ou grupos de usuários à **lista de permissão**. Somente usuários na **lista de permissão** podem acessar aplicativos e áreas de trabalho no grupo de entrega. Você também pode adicionar usuários e grupos de usuários a uma lista de bloqueio clicando em **Add block list**, o que impede que os usuários usem aplicativos e áreas de trabalho no grupo de entrega selecionado. Uma lista de bloqueio só é significativa quando usada para bloquear usuários na lista de permissão.

Etapa 6. Aplicativos

É bom saber:

- Não é possível adicionar aplicativos a grupos de entrega de acesso ao PC remoto.
- Por padrão, os novos aplicativos adicionados são colocados em uma pasta chamada Applications. 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 outro com o mesmo nome na pasta, você será solicitado a renomear o aplicativo que está adicionando. Se você recusar, o aplicativo é adicionado com um sufixo que o torna exclusivo dentro na pasta de aplicativos.
- Quando você adiciona um aplicativo a mais de um grupo de entrega, um problema de visibilidade pode ocorrer se você não tiver permissão para exibir o aplicativo em todos os grupos de entrega. Nesses casos, consulte um administrador com mais permissões ou estenda o seu escopo 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 Application name (for user). Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

Selecione o menu **Add** para exibir as origens do aplicativo.

- **From Start menu:** aplicativos que são detectados em uma máquina criada a partir da imagem no catálogo selecionado. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados; selecione aqueles que deseja adicionar e selecione **OK**.
- **Manually defined:** aplicativos localizados na implantação ou em outro lugar na sua rede. Quando você seleciona essa origem, uma nova página é iniciada 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**.
- **Existing:** aplicativos adicionados anteriormente à implantação, talvez em outro grupo de entrega. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados; selecione aqueles que deseja adicionar e selecione **OK**.
- **App-V:** aplicativos em pacotes App-V. Quando você seleciona essa origem, uma nova página é iniciada na qual você seleciona o servidor App-V ou a biblioteca de aplicativos. Na exibição resultante, selecione os aplicativos que deseja adicionar e selecione **OK**.

Se a origem de um aplicativo ou um aplicativo não estiver disponível ou válido, ele não estará visível ou não poderá ser selecionado. Por exemplo, a origem **Existing** não está disponível se nenhum aplicativo tiver sido adicionado à implantação. Ou um aplicativo pode não ser compatível com os tipos de sessão com suporte nas máquinas do catálogo de máquinas selecionado.

Etapa 7. App Protection

As informações a seguir complementam o artigo App Protection na documentação do Citrix Virtual Apps and Desktops. Para usar o App Protection 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 válidos do App Protection. Para comprar o recurso App Protection, você pode entrar em contato com o seu representante de vendas da Citrix.
- O App Protection exige confiança em XML. Para ativar a confiança em XML, vá para **Settings > Enable XML trust**.
- Em relação à proteção contra captura de tela:
  - No Windows e no macOS, somente a janela do conteúdo protegido fica em branco. O App Protection fica ativo quando uma janela protegida não é minimizada.

  - No Linux, toda a captura fica em branco. O App Protection fica ativo independentemente de uma janela protegida ser minimizada ou não.

Etapa 8. Áreas de trabalho ou regras, em Desktops (ou Desktop Assignment Rules)

O título desta página depende do catálogo de máquinas que você escolheu anteriormente no assistente:

- Se você escolheu um catálogo contendo máquinas em pool, a página será intitulada **Desktops**.
- Se você escolheu um catálogo contendo máquinas atribuídas e especificou "Desktops"no **Delivery Type** página, a página é intitulada **Desktop Assignment Rules**.
- Se você escolheu um catálogo contendo máquinas atribuídas e especificou "Applications"na página **Delivery Type**, a página é intitulada **Applications**.

Selecione **Add**. Na caixa de diálogo:

- Nos campos **Display name** e **Description**, digite as informações a serem exibidas no aplicativo Citrix Workspace.
- Para adicionar uma restrição de marca a uma área de trabalho, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca no menu.
- Usando os botões de opção, você pode:
  - **Permitir que todos com acesso a esse grupo de entrega usem uma área de trabalho.** Todos os usuários do grupo de entrega podem iniciar uma área de trabalho (para grupos com máquinas em pool) ou ter uma máquina atribuída ao iniciar a área de trabalho (para grupos com máquinas atribuídas).
  - **Restringir o uso da área de trabalho** adicionando usuários e grupos de usuários à **lista de permissão**. Somente usuários na **lista de permissão** podem acessar uma área de trabalho. Você também pode adicionar usuários e grupos de usuários a uma lista de bloqueio clicando em **Add block list**, o que impede que os usuários usem áreas de trabalho no grupo de entrega selecionado. Uma lista de bloqueio só é significativa quando usada para bloquear usuários na lista de permissão.
- Se o grupo contém máquinas atribuídas, especifique o número máximo de áreas de trabalho por usuário. Esse valor deve ser um ou maior.
- Ative ou desative a área de trabalho (para máquinas em pool) ou a regra de atribuição de área de trabalho (para máquinas atribuídas). Desativar uma área de trabalho interrompe a entrega da área de trabalho. Desativar uma regra de atribuição de área de trabalho interrompe a atribuição automática da área de trabalho aos usuários.
- Quando terminar com a caixa de diálogo, selecione **OK**.

Etapa 9. Atribuição de licença

Determine 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 Licenciamento multitipos.

Etapa 10. Resumo

Insira um nome para o grupo de entrega. Você também pode (opcionalmente) inserir uma descrição, que aparece no aplicativo Workspace e na interface de gerenciamento Full Configuration.

Revise as informações de resumo e selecione **Finish**. Se você não selecionou nenhum aplicativo ou especificou nenhuma área de trabalho para ser entregue, você será perguntado se deseja continuar.

Mais informações

- Gerenciar grupos de entrega
- Aplicativos

Gerenciar grupos de entrega

November 21, 2023

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 definir outras configurações que não estão disponíveis quando você cria um grupo de entrega.

Os procedimentos são organizados por categorias: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Prevent users from connecting to machines" é descrito na categoria de máquinas, mas também afeta os usuários. Portanto, se você não conseguir encontrar uma tarefa em uma categoria, procure em uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Applications contém informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer permissões relacionadas à função interna de Administrador de grupos de entrega. Para obter detalhes, consulte Administração delegada.

Geral

- Alterar o tipo de entrega
- Alterar endereços do StoreFront
- Alterar o nível funcional
- Gerenciar grupos de entrega de Remote PC Access
- Alterar a licença para um grupo de entrega
- Organizar grupos de entrega usando pastas
- Gerenciar proteção de aplicativo

Alterar o tipo de entrega de um grupo de entrega

O tipo de entrega indica o que o grupo pode entregar: aplicativos, áreas de trabalho ou ambos.

Antes de alterar um tipo de **aplicativo** para o tipo de **Desktops**, exclua todos os aplicativos do grupo.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Delivery Type**, selecione o tipo de entrega desejado.
4. Selecione **Apply** 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. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **StoreFront**, indique se você especificará um endereço de servidor StoreFront posteriormente (**Manually**) ou selecione **Add new** para especificar os servidores StoreFront que deseja usar (**Automatically**).
4. Selecione **Apply** 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 do servidor StoreFront selecionando **StoreFront** no painel esquerdo do console.

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 usar o Citrix Provisioning (anteriormente Provisioning Services), atualize a versão do VDA no console Citrix Provisioning.
- Inicie as máquinas que contêm o VDA atualizado para que possam se registrar no Citrix DaaS. Esse processo informa o console sobre o que deve ser alterado no grupo de entrega.
- Se você precisa continuar usando versões anteriores do VDA, os novos recursos 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. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Change Functional Level** na barra de ações. A ação **Change Functional Level** aparece somente se forem detectados VDAs atualizados.

A tela indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Você pode cancelar a ação de alteração, resolver o problema das máquinas e 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 selecione **Undo Functional Level Change** na barra de ações.

Gerenciar grupos de entrega de Remote PC Access

Se uma máquina em um catálogo de máquinas Remote PC Access não está atribuída a um usuário, a máquina é 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 de catálogo de máquinas a grupos de entrega tem um valor de prioridade. A prioridade determina a qual grupo de entrega essa máquina é atribuída quando ela 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 Remote PC Access tiver várias atribuições de grupo de entrega, o software seleciona a correspondência com a prioridade mais alta. Use o SDK do PowerShell para definir o valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas Remote PC Access são associados a um grupo de entrega. Isso significa que as contas de máquina ou unidades organizacionais adicionadas ao catálogo posteriormente podem ser adicionadas ao grupo de entrega. Esta associação pode ser ativada ou desativada.

Para adicionar ou remover uma associação de catálogo de máquinas Remote PC Access com um grupo de entrega:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo Remote PC Access.

3. Na seção **Details**, selecione a guia **Machine Catalogs** e selecione um catálogo Remote PC Access.
4. Para adicionar ou restaurar uma associação, selecione **Add Desktops**. Para remover uma associação, selecione **Remove Association**.

Alterar a licença para um grupo de entrega

Para alterar o direito de licença para um grupo de entrega, siga estas etapas:

1. Selecione **Delivery Groups** no painel de navegação.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **License Assignment**, selecione a licença que você deseja que o grupo use.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Para obter mais informações sobre direitos de nível de grupo de entrega, consulte Licenciamento multitipos.

Organizar grupos de entrega usando pastas

Você pode criar pastas para organizar grupos de entrega e facilitar o acesso.

Funções necessárias Por padrão, você precisa ter a seguinte função integrada para criar e gerenciar pastas do grupo de entrega: administrador da nuvem, administrador completo ou administrador do grupo de entrega. Se necessário, você pode personalizar funções para criar e gerenciar pastas do grupo de entrega. Para obter mais informações, consulte Permissões necessárias.

Criar uma pasta para grupos de entrega Antes de começar, planeje como organizar seus grupos de entrega. Considere o seguinte:

- Você pode aninhar pastas com até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de entrega e subpastas.
- Todos os nós em **Full Configuration** (como os nós **Machine Catalogs**, **Applications** e **Delivery groups**) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outros nós ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nos diferentes nós.

Para criar uma pasta de grupo de entrega, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.

2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Create Folder** na barra **Action**.
3. Insira um nome para a nova pasta e clique em **Done**.

> **Dica:**
>
> Se você criar uma pasta em um local não desejado, 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. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Exibir grupos por pasta. Você também pode ativar **View all** acima da hierarquia de pastas para exibir todos os grupos de uma vez só.
3. Clique com o botão direito em um grupo e selecione **Move Delivery Group**.
4. Selecione a pasta para a qual deseja mover o grupo e clique em **Done**.

> **Dica:**
>
> Você pode arrastar um grupo para uma pasta.

Gerenciar pastas de grupos de entrega

Você pode excluir, renomear e mover pastas do grupo de entrega.

Lembre-se de que você só pode excluir uma pasta se ela e suas subpastas não contiverem grupos de entrega.

Para gerenciar uma pasta, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Action**, conforme necessário:
   - Para renomear a pasta, selecione **Rename Folder**.
   - Para excluir a pasta, selecione **Delete Folder**.
   - Para mover a pasta, selecione **Move Folder**.
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 para grupos de entrega	Create Delivery Group Folder
Excluir pastas de grupos de entrega	Remove Delivery Group Folder
Mover pastas de grupos de entrega	Move Delivery Group Folder
Renomear pastas do grupo de entrega	Edit Delivery Group Folder
Mover grupos de entrega para pastas	Edit Delivery Group Folder e Edit Delivery Group Properties

Gerenciar proteção de aplicativo

As informações a seguir complementam o 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. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **App Protection**, você pode ativar **Anti-keylogging** e **Anti-screen-capturing**.

- Você deve ter uma assinatura válida do Citrix Cloud e direitos válidos de proteção de aplicativos. Para comprar o recurso de proteção de aplicativos, você pode entrar em contato com o seu representante de vendas da Citrix.
- A proteção de aplicativos exige confiança em XML. Para ativar a confiança em XML, vá para **Settings > Enable XML trust**.
- Em relação à proteção contra captura de tela:
  - No Windows e no macOS, somente a janela do conteúdo protegido fica em branco. A proteção de aplicativo fica ativa quando uma janela protegida não é minimizada.
  - No Linux, toda a captura fica em branco. A proteção de aplicativo fica ativa independentemente de uma janela protegida ser minimizada ou não.

Usuários

> **Nota:**
>
> A opção **Leave user management to Citrix Cloud** foi removida. Para grupos de entrega em que as atribuições de usuários foram tratadas por meio do Citrix Cloud, continue gerenciando-os na biblioteca do Citrix Cloud.

Este tópico abrange as seguintes seções:

- Alterar configurações do usuário
- Adicionar ou remover usuários

Alterar as configurações do usuário em um grupo de entrega

O nome dessa página aparece como **User Settings** ou **Basic Settings**.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **User Settings**, altere qualquer uma das configurações na tabela a seguir.
4. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou selecione **OK** para aplicar as alterações e fechar a janela.

Definição	Descrição
Descrição	O texto que o Citrix Workspace (ou StoreFront) usa e que os usuários veem.
Enable Delivery Group	Se o grupo de entrega está ativado ou não.
Time zone	O fuso horário no qual as máquinas desse grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site. **Nota:** alterar o fuso horário em um grupo de entrega pode reinicializar as máquinas desse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

Definição	Descrição
Enable Secure ICA	Protege comunicações de e para máquinas no grupo de entrega usando SecureICA, que criptografa o protocolo ICA. O nível padrão é 128 bits. O nível pode ser alterado usando o SDK. A Citrix recomenda o uso de mais métodos de criptografia, como a criptografia TLS, ao atravessar redes públicas. Além disso, SecureICA não verifica a integridade dos dados.
Maximum desktops per user	Quantos desktops um usuário pode ter.

Adicionar ou remover usuários em um grupo de entrega

Para obter informações detalhadas sobre usuários, consulte Usuários.

1. Em **Manage > Full Configuration**, 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**:
   - Para adicionar usuários, selecione **Add** e, em seguida, especifique os usuários que deseja adicionar.
   - Para remover usuários, selecione um ou mais usuários e selecione **Remove**.
   - Marque ou desmarque a caixa de seleção para permitir o acesso por usuários não autenticados.
4. Selecione **Apply** 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 gerenciar atribuições de usuário:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups**.
2. Selecione um grupo e, em seguida, selecione **Edit Delivery Group** na barra de ações.
3. Na página **Machine Allocation**, adicione ou remova usuários. Para adicionar usuários, navegue até eles ou insira uma lista de nomes de usuário separados por ponto-e-vírgula.

Ao inserir nomes de usuário, considere o seguinte:

- 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`.

Máquinas

- Alterar atribuições de máquinas a usuários
- Atualizar uma máquina
- Adicionar, alterar ou remover uma restrição de marca para uma área de trabalho
- Remover uma máquina
- Restringir o acesso a máquinas
- Impedir que usuários se conectem a uma máquina (modo de manutenção)
- Desligar e reiniciar máquinas
- Criar e gerenciar agendamentos de reinicialização de máquinas
- Máquinas para gerenciar carga
- Gerenciar Autoscale

Além dos recursos descritos neste artigo, consulte AutoScale para obter informações sobre proativamente ligar/desligar máquinas de gerenciamento.

Alterar atribuições de máquinas para usuários em um grupo de entrega

Você pode alterar as atribuições de máquinas de SO de sessão única provisionadas com MCS. Não é possível alterar atribuições de máquinas com SO multissessão ou máquinas provisionadas com o Citrix Provisioning.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Machine Allocation**, especifique os novos usuários.
4. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou selecione **OK** para aplicar as alterações e fechar a janela.

Atualizar uma máquina em um grupo de entrega

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e selecione **View Machines** na barra de ações.
3. Selecione uma máquina e, em seguida, selecione **Update Machines** na barra de ações.

Para escolher uma imagem diferente, selecione **Master Image** e, em seguida, selecione um instantâneo.

Para aplicar alterações e notificar os usuários da máquina, selecione **Rollout notification to end-users**. Em seguida, especifique:

- Quando atualizar a imagem: agora ou na próxima reinicialização

- A hora de distribuição de reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados sobre a reinicialização ou não
- A mensagem que os usuários receberão

Adicionar, alterar ou remover uma restrição de marca para uma área de trabalho

Adicionar, alterar e remover restrições de marca pode ter efeitos imprevisíveis sobre quais áreas de trabalho são consideradas para a inicialização. Consulte as considerações e precauções em Marcas.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Desktops**, selecione a área de trabalho e selecione **Edit**.
4. Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca.
5. Para alterar ou remover uma restrição de marca siga, escolha uma ação:
   - Selecione uma marca diferente.
   - Remova a restrição de marca desmarcando **Restrict launches to machines with this tag**.
6. Selecione **Apply** 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

A remoção de uma máquina a exclui de um grupo de entrega. Ela não a exclui do catálogo de máquinas usado pelo grupo de entrega. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes que possam ser removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto ela está sendo removida, coloque a máquina no modo de manutenção antes de desligá-la.

As máquinas podem conter dados pessoais, portanto, seja cauteloso antes de alocar a máquina para outro usuário. Considere refazer a imagem da máquina.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e selecione **View Machines** na barra de ações.
3. Assegure-se de que a máquina está desligada.
4. Selecione a máquina e, em seguida, selecione **Remove from Delivery Group** na barra de ações.

Você também pode remover uma máquina de um grupo de entrega através da conexão que a máquina usa.

Restringir o acesso a máquinas em um grupo de entrega

Quaisquer alterações que você fizer para restringir o acesso a máquinas em um grupo de entrega substituem as configurações anteriores, independentemente do método usado. Você pode:

- **Restringir o acesso de administradores que usam escopos de administração delegada:** você pode criar e atribuir um escopo que permita que os administradores acessem todos os aplicativos e outro escopo que forneça acesso a apenas determinados aplicativos. Para obter detalhes, consulte Administração delegada.
- **Restringir o acesso de usuários por meio de expressões de política SmartAccess:** use expressões de política para filtrar conexões de usuário realizadas por meio do Citrix Gateway.

  1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
  2. Selecione um grupo e clique em **Edit** na barra de ações.
  3. Na página da **Access Policy**, selecione **Connections through Citrix Gateway**.
  4. Para escolher um subconjunto dessas conexões, selecione **Connections meeting any of the following filters**. Em seguida, defina o site Citrix Gateway e adicione, edite ou remova as expressões de política do SmartAccess para os cenários permitidos de acesso do usuário. Para obter detalhes, consulte a documentação do Citrix Gateway.
  5. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou selecione **Save** para aplicar as alterações e fechar a janela.

- **Restringir o acesso de usuários por meio de filtros de exclusão:** use filtros de exclusão nas políticas de acesso que você definiu no SDK. As políticas de acesso são aplicadas a grupos de entrega para refinar as conexões. Por exemplo, você pode restringir o acesso da máquina a um subconjunto de usuários e especificar dispositivos de usuário permitidos. Os filtros de exclusão refinam ainda mais as políticas de acesso. Por exemplo, por segurança, você pode negar o acesso a um subconjunto de usuários ou dispositivos. Por padrão, os filtros de exclusão são desativados.

  Por exemplo, para impedir o acesso de um laboratório de ensino em uma sub-rede de uma rede corporativa a um grupo de entrega específico, independentemente de quem está usando as máquinas no laboratório, use o comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

  Você pode usar o asterisco (*) como curinga para corresponder a todas as marcas que começam com a mesma expressão de política. Por exemplo, se você adicionar a marca `VPDesktops_Direct` a uma máquina e `VPDesktops_Test` a outra, definir a marca no script `Set-BrokerAccessPolicy` como `VPDesktops_*` aplica o filtro às duas máquinas.

Se você estiver conectado usando um navegador da Web ou com o recurso de experiência do usuário do aplicativo Citrix Workspace ativado na loja, não será possível usar um filtro de exclusão de nome cliente.

Impedir que os usuários se conectem a uma máquina (modo de manutenção) em um grupo de entrega

Quando precisar interromper temporariamente novas conexões às máquinas, você pode ativar o modo de manutenção de uma ou de todas as máquinas em um grupo de entrega. Você pode fazer isso antes de aplicar patches ou usar ferramentas de gerenciamento.

- Quando uma máquina com SO multissessão 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 computador usando Remote PC Access) está no modo de manutenção, os usuários não podem se conectar ou reconectar. As conexões atuais permanecem ativas até que se desconectem ou seja feito logoff.

Para ativar ou desativar o modo de manutenção:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo.
3. Para ativar o modo de manutenção para todas as máquinas do grupo de entrega, selecione **Turn On Maintenance Mode** na barra de ações.

   Para ativar o modo de manutenção para uma máquina, selecione **View Machines** na barra de ações. Selecione uma máquina e selecione **Turn On Maintenance Mode** 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 **Turn Off Maintenance Mode** na barra de ações.

As configurações da Conexão de Área de Trabalho Remota (RDC) do Windows também afetam se uma máquina com SO multissessão está ou não no modo de manutenção. O modo de manutenção é ativado quando ocorre uma das seguintes circunstâncias:

- O modo de manutenção é definido como ativado, conforme descrito anteriormente.
- A RDC está definida como **Não permitir conexões com este computador**.
- A RDC não está definida como **Não permitir conexões com este computador** e a configuração de Remote Host Configuration User Logon Mode 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 Remote PC Access.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e selecione **View Machines** na barra de ações.
3. Selecione a máquina e, em seguida, selecione uma das seguintes ações na barra de ações:

   > **Nota:**
   >
   > - As ações a seguir se aplicam somente a máquinas com gerenciamento de energia.
   > - Algumas opções podem não estar disponíveis, dependendo do estado da máquina.

   - **Force shut down:** força o desligamento da máquina e atualiza a lista de máquinas.
   - **Restart:** solicita que o sistema operacional seja desligado e, em seguida, inicializa a máquina novamente. Se o sistema operacional não conseguir, a máquina permanecerá em seu estado atual.
   - **Force restart:** força o desligamento do sistema operacional e, em seguida, reinicializa a máquina.
   - **Suspend:** pausa a máquina sem desligá-la e atualiza a lista de máquinas.
   - **Shut down:** solicita que o sistema operacional seja desligado.

Para ações não forçadas, se a máquina não for desligada em 10 minutos, ela será encerrada. Se o Windows tentar instalar atualizações durante o desligamento, existe o risco de a máquina ser encerrada antes do término das atualizações.

Criar e gerenciar agendamentos de reinicialização de máquinas em um grupo de entrega

> **Nota:**
>
> - Quando um agendamento de reinicialização é aplicado a um grupo de entrega com AutoScale habilitado, suas máquinas são simplesmente desligadas e ficam aguardando que o AutoScale volte a 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 nos custos. Recomendamos que você use o AutoScale para ligar as máquinas.
> - Alterar o fuso horário em um grupo de entrega pode reinicializar as máquinas desse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora

> do horário de produção.

O agendamento de reinicialização especifica a periodicidade de reinicialização das máquinas em um grupo de entrega. Você pode criar um ou mais agendamentos para um grupo de entrega. Um agendamento pode afetar:

- Todas as máquinas no grupo.
- Uma ou mais máquinas (mas não todas) no grupo. As máquinas são identificadas por uma marca que você aplica à máquina. Isso é chamado de restrição de marca, porque a marca restringe uma ação a apenas os itens (nesse caso, as máquinas) que têm a marca.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você quer que cada máquina seja reinicializada uma vez por semana e que as máquinas usadas pelo pessoal da contabilidade sejam reinicializadas diariamente. Para isso, configure um cronograma para todas as máquinas e outro cronograma 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 "start all affected machines at the same time"ou um intervalo que provavelmente usará para reiniciar todas as máquinas afetadas.

Você pode ativar ou desativar um agendamento. Desabilitar um agendamento pode ser útil durante a realização de testes, durante intervalos especiais ou quando você estiver preparando o cronograma de agendamentos antes de precisar deles.

Não é possível usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reinicializar.

Sobreposição de agendamentos Pode acontecer de os agendamentos se sobreporem. No exemplo acima, os dois agendamentos afetam as máquinas da contabilidade. Essas máquinas podem ser reinicializadas duas vezes aos domingos. O código de agendamento foi projetado para evitar a reinicialização da mesma máquina com mais frequência do que o desejado, mas não é garantido.

- Se os agendamentos coincidirem precisamente na hora de início e na duração, é mais provável que as máquinas serão reinicializadas apenas uma vez.
- Quanto mais diferentes forem a hora de início e a duração nos agendamentos, maior a probabilidade de que ocorrerão várias reinicializações.
- O número de máquinas afetadas por um agendamento também afeta a probabilidade de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário das máquinas do departamento de contabilidade, dependendo da duração especificada para cada.

Para uma análise detalhada dos agendamentos de reinicialização, consulte Reboot schedule internals.

Exibir agendamentos de reinicialização

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Selecione a página **Restart Schedule**.

A página **Restart Schedule** contém as seguintes informações sobre cada agendamento configurado:

- Nome do agendamento.
- Restrição de marca usada, se houver.
- Com que frequência as reinicializações da máquina ocorrem.
- Se os usuários da máquina recebem uma notificação.
- Se o agendamento está habilitado. Desabilitar um agendamento pode ser útil durante a realização de testes, durante intervalos especiais ou quando você estiver preparando o cronograma de agendamentos antes de precisar deles.

Adicionar (aplicar) marcas Quando você configura um agendamento de reinicialização que usa uma restrição de marca, verifique se a marca foi adicionada (aplicada) às máquinas afetadas pelo agendamento. No exemplo acima, cada uma das máquinas usadas pelo pessoal de contabilidade tem uma marca aplicada. Para obter detalhes, consulte Marcas.

Embora você possa aplicar mais de uma marca a uma máquina, um agendamento de reinicialização pode especificar apenas uma marca.

1. Em **Manage > Full Configuration**, 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 marca.
4. Selecione **Manage Tags** na barra de ações.
5. Se a marca existir, ative a caixa de seleção ao lado do nome da marca. Se a marca não existir, selecione **Create** e, em seguida, especifique o nome da marca. Depois que a marca é criada, ative a caixa de seleção ao lado do nome da marca recém-criada.
6. Selecione **Save** na caixa de diálogo **Manage Tags**.

Criar um agendamento de reinicialização

1. Em **Manage > Full Configuration**, 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 ativar o agendamento, selecione **Yes**. Para desativar o agendamento, selecione **No**.
- Digite um nome e uma descrição do agendamento.
- Em **Restrict to tag**, aplique uma restrição de marca.
- Em **Include machines in maintenance mode**, escolha se deseja incluir neste agendamento de reinicialização as máquinas que estão no modo de manutenção. Para usar o PowerShell, consulte Reinicializações agendadas para máquinas no modo de manutenção.
- Em **Restart frequency**, selecione com que frequência a reinicialização ocorre: diariamente, semanalmente, mensalmente ou uma vez. Se você selecionar **Weekly** ou **Monthly**, poderá especificar um ou mais dias específicos.
- Em **Repeats every**, especifique com que frequência você deseja que o agendamento seja executado.
- Em **Start date**, especifique uma data de início para a primeira ocorrência do agendamento.
- Em **Begin restart at**, especifique, no formato 24 horas, a hora do dia para iniciar a reinicialização.
- Em **Restart duration**:
  - Se você não quiser usar a reinicialização natural, selecione **Restart all machines at the same time** ou **Restart all machines within a time period**.
  - Se você quiser usar a reinicialização natural, selecione **Restart all machines after draining all sessions**.

    Ao iniciar um agendamento de reinicialização configurado para usar a reinicialização natural:

    * 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:**
    >
    > Você pode usar essa opção para máquinas com gerenciamento de energia e também para máquinas que não são gerenciadas por energia.

- Em **Send notification to users**, escolha se deseja exibir uma mensagem de notificação nas máquinas aplicáveis antes de iniciar uma reinicialização. Por padrão, nenhuma mensagem é exibida.

- Se optar por exibir uma mensagem 15 minutos antes do início da reinicialização, você pode escolher (em **Notification frequency**) para 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 reinicializar, inclua a variável **%m%**. A menos que você opte por reinicializar todas as máquinas ao mesmo tempo, a mensagem aparece em cada máquina no momento apropriado antes da reinicialização.

5. Clique em **Done** para aplicar as alterações e fechar a janela **Add Restart Schedule**.
6. Clique em **Apply** para aplicar as alterações feitas e manter a janela **Edit Delivery Group** aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Executar imediatamente um agendamento de reinicialização Um agendamento de reinicialização especifica quando as máquinas em um grupo de entrega são reiniciadas regularmente. Você também pode executar um agendamento de reinicialização imediatamente para reinicializar as máquinas nesse agendamento.

Para executar um agendamento de reinicialização imediatamente, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega aplicável e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Restart Schedule**, selecione um agendamento que você deseja executar e, em seguida, selecione **Run schedule now**.

> **Nota:**
>
> - Você não pode executar um agendamento imediatamente se ele estiver definido com a configuração **Restart all machines after draining sessions**.
> - Você pode aplicar **Run schedule now** apenas a um agendamento por vez.
> - Depois de editar um agendamento, **Run schedule now** fica indisponível. Selecione **Apply** para disponibilizá-lo.

Editar, remover, ativar ou desativar um agendamento de reinicialização

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Restart Schedule**, marque a caixa de seleção de um agendamento.

   - Para editar um agendamento, selecione **Edit**. Atualize a configuração do agendamento, usando as orientações em Criar um agendamento de reinicialização.

- Para ativar ou desativar um agendamento, selecione **Edit**. Marque ou desmarque a caixa de seleção **Enable restart schedule**.
- Para remover um agendamento, selecione **Remove**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma marca aplicada às máquinas nas máquinas afetadas.

Reinicializações programadas atrasadas devido à interrupção do banco de dados

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

Se ocorrer uma interrupção do banco de dados do site antes da reinicialização agendada começar para as máquinas (VDAs) em um grupo de entrega, as reinicializações iniciam quando a interrupção termina. Isso pode ter resultados inesperados.

Por exemplo, digamos que você agendou as reinicializações de um grupo de entrega para ocorrer durante um horário fora do período de produção (começando às 3h). Uma interrupção do banco de dados do site ocorre uma hora antes do início da reinicialização agendada (2h). A interrupção dura seis horas (até as 8h). O cronograma de reinicialização começa quando a conexão entre o Delivery Controller e o banco de dados do site é restaurada. As reinicializações dos VDAs agora começam cinco horas após o agendamento original. Isso pode resultar na reinicialização dos VDAs durante o horário de produção.

Para ajudar a evitar esta situação, você pode usar o parâmetro `MaxOvertimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além da hora de início programada que um agendamento de reinicialização pode começar.

- Se a conexão do banco de dados for restaurada dentro desse tempo (horário agendado + `MaxOvertimeStartMins`), a reinicialização do VDA começa.
- Se a conexão do banco de dados não for restaurada dentro desse período de tempo, as reinicializações de VDA não começam.
- Se esse parâmetro for omitido ou tiver 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 no modo de manutenção Para indicar se um agendamento de reinicialização afeta máquinas que estão no modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria um agendamento que reinicializa as máquinas que estão e as máquinas que não estão no 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.

Máquinas que gerenciam carga em grupos de entrega

Você pode gerenciar a carga somente de máquinas com SO multissessão.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as atuais condições do ambiente. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** uma máquina com SO multissessão 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 fornece máquinas com SO multissessão receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações de métricas de desempenho, como CPU, disco e uso de memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga.

  Um índice de carga de servidor de 10000 indica que o servidor está totalmente carregado. Se nenhum outro servidor estiver disponível, os usuários poderão receber uma mensagem informando que a área de trabalho ou o aplicativo não está disponível atualmente quando iniciarem uma sessão.

  Você pode monitorar o índice de carga no Director (Monitor), uma pesquisa de interface de gerenciamento Full Configuration e o SDK.

  Nas exibições do console, para exibir a coluna **Server Load Index** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse em um cabeçalho de coluna e selecione **Select Column**. Em **Machine category**, selecione **Load Index**.

  No SDK, use o cmdlet `Get-BrokerMachine`. Para obter detalhes, consulte CTX202150.
- **Concurrent logon tolerance policy setting:** o número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões XenApp 6.x.)

Quando todos os servidores superam ou se encontram no limite 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 é selecionado.

Gerenciar Autoscale

Por padrão, o Autoscale está desativado para grupos de entrega. Para gerenciar o Autoscale para um grupo de entrega (se aplicável), siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Manage Autoscale** na barra de ações. A janela **Manage Autoscale** é exibida.
3. Defina as configurações conforme necessário. Para obter informações sobre as configurações de Autoscale, consulte Autoscale.
4. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou selecione **Save** 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 da sessão e o prolongamento da sessão
- Configurar roaming de sessão
- Reconexão da sessão de controle quando desconectada da máquina no modo de manutenção

Fazer logoff ou desconectar uma sessão ou enviar uma mensagem aos usuários do grupo de entrega

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e selecione **View Machines** na barra de ações.
3. Para fazer logoff de um usuário de uma sessão, selecione a sessão ou a área de trabalho e, em seguida, selecione **Log off** na barra de ações. A sessão fecha e a máquina fica disponível para outros usuários, a menos que esteja alocada para um usuário específico.
4. Para desconectar uma sessão, selecione a sessão ou a área de trabalho e, em seguida, selecione **Disconnect** na barra de ações. Os aplicativos continuam sendo executados e a máquina permanece alocada para o usuário. O usuário pode se reconectar à mesma máquina.
5. Para enviar uma mensagem aos usuários, selecione a sessão, a máquina ou o usuário e, em seguida, selecione **Send message** na barra de ações. Digite a mensagem.

Configurar a pré-inicialização de sessão e o prolongamento de sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas com SO multissessão.

Os recursos de pré-inicialização de sessão e de prolongamento de sessão ajudam os usuários especificados a acessar aplicativos rapidamente, ao:

- Iniciar sessões antes de serem solicitadas (pré-inicialização da sessão)
- Manter as sessões do aplicativo ativas depois que um usuário fecha todos os aplicativos (prolongamento de sessão)

Por padrão, a pré-inicialização de sessão e o prolongamento de sessão não são usados. Uma sessão é inicializada quando o usuário inicia um aplicativo e permanece ativa até que o último aplicativo aberto na sessão seja fechado.

Considerações:

- O grupo de entrega deve oferecer suporte a aplicativos e as máquinas devem estar executando um VDA de SO multissessão, versão mínima 7.6.
- Esses recursos são compatíveis apenas ao usar o aplicativo Citrix Workspace para Windows e também exigem mais configuração do aplicativo Citrix Workspace. Para obter instruções, procure por pré-inicialização de sessão na documentação do produto para a sua versão do aplicativo Citrix Workspace para Windows.
- O aplicativo Citrix Workspace para HTML5 não é suportado.
- Ao usar a pré-inicialização de sessão, se a máquina de um usuário for colocada no modo suspender ou hibernar, a pré-inicialização não funciona (independentemente das configurações de pré-inicialização da sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário fizer logoff do aplicativo Citrix Workspace, a sessão será encerrada e a pré-inicialização não se aplica mais.
- Ao usar a pré-inicialização de sessão, as máquinas cliente físicas não podem usar as funções de gerenciamento de energia suspender ou hibernar. Usuários de máquinas cliente podem bloquear suas sessões, mas não devem fazer logoff.
- Sessões pré-inicializadas e prolongadas consomem uma licença simultânea, mas somente quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. As sessões pré-inicializadas e prolongadas não utilizadas se desconectam após 15 minutos por padrão. Esse valor pode ser configurado no PowerShell (cmdlet `New`/`Set-BrokerSessionPreLaunch`).
- O planejamento e monitoramento minuciosos dos padrões de atividade de seus usuários são essenciais para adaptar esses recursos para complementarem uns aos outros. A configuração ideal equilibra os benefícios da disponibilidade mais rápida de aplicativos para os usuários em relação ao custo de manter as licenças em uso e os recursos alocados.
- Você também pode configurar a pré-inicialização da sessão para um horário agendado do dia no aplicativo Citrix Workspace.

Quanto tempo as sessões pré-inicializadas e prolongadas não utilizadas permanecem ativas
Existem várias maneiras de especificar 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 termine.

- **Tempo limite:** um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-inicializada ou prolongada não utilizada permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-inicializadas terminarão antes que ofereçam ao usuário o benefício do acesso rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário recebidas poderão ser negadas porque o servidor não tem recursos suficientes.

  Você pode ativar o tempo limite somente a partir do SDK (cmdlet `New`/`Set-BrokerSessionPreLaunch`), não do console de gerenciamento. Se você desativar o tempo limite, ele não aparecerá na exibição do console do grupo de entrega ou nas páginas **Edit Delivery Group**.

- **Limites:** o encerramento automático de sessões pré-inicializadas e prolongadas com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, pressupondo-se que os recursos do servidor estejam disponíveis. Sessões pré-inicializadas e prolongadas não utilizadas não causam conexões negadas porque elas são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

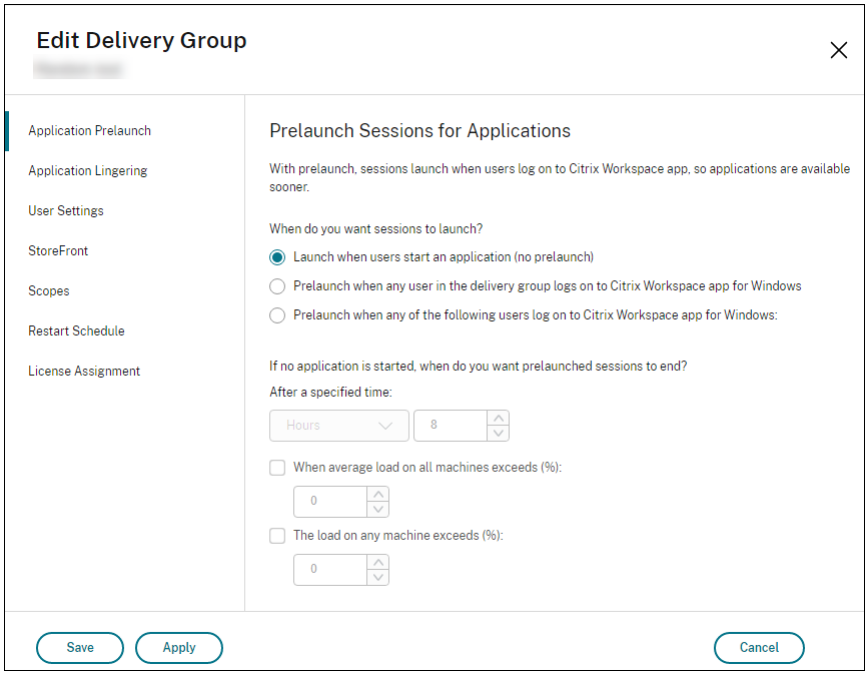
  Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-inicialização ou prolongada por mais tempo são encerradas. As sessões são encerradas uma por uma em intervalos de minutos até que a carga caia abaixo do limite. Enquanto o limite for excedido, nenhuma nova sessão de pré-inicialização será iniciada.

Os servidores com VDAs que não se registraram no Controller e os servidores no modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-inicialização e prolongadas terminem automaticamente para liberar capacidade.

Para ativar a pré-inicialização da sessão

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Application Prelaunch**, ative a pré-inicialização da sessão escolhendo quando as sessões são iniciadas:
   - Quando um usuário inicia um aplicativo. Essa é a configuração padrão. A pré-inicialização da sessão está desativada.

- Quando um usuário no grupo de entrega faz logon no aplicativo Citrix Workspace para Windows.
- Quando uma pessoa em uma lista de usuários e grupos de usuários faz logon no aplicativo Citrix Workspace para Windows. Certifique-se de especificar também usuários ou grupos de usuários se escolher essa opção.



4. Uma sessão pré-inicializada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-inicializada não for utilizada), as configurações a seguir afetarão quanto tempo a sessão permanece ativa.

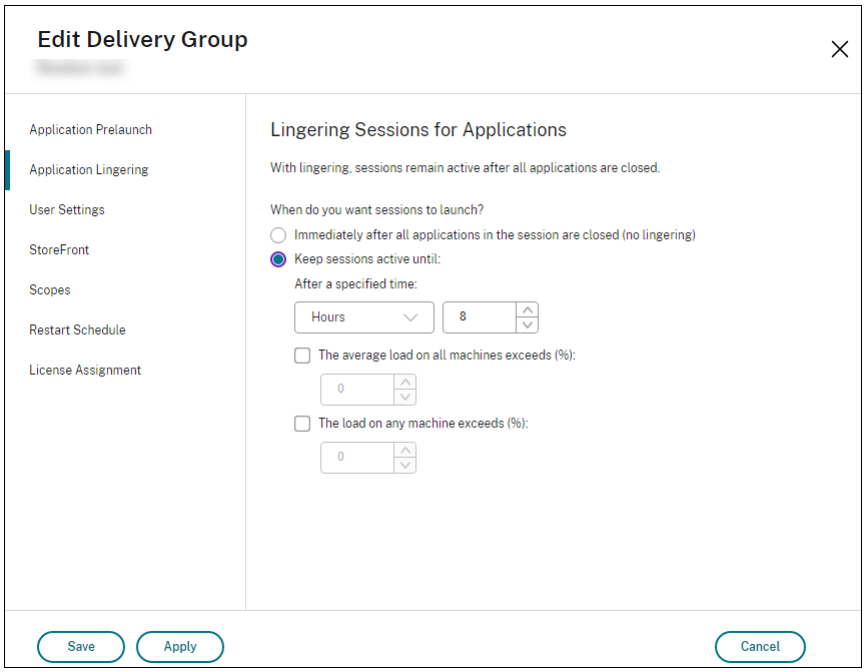
   - Quando um intervalo de tempo especificado se esgotar. Você pode alterar o intervalo de tempo (1—99 dias, 1—2376 horas ou 1—142.560 minutos).
   - Quando a carga média em todas as máquinas no grupo de entrega exceder uma porcentagem especificada (1—99%).
   - Quando a carga em qualquer máquina no grupo de entrega exceder uma porcentagem especificada (1—99%).

   Recapitulando, uma sessão pré-inicializada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado se esgota ou um limite de carga especificado é excedido.

Para ativar o prolongamento de sessão

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.

3. Na página **Application Lingering**, ative a o prolongamento da sessão selecionando **Keep sessions active until**.



4. Várias configurações afetam quanto tempo uma sessão prolongada permanece ativa se o usuário não iniciar outro aplicativo.

   - Quando um intervalo de tempo especificado se esgotar. 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 exceder uma porcentagem especificada: 1—99%.
   - Quando a carga em qualquer máquina no grupo de entrega exceder uma porcentagem especificada: 1—99%.

   Recapitulando, uma sessão prolongada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado se esgota ou um limite de carga especificado é excedido.

Configurar roaming de sessão

Por padrão, o roaming de sessão está habilitado para grupos de entrega. As sessões se movem 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 disponíveis nos dois dispositivos simultaneamente. Você pode exibir os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo, ou se existem ou não sessões atuais. Muitas vezes, as impressoras e outros recursos atribuídos ao aplicativo também seguem. Como alternativa, você também pode usar o PowerShell. Para obter mais informações, consulte Roaming de sessão.

Configurar roaming de sessão para aplicativos Para configurar o roaming de sessão para aplicativos, siga estas etapas:

1. Em **Manage > Full Configuration**, 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**, ative o roaming de sessão marcando a caixa de seleção **Sessions roam with users as they move between devices**.
   - Quando ativada, se um usuário iniciar uma sessão de aplicativo e depois se mover para outro dispositivo, a mesma sessão será usada e ficará disponível nos dois dispositivos. Quando desativada, a sessão não fará mais o roaming entre dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

Configurar o roaming de sessão para áreas de trabalho Para configurar o roaming de sessão para uma área de trabalho, siga estas etapas:

1. Em **Manage > Full Configuration**, 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 a área de trabalho e selecione **Edit**.
4. Ative o roaming de sessão marcando a caixa de seleção **Session roaming**.
   - Quando ativada, se o usuário iniciar uma área de trabalho e depois se mover para outro dispositivo, a mesma sessão é usada e os aplicativos ficam disponíveis nos dois dispositivos. Quando desativada, a sessão não fará mais o roaming entre dispositivos.
5. Selecione **OK** para aplicar as alterações e fechar a janela.

Reconexão da sessão de controle quando desconectada da máquina no modo de manutenção

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

Você pode controlar se as sessões desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes do fim de maio de 2021, a reconexão não era permitida para sessões de desktop em pool de sessão única que tinham desconectado das máquinas no modo de manutenção. Agora você pode configurar um grupo de entrega para permitir ou proibir reconexões (independentemente do tipo VDA) após a desconexão de uma máquina no modo de manutenção.

Ao criar ou editar um grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use o `-AllowReconnectInMaintenanceMode <boolean>` parâmetro para permitir ou proibir reconexões para máquinas que foram desconectadas de uma máquina no modo de manutenção.

- Quando definido como true, as sessões podem se reconectar a máquinas no grupo.
- Quando definido como false, as sessões não podem se reconectar a máquinas no grupo.

Valores padrão:

- Sessão única: Desativado
- Multissessão: Ativado

Solução de problemas

- Os VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização dos recursos disponíveis. Há várias razões para que um VDA não possa ser registrado, muitas das quais um administrador pode resolver. A exibição de detalhes fornece informações sobre solução de problemas no assistente de criação de catálogo e depois de adicionar 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 que não estão. Por exemplo, uma ou mais máquinas estão ligadas e não estão no modo de manutenção, mas, no momento, não estão registradas em um Controller. Ao visualizar uma máquina "não registrada, mas que deveria estar", consulte a guia **Troubleshoot** no painel de detalhes para ver as possíveis causas e as ações corretivas recomendadas.

  Para mensagens sobre o nível funcional, consulte Versões e níveis funcionais do VDA.

  Para obter informações sobre a solução de problemas de registro VDA, consulte CTX136668.

- Na exibição de um grupo de entrega, a **versão instalada do VDA** no painel de detalhes pode diferir da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.

- Para máquinas que apresentam o status **Power State Unknown**, consulte CTX131267 para obter instruções.

Criar grupos de aplicativos

August 17, 2023

Introdução

Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos que são 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. 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.

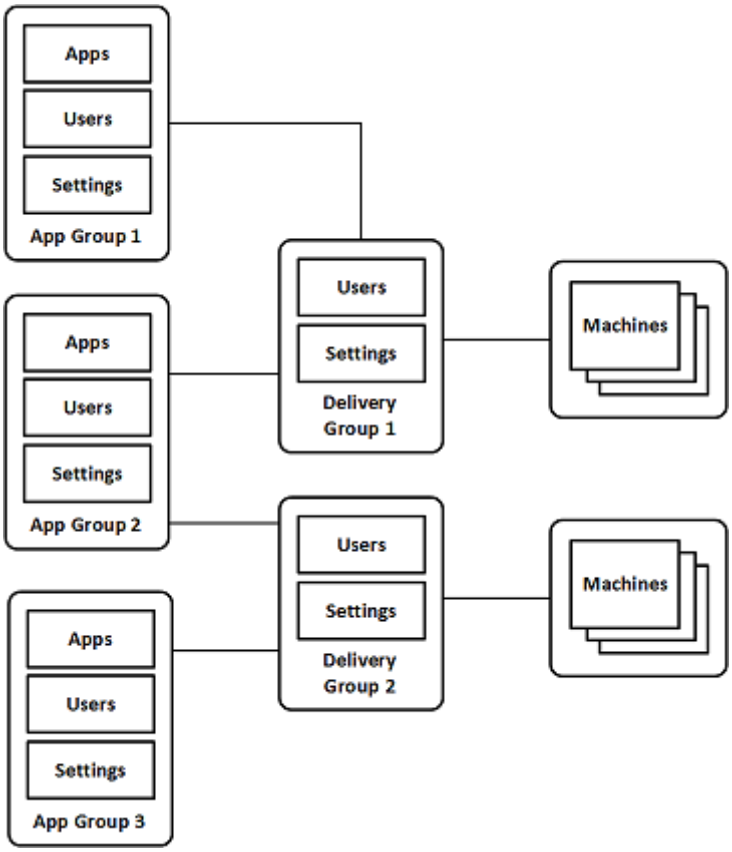
Usar grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em comparação com o uso de mais grupos de entrega:

- 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 de cada vez.
- O compartilhamento de sessão entre grupos de aplicativos pode economizar no consumo de recursos. Em outros casos, desativar o compartilhamento de sessões entre grupos de aplicativos pode ser benéfico.
- Você pode usar o recurso de restrição de marca para publicar aplicativos a partir de um grupo de aplicativos, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Com as restrições de marcas, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando nos custos associados com a implantação e gerenciamento de máquinas adicionais. Uma restrição de marca pode ser considerada como uma subdivisão (ou partição) de máquinas em um grupo de entrega. Usar um grupo de aplicativos ou áreas de trabalho com restrição de marca pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Exemplo de configurações

Exemplo 1

O gráfico a seguir mostra uma implantação que inclui grupos de aplicativos:



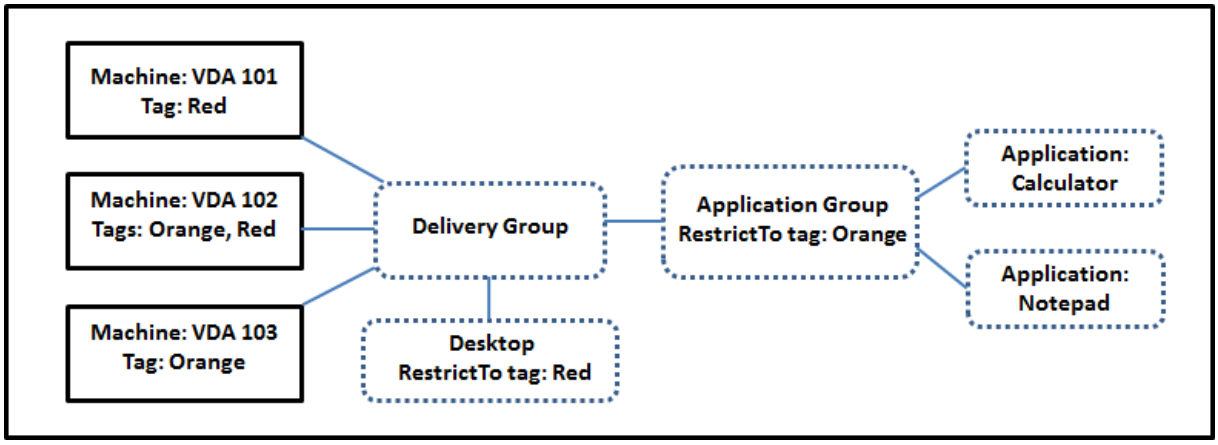
Nesta configuração, os aplicativos são adicionados aos grupos de aplicativos, não aos grupos de entrega. Os grupos de entrega especificam quais máquinas serão usadas. (Embora não sejam mostradas, as máquinas estão em catálogos de máquinas.)

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 de um grupo de aplicativos deveria ser um subconjunto (uma restrição) das listas de usuários dos grupos de entrega associados. As configurações no grupo de aplicativos 1 (como o compartilhamento de sessão de aplicativos entre grupos de aplicativos, grupos de entrega associados) se aplicam a aplicativos e usuários no grupo. As configurações no grupo de entrega 1 (tal como suporte de usuário anônimo) se aplicam aos usuários nos grupos de aplicativos 1 e 2, porque esses grupos de aplicativos foram associados ao 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, que indica a ordem na qual os grupos de entrega serão verificados quando um aplicativo for iniciado. Os grupos de entrega com prioridade igual têm balanceamento de 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 as restrições de marca para limitar quais máquinas serão consideradas para determinadas inicializações de área de trabalho e aplicativo. O site tem um grupo de entrega compartilhado, uma área de trabalho publicada e um grupo de aplicativos configurado com dois aplicativos.



As marcas forem adicionadas a cada uma das três máquinas (VDA 101-103).

O grupo de aplicativos foi criado com a restrição de marca "Orange", de modo que cada um de seus aplicativos (Calculadora e Bloco de Notas) só pode ser iniciado em máquinas desse grupo de entrega que tenham a marca "Orange": VDA 102 e 103.

Para obter exemplos e orientações mais abrangentes sobre o uso de restrições de marcas em grupos de aplicativos (e áreas de trabalho), 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 está ativado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Veja Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativos entre grupos de aplicativos está ativado. Veja Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. Isso requer:

1. Atualização dos VDAs nas máquinas usadas no grupo de entrega.
2. Mudança para um nível de função mais alto dos catálogos de máquinas que contêm essas máquinas

3. Mudança para um nível de função mais alto do grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ter a versão mínima 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna Administrador do Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo se refere a "associar"um aplicativo a mais de um grupo de aplicativos para diferenciar essa ação de adicionar uma nova instância desse aplicativo de uma fonte disponível. Da mesma forma, os grupos de entrega estão associados a grupos de aplicativos (e vice-versa), em vez de serem adições ou componentes um do outro.

Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão do aplicativo está ativado, todos os aplicativos são iniciados na mesma sessão do aplicativo. Isso economiza os custos associados com a inicialização de sessões de aplicativos adicionais e permite o uso de recursos do 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 sessões.

Quando você usa 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 quando você está usando apenas grupos de entrega:

- Compartilhamento de sessão ativado entre grupos de aplicativos.
- Compartilhamento de sessão ativado somente entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desativado.

Compartilhamento de sessão entre grupos de aplicativos

Você pode ativar o compartilhamento de sessão de aplicativo entre grupos de aplicativos ou desativá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo da utilidade de ativar o compartilhamento de sessão entre grupos de aplicativos:**

  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 são anexados ao mesmo grupo de entrega. Um usuário que tem acesso aos dois grupos de aplicativos inicia uma sessão de aplicativo iniciando o Word e, em seguida,

inicia o Bloco de Notas. Se a sessão existente do usuário executando o Word é 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 marca 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 da utilidade de desativar o compartilhamento de sessão entre grupos de aplicativos:**

  Você tem um conjunto de aplicativos que não interoperam bem com outros aplicativos instalados nas mesmas máquinas, como duas versões diferentes do mesmo pacote de software ou duas versões diferentes do mesmo navegador da web. Você vai preferir não permitir que um usuário inicie ambas as versões na mesma sessão.

  Você cria um grupo de aplicativos para cada versão do pacote de software e adicione os aplicativos para cada versão do pacote de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desativado 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 com versões diferentes (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.

Esse recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de área restrita de segurança. Não é infalível e tampouco pode impedir que os usuários iniciem aplicativos em suas sessões através de outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver na capacidade máxima, não serão iniciadas novas sessões 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 têm o compartilhamento de sessão de aplicativos permitido. (As sessões que usam o recurso de prolongamento de sessão estão disponíveis para todos os grupos de aplicativos.) Esses recursos devem ser ativados e configurados em cada um dos grupos de entrega associados ao grupo de aplicativos. Não é possível configurá-los nos grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativos entre grupos de aplicativos é ativado 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. Veja Gerenciar grupos de aplicativos.

Desativar o compartilhamento de sessão em um grupo de aplicativos

Você pode impedir o compartilhamento de sessão do aplicativo entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo da utilidade de desativar o compartilhamento de sessão em grupos de aplicativos:**

  Você deseja que seus usuários acessem várias sessões simultâneas de um aplicativo em tela cheia 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 nele especificado iniciar um aplicativo após o outro, eles são iniciados em sessões separadas e o usuário pode mover cada um deles para um monitor separado.

Por padrão, o compartilhamento de sessão de aplicativos é ativado 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. Veja 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 aplicativo Citrix Workspace. As categorias de aplicativos permitem gerenciar coleções de aplicativos no Citrix Workspace.

Para criar um grupo de aplicativos:

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Para organizar grupos de aplicativos usando pastas, crie pastas na pasta raiz **Application Groups**.
3. Selecione a pasta na qual deseja criar o grupo e clique em **Create Application Group**. O assistente de criação de grupos é iniciado com uma página de **introdução**. Você pode remover essa página das inicializações futuras do assistente.
4. Siga o assistente para definir as configurações nas páginas descritas abaixo. Quando terminar cada página, selecione **Next** até chegar à página **Summary**.

Etapa 1. Grupos de entrega

A página **Delivery Groups** lista todos os grupos de entrega, com o número de máquinas que cada grupo contém.

- A lista **Compatible Delivery Groups** contém grupos de entrega que você pode selecionar. Grupos de entrega compatíveis contêm máquinas com SO de área de trabalho ou servidor aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Incompatible Delivery Groups** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como, por exemplo, por conter máquinas atribuídas estáticas.

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 somente áreas de trabalho, se as duas condições a seguir forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.
- Você tem a permissão Edit Delivery Group

O tipo de grupo de entrega é automaticamente convertido em "áreas de trabalho e aplicativos" quando o assistente de criação do 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 no momento), o grupo de aplicativos não pode ser usado para entregar aplicativos até especificar pelo menos um grupo de entrega. Além disso, você não pode adicionar aplicativos ao grupo de aplicativos a partir da origem do menu **From Start** se não houver grupos de entrega especificados.

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 deseja associar com o grupo de aplicativos.

Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca na lista suspensa.

Etapa 2. Usuários

Especifique quem pode usar os aplicativos no grupo de aplicativos. Você pode dar permissão a todos os usuários e grupos de usuários nos grupos de entrega selecionados na página anterior ou selecionar os usuários e grupos de usuários específicos desses grupos de entrega. Se você restringir o uso a usuários que especificar, somente os usuários especificados no grupo de entrega e o grupo de aplicativos podem acessar os aplicativos nesse grupo de aplicativos. Essencialmente, a lista de usuários no grupo de aplicativos fornece um filtro nas listas de usuários nos grupos de entrega.

A ativação ou desativação do uso do aplicativo por usuários não autenticados está disponível somente 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 adicionados são colocados em uma pasta chamada **Applications**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e já existir outro com o mesmo nome na pasta, você será solicitado a renomear 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 para 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. Veja Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Application name (for user)** no Studio na interface de gerenciamento Full Configuration. 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 exibir o aplicativo em todos os grupos. Nesses casos, consulte um administrador com mais permissões ou estenda o seu escopo para incluir todos os grupos aos quais o aplicativo foi adicionado.

Selecione o menu suspenso **Add** para exibir as origens do aplicativo.

- **From Start menu:** aplicativos que são detectados em uma máquina nos grupos de entrega selecionados. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas de seleção dos aplicativos a serem adicionados e selecione **OK**.

  Essa origem não pode ser selecionada se você selecionou 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.

- **Manually defined:** aplicativos localizados no site ou em outro lugar na sua rede. Quando você seleciona essa origem, uma nova página é iniciada 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**.

- **Existing**: aplicativos adicionados anteriormente ao site. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas

de seleção dos aplicativos a serem adicionados e selecione **OK**. Essa origem não pode ser selecionada se o site não tiver aplicativos.

- **App-V**: aplicativos em pacotes App-V. Quando você seleciona essa origem, uma nova página é iniciada onde você seleciona **App-V Server** ou **Application Library**. Na exibição resultante, marque as caixas de seleção dos aplicativos a serem adicionados e selecione **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V. Esta origem não pode ser selecionada (ou pode não aparecer) se o App-V não estiver configurado para o site.

  > **Nota:**
  >
  > No VDA versão 2003 e posterior, a publicação de pacotes App-V a partir de URLs HTTP não é suportada. Você não pode selecionar esses aplicativos na lista.

Como observado, certas entradas no menu suspenso **Add** não serão selecionáveis se não houver uma origem válida desse tipo. As origens incompatíveis não são listadas (por exemplo, não é possível adicionar grupos de aplicativos a grupos de aplicativos, de modo que a origem não é listada quando você cria um grupo de aplicativos).

Etapa 4. Escopos

Esta página só aparece se você tiver criado anteriormente um escopo personalizado. Por padrão, o escopo **All** 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 selecione **Finish**.

Gerenciar grupos de aplicativos

January 27, 2023

Introdução

Este artigo descreve como gerenciar os grupos de aplicativos que você criou.

Consulte Aplicativos para obter informações sobre o gerenciamento de aplicativos em grupos de aplicativos ou grupos de entrega, incluindo como:

- Adicionar ou remover aplicativos em um grupo de aplicativos.
- Alterar associações de grupos de aplicativos.

O gerenciamento de grupos de aplicativos requer as permissões de administrador delegado da função interna Delivery Group Administrator. Para obter detalhes, consulte Administração delegada.

Ativar ou desativar um grupo de aplicativos

Quando um grupo de aplicativos está ativado, ele pode entregar os aplicativos que foram adicionados a ele. A desativação de um grupo de aplicativos desativa cada aplicativo naquele grupo. No entanto, se esses aplicativos também estiverem associados a outros grupos de aplicativos ativados, eles poderão ser entregues a partir desses outros grupos. Do mesmo modo, se o aplicativo foi explicitamente adicionado aos grupos de entrega associados ao grupo de aplicativos (além de ser adicionado ao grupo de aplicativos), a desativação do grupo de aplicativos não afetará os aplicativos nesses grupos de entrega.

Um grupo de aplicativos é ativado quando você o cria. Você não pode alterar isso ao criar o grupo.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Na página **Settings**, marque ou desmarque a caixa de seleção**Enable Application Group**.
4. Selecione **Apply** 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 compartilhamento de sessão do aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é ativado 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. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Na página **Settings**, marque ou desmarque a caixa de seleção **Enable application session sharing between Application Groups**.
4. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Desativar o compartilhamento de sessão do aplicativo em um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é ativado por padrão quando você cria um grupo de aplicativos. Se você desativar o compartilhamento de sessão do aplicativo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanece ativado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão do aplicativo desativado entre os aplicativos que eles contêm. Em algumas circunstâncias, isso pode ser desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não integrados em janelas de aplicativos em tamanho real em monitores separados.

Quando você desativa o compartilhamento de sessão do aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão do aplicativo. Se uma sessão desconectada adequada estiver disponível, e que esteja 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 é reconectada, em vez de uma nova ser criada. Se várias sessões desconectadas adequadas estão disponíveis, uma das sessões é escolhida para a reconexão, de forma aleatória, mas determinística. Se a situação ocorre novamente nas mesmas circunstâncias, a mesma sessão é escolhida, mas a sessão não é necessariamente previsível de outra forma.

Você pode usar o SDK do PowerShell para desativar o compartilhamento de sessão do aplicativo para todos os aplicativos em um grupo de aplicativos existente ou para criar um grupo de aplicativos com compartilhamento de sessão do aplicativo desativado.

Exemplos de cmdlet do PowerShell

Para desabilitar o compartilhamento de sessão, use os cmdlets New-BrokerApplicationGroup ou Set-BrokerApplicationGroup do Broker PowerShell com o parâmetro SessionSharingEnabled definido como False e o parâmetro SingleAppPerSession definido como True.

- Por exemplo, para criar um grupo de aplicativos com compartilhamento de sessão do aplicativo desativado para todos os aplicativos do grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -
  SingleAppPerSession $True
  ```

- Por exemplo, para desativar o compartilhamento de sessão do aplicativo entre todos os aplicativos em um grupo de aplicativos existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -
  SingleAppPerSession $True
  ```


Considerações

- Para ativar a propriedade `SingleAppPerSession` você deve definir a propriedade `SessionSharingEnabled` como False. As duas propriedades não devem ser ativadas ao mesmo tempo. O parâmetro `SessionSharingEnabled` refere-se ao compartilhamento de sessões entre grupos de aplicativos.
- O compartilhamento de sessão do aplicativo funciona apenas para aplicativos associados a grupos de aplicativos, mas que não estão associados a grupos de entrega. Todos os aplicativos que estão associados diretamente a um grupo de entrega compartilham sessões por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, verifique se os grupos não têm configurações conflitantes. Por exemplo, um grupo com a opção definida como True e outro grupo com a opção definida como False resulta em um comportamento imprevisível.

Renomear um grupo de aplicativos

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Rename Application Group** na barra de ações.
3. Especifique o novo nome exclusivo e selecione **OK**.

Adicionar, remover ou alterar a prioridade das associações de grupos 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 somente áreas de trabalho, se as duas condições a seguir forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão anterior a 7.9.
- Você tem a permissão Edit Delivery Group

O tipo de grupo de entrega é automaticamente convertido em "áreas de trabalho e aplicativos" quando a caixa de diálogo **Edit Application Group** é confirmada.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.

3. Selecione a página **Delivery Groups**.
4. Para adicionar grupos de entrega, selecione **Add**. Marque as caixas de seleção dos grupos de entrega disponíveis. (Grupos de entrega incompatíveis não podem ser selecionados.) Quando terminar suas seleções, selecione **OK**.
5. Para remover grupos de entrega, marque as caixas de seleção dos grupos que deseja remover e selecione **Remove**. Confirme a exclusão quando solicitado.
6. Para alterar a prioridade dos grupos de entrega, marque a caixa de seleção do grupo de entrega e selecione **Edit Priority**. Digite a prioridade (0 = mais alta) e selecione **OK**.
7. Selecione **Apply** 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 marca em um grupo de aplicativos

Adicionar, alterar e remover restrições de marca pode ter efeitos imprevisíveis sobre quais máquinas são consideradas para a inicialização do aplicativo. Consulte as considerações e precauções em Marcas.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Delivery Groups**.
4. Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca no menu.
5. Para alterar ou remover uma restrição de marca, selecione uma marca diferente no menu ou remova a restrição de marca desmarcando **Restrict launches to machines with this tag**.
6. Selecione **Apply** 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. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Users**. Indique se deseja permitir que todos os usuários nos grupos de entrega associados usem aplicativos no grupo de aplicativos ou apenas usuários e grupos especí-

ficos. Para adicionar usuários, selecione **Add** e, em seguida, especifique os usuários que deseja adicionar. Para remover usuários, selecione um ou mais usuários e selecione **Remove**.

4. Selecione **Apply** 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 etapas a seguir para adicionar, alterar ou remover um ícone de aplicativo.

1. No painel de navegação, selecione **Applications**.
2. Na guia **All Applications**, selecione um aplicativo e, em seguida, selecione **Properties**.

   Para fazer alterações no nível de um grupo de aplicativos, navegue para a guia **Application Groups**, selecione um aplicativo em um grupo e selecione **Properties**.
3. Selecione a página **Delivery** e, em seguida, selecione **Change**. A janela **Select Icon** é exibida.
4. Na janela **Select Icon**, siga um destes procedimentos:

   - Para adicionar um ícone, selecione **Add** e, em seguida, navegue até o ícone.
   - Para remover um ícone, selecione-o e selecione **Remove**.
   - Para alterar um ícone, selecione-o para o aplicativo.

   > **Importante:**
   >
   > - Não é possível adicionar um ícone cujo tamanho seja maior que 200 KB.
   > - Você pode adicionar apenas arquivos .icon.
   > - Você não pode remover ícones internos.
   > - Não é possível remover um ícone de um aplicativo que está em uso.

5. Selecione **OK** para aplicar as alterações e fechar a janela.

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (não é possível editar o escopo All). Para obter mais informações, consulte Administração delegada.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Scopes**. Marque ou desmarque a caixa de seleção ao lado dos escopos que você deseja alterar.

4. Selecione **Apply** 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 fará com que um ou mais aplicativos não mais pertençam a um grupo, você será avisado de que a exclusão do grupo também excluirá os aplicativos. Você pode então confirmar ou cancelar a exclusão.

A exclusão de um aplicativo não o exclui de seu local de origem. No entanto, se quiser torná-lo disponível novamente, você deve adicioná-lo novamente.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Delete Group** 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 e facilitar o acesso.

Funções necessárias

Por padrão, você precisa ter uma das seguintes funções internas para criar e gerenciar pastas para grupos de aplicativos:

- Cloud Administrator
- Full Administrator
- Application Group Administrator

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 grupos de aplicativos	Create Application Group Folder
Excluir pastas de grupos de aplicativos	Remove Application Group Folder
Mover pastas de grupos de aplicativos	Move Application Group Folder
Renomear pastas de grupos de aplicativos	Edit Application Group Folder

Ação	Permissões necessárias
Mover grupos de aplicativos para pastas	Edit Application Group Folder, Edit Application Group Properties

Para obter mais informações, consulte Criar e gerenciar funções.

Cria e gerenciar pastas

Você pode usar a barra Actions ou o menu ativado pelo botão direito do mouse para criar e gerenciar pastas de grupos de aplicativos. Você também pode arrastar um grupo de aplicativos ou uma pasta para o local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas com até cinco níveis (excluindo a pasta raiz 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 recursos em Full Configuration (como catálogos de máquinas, grupos de entrega, aplicativos e grupos de aplicativos) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outras pastas de recursos ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nas diferentes árvores de pastas.

Remote PC Access

July 28, 2023

> **Nota:**
>
> Este artigo descreve como configurar o acesso remoto ao PC usando a interface Full Configuration. Se você estiver usando a interface Quick Deploy, siga as orientações em Acesso remoto ao PC no Quick Deploy.

O Remote PC Access é um recurso do Citrix Virtual Apps and Desktops que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos

os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

O Remote PC Access usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam áreas de trabalho e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos que os necessários para implantar o Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

O recurso consiste em um catálogo de máquinas do tipo **Remote PC Access** que proporciona a seguinte funcionalidade:

- Capacidade de adicionar máquinas especificando unidades organizacionais. 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 do usuário com base no usuário que faz login no PC Windows do escritório. Oferecemos suporte a atribuições de usuário único e multiusuário. Por padrão, o Citrix DaaS atribui automaticamente vários usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, navegue até **Full Configuration > Settings** e desative a configuração **Enable automatic assignment of multiple users for Remote PC Access**.

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 físicos Linux
- PCs físicos em pool (isto é, aleatoriamente atribuídos, não dedicados)

> **Observações:**
>
> Para obter detalhes sobre as versões do SO com suporte, consulte os requisitos do sistema para o VDA para SO de sessão única e Linux VDA.
>
> Para implantações locais, o Remote PC Access é válido apenas para licenças do Citrix DaaS Advanced ou Premium. As sessões consomem licenças da mesma maneira que outras sessões do Citrix Virtual Desktops. Para o Citrix Cloud, o acesso remoto ao PC é válido para Citrix DaaS e Workspace Premium Plus.

Considerações

Embora todos os requisitos e considerações técnicas que se aplicam ao Citrix Virtual Apps and Desktops e Citrix DaaS em geral também se apliquem ao Remote PC Access, alguns podem ser mais rele-

vantes ou exclusivos para casos de uso de PC físico.

> **Importante:**
>
> Os sistemas físicos do Windows 11 (e alguns que executam o Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software do 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 da linha de comando do VDA
> - Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada acima não tenha sido usada
> `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - Nome: ForceEnableRemotePC
> - Tipo: DWORD
> - Dados: 1

Considerações sobre implantação

Ao planejar a implantação do Remote PC Access, adote algumas medidas gerais.

- Você pode adicionar o Remote PC Access a uma implantação existente do Citrix Virtual Apps and Desktops e Citrix DaaS. Antes de escolher essa opção, considere o seguinte:
  - Os Delivery Controllers ou os Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os bancos de dados locais do site e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os VDAs existentes e os novos VDAs do Remote PC Access ultrapassam o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs no escritório por meio de um processo automatizado. A seguir estão as duas opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instale VDAs usando SCCM.
  - Scripts de implantação: Instale VDAs usando scripts.
- Veja as Considerações de segurança do Remote PC Access.

Considerações do catálogo de máquinas

O tipo de catálogo de máquinas exigido depende do caso de uso:

- Catálogo de máquinas de Remote PC Access
  - PCs Windows/Linux dedicados
  - PCs Windows/Linux multiusuário dedicados Esse caso de uso se aplica a PCs físicos de escritório que vários usuários podem acessar remotamente em turnos diferentes.
  - PCs Windows/Linux em pool. Esse 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 em que as contas da máquina residem, selecione UOs de nível inferior para obter maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de bancos/caixas/guichês, selecione **Tellers** para obter maior granularidade. Caso contrário, você pode selecionar **Officers** ou **Bank** baseado nas exigências.
- Mover ou excluir UOs depois de atribuídas a um catálogo de máquinas de Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Portanto, tenha o cuidado de planejar adequadamente para que as atualizações de atribuição da unidade organizacional a catálogos de máquina sejam contabilizadas 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 às restrições da estrutura da 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.
- Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Remote PC Access**.

Considerações do Linux VDA

Estas considerações são específicas para o Linux VDA:

- Physical monitor blanking for Remote PC Access VDAs está disponível, mas não para todas as distribuições Linux. Para as distribuições Linux não suportadas, use o Linux VDA em máquinas físicas somente no modo não 3D. Caso contrário, 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.

- Recomendamos que você use catálogos de máquina do tipo SO de sessão única para máquinas físicas Linux.

Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e as considerações para PCs físicos.

- Não há suporte para:
  - Chaveadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo notebooks e PCs All-in-One e NVIDIA Optimus.
  - Máquinas de inicialização dupla.
- Conecte o teclado e o mouse diretamente ao PC. 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.
- Os PCs devem ser ingressados em um domínio do Active Directory Domain Services
- A inicialização segura é suportada apenas no Windows 10.
- O PC 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, faça o seguinte:
  1. Defina as configurações de energia para deixar o adaptador sem fio ligado.
  2. 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. O PC não está disponível para acesso remoto até que um usuário tenha feito logon.
  3. Certifique-se de que os Delivery Controllers ou os Cloud Connectors possam ser acessados da rede Wi-Fi.
- Você pode usar o Remote PC Access em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:
  1. Desative o recurso de hibernação.
  2. Desative o recurso de suspensão.
  3. Defina a ação de fechar a tampa como **Não fazer nada**.

4. Defina a ação “pressionar o botão de energia”como **Desligar**.
5. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Remote PC Access é suportado em dispositivos Surface Pro com Windows 10. Siga as mesmas instruções para laptops mencionadas anteriormente.
- Se estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixa o laptop, o VDA se registra novamente nos Delivery Controllers ou 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. Os 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.

  Faça o seguinte para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

  1. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão**, e defina **Suspender** como **Nunca**.
  2. 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.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, o recurso aparece como indisponível se já estiver sendo usado 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 Remote PC Access ao usar o catálogo da máquinas do tipo **Remote PC Access**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquina.

1. Somente site local –Para usar o recurso Wake on LAN integrado, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para o Remote PC Access:

   a) Selecione o tipo de site **Remote PC Access**.

b) Em **Power Management**, escolha se deseja ativar ou desabilitar o gerenciamento de energia para o catálogo de máquinas Remote PC Access. 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) Forneça as informações nas páginas **Users** e **Machine Accounts**

Ao concluir essas etapas, é criado um catálogo de máquinas chamado **Remote PC Access Machines** e um grupo de entrega chamado **Remote PC Access Desktops**.

3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a) Crie um catálogo de máquinas do tipo **Remote PC Access** (página Operating System do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Tenha o cuidado de atribuir a unidade organizacional correta para que os PCs de destino sejam disponibilizados para uso com o Remote PC Access.
   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 Create delivery groups. Tenha o cuidado de atribuir o grupo de entrega a um grupo do Active Directory que contém os usuários que exigem acesso a seus PCs.

4. Implantar o VDA nos PCs do escritório.

   - Recomendamos usar o instalador VDA do núcleo do SO de sessão única (`VDAWorkstationCoreSetu .exe`).
   - Você também pode usar o instalador de VDA completo de sessão única (`VDAWorkstationSetup .exe`) com a opção `/remotepc /physicalmachine`, que chega ao mesmo resultado que o uso do instalador de VDA básico.
   - Ative a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto por meio do Citrix Director. Para 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 de VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Para incluir esse componente, use 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 SCCM.
   - Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

Depois que você concluir com êxito as etapas 2 a 4, os usuários são atribuídos automaticamente às suas próprias máquinas quando fazem logon localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente usado 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 com suporte.

Recursos gerenciados através do registro

> **Cuidado:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina Remote PC Access entre em um estado de suspensão, adicione a configuração de registro ao VDA e reinicialize a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra no modo de suspensão depois que o timer pré-configurado de inatividade expira. Depois que a máquina acorda, ela se registra novamente no Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dados: 1

Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é desconectada automaticamente quando um usuário local inicia uma sessão na máquina (pressionando CTRL+ATL+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e reinicialize a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Dados: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é confirmada dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dados:
  - 1 - O usuário remoto sempre tem prioridade se não responder à mensagem na interface do usuário dentro do período de tempo limite especificado. Esse comportamento é o padrão se esse parâmetro não estiver configurado.
  - 2 - O usuário local tem prioridade.

O tempo limite padrão para impor o modo Remote PC Access é de 30 segundos. Você pode configurar esse tempo limite, mas não o defina abaixo 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 do tempo limite em valores decimais

Quando um usuário quiser forçar o acesso ao console, o usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local da 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 no PC enquanto estiver em uso por um usuário remoto, o usuário remoto receberá uma mensagem. A mensagem pergunta se deve permitir ou negar a conexão do usuário local. Permitir que a conexão desconecta a sessão do usuário remoto.

Wake on LAN

O Remote PC Access suporta Wake on LAN, o que dá aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs no escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina for desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede em que o PC reside quando instruído pelo Delivery Controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura adicionais ou soluções de terceiros para a entrega dos pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN legado baseado em SCCM. O Wake on LAN integrado a SCCM é uma opção alternativa de Wake on LAN para Remote PC Access que só está disponível

com o Citrix Virtual Apps and Desktops local. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN —SCCM integrado.

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 sobre a capacidade de suporte, consulte os Requisitos do sistema para VDA.
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows

Configurar o Wake on LAN

Para configurar o Wake on LAN, você pode usar a interface de gerenciamento Full Configuration ou o PowerShell.

Configurar o Wake on LAN na interface Full Configuration Para criar a conexão Wake on LAN:

1. Navegue até o nó **Hosting** à esquerda.
2. Selecione **Add Connection and Resources**.
3. Na página **Connection** do assistente, forneça o seguinte:
   a) Tipo de conexão: PC remoto Wake on LAN
   b) Nome da zona: selecione a zona em que o catálogo de acesso remoto ao PC reside
   c) Nome da conexão: insira um nome para a conexão Wake on LAN.
4. Finalize as etapas restantes no assistente Add Connection and Resources.

Para adicionar a conexão Wake on LAN a um catálogo de máquinas do Remote PC Access:

1. Se você estiver criando um novo catálogo de máquinas de Acesso Remoto ao PC, poderá adicionar a conexão na página **Machine Type** do assistente Machine Catalog Setup usando a lista suspensa.

2. Se você quiser adicionar a conexão Wake on LAN a um catálogo de máquinas existente:

   a) Navegue até o nó **Machine Catalogs** à esquerda.
   b) Selecione o catálogo de máquinas do Remote PC Access apropriado.
   c) Clique com o botão direito do mouse no catálogo da máquina ou selecione o menu **More** acima.
   d) Selecione **Edit Machine Catalog**.
   e) Na página **Power Management**, selecione **Yes**.
   f) Selecione a conexão apropriada na lista suspensa.
   g) Selecione **Save**.

> **Nota:**
>
> A configuração do Wake on LAN por meio da interface Full Configuration está disponível apenas com o Citrix DaaS no momento.

Configurar o Wake on LAN por meio do PowerShell Para configurar o Wake on LAN por meio do PowerShell:

1. Crie o catálogo de máquinas Remote PC Access se ainda não tiver um.
2. Crie a conexão de host Wake on LAN se ainda não tiver uma.
3. Obtenha o identificador exclusivo da conexão de host Wake on LAN.
4. Associe a conexão de host Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host 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
 }

<!--NeedCopy-->
```

Quando a conexão do host estiver pronta, execute os seguintes comandos para obter o identificador exclusivo de conexão do host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Depois de obter o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo da máquinas do Remote PC Access:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

Considerações de design

Ao planejar o uso do Wake on LAN com Remote PC Access, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host Wake on LAN.
- Para que um PC acorde outro PC, os dois PCs devem estar na mesma sub-rede e usar a mesma conexão de host 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 a sua implantação contém mais de uma zona, você precisa de uma conexão de host Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Os pacotes mágicos são transmitidos usando o endereço de transmissão 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 conseguir acordar as máquinas nessa sub-rede.

Considerações operacionais

Veja as considerações a seguir 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 Wake on LAN integrado.
- Wake on LAN só pode ser usado para acordar PCs. Ele não suporta outras ações de energia, como reinicializar ou desligar.
- Os pacotes mágicos são enviados de uma destas duas maneiras:
  1. Quando um usuário tenta iniciar uma sessão no PC e o VDA não está registrado
  2. Quando um administrador envia manualmente um comando de ativação da interface Full Configuration ou do PowerShell
- Como o Delivery Controller não tem conhecimento do estado de energia de um PC, a interface Full Configuration exibe **Not Supported** no 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

Desligamento do monitor não funciona

Se o monitor local do PC Windows não for desligado enquanto houver uma sessão HDX ativa (o monitor local exibir 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 prioridade maior ao Citrix Indirect Display Driver (IDD) do que ao 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 obter mais detalhes sobre as prioridades do adaptador de exibição e criação de monitor, consulte o artigo CTX237608 do Knowledge Center.

A sessão desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão ativada

A notificação de gerenciamento de sessão controlada pelo valor do registro **SasNotification** funciona somente quando o modo Remote PC Access está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, 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 Remote PC Access são gravadas no log de Eventos de Aplicativos do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas, descartando-se as 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 do Remote PC Access estiver ativado, as transmissões direcionadas por sub-rede não iniciarão máquinas que estejam em uma sub-rede diferente daquela do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando transmissões direcionadas por sub-rede e o suporte AMT não estiver disponível, tente o método Wake-up proxy ou 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 sensível ao toque

Quando o VDA habilita o modo Remote PC Access, a máquina ignora a entrada local da tela sensível ao toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, 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

Veja a seguir outros recursos para Remote PC Access:

- Orientação sobre o projeto da solução: Remote PC Access Design Decisions
- Exemplos de arquiteturas do Remote PC Access: Reference Architecture for Citrix Remote PC Access Solution.

Remover componentes

February 23, 2023

Para remover componentes que você instalou (como VDAs), a Citrix recomenda o uso do recurso Windows para remover ou alterar programas. Como alternativa, você pode remover componentes usando a linha de comando ou um script.

Quando você remove componentes, os pré-requisitos não são removidos e as configurações de firewall não são alteradas.

Quando você remove um VDA, a máquina reinicia automaticamente após a remoção, por padrão.

Remover componentes usando o recurso Windows para remover ou alterar programas

Usando o recurso Windows para remover ou alterar programas:

- Para remover um VDA, selecione **Citrix Virtual Delivery Agent** <*versão*> e, em seguida, clique com o botão direito e selecione **Uninstall**. O instalador é iniciado e você pode selecionar os componentes a serem removidos.
- Para remover o Servidor de Impressão Universal, clique com o botão direito em **Citrix Universal Print Server** e selecione **Uninstall**.

Remover uma VDA por meio de 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 obter descrições de sintaxe.

- Para remover apenas o VDA ou apenas o aplicativo Citrix Workspace, use as opções `/remove` e `/components`.
- Para remover o aplicativo VDA e Citrix Workspace, use a opção `/removeall`.

Por exemplo, o comando a seguir remove o aplicativo VDA e Citrix Workspace de uma máquina com sistema operacional 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 sistema operacional de sessão única.

```
VDAWorkstationSetup.exe /remove /components vda
```

Você também pode remover um VDA usando um script fornecido pela Citrix. Veja Remover VDAs usando o script.

Camada de personalização de usuário

June 6, 2023

O recurso de camada de personalização do usuário do Citrix Virtual Apps and Desktops amplia os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e aplicativos instalados localmente em todas as sessões. Equipado com a tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e Machine Creation Services (MCS) em catálogos de máquinas não persistentes.

Você instala os componentes da camada de personalização do usuário juntamente com o Virtual Delivery Agent dentro da imagem mestre. Um arquivo VHD armazena localmente os aplicativos instalados pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

> **Importante:**
>
> Você pode implantar camadas de personalização de usuário no Citrix Virtual Apps and Desktops ou camadas de usuário do App Layering ativadas em um modelo de imagem, não as duas. Não instale o recurso da camada de personalização do usuário em uma camada dentro do App Layering.

Esse recurso substitui o Personal vDisk (PvD), além de fornecer uma experiência de espaço de trabalho persistente para usuários em um ambiente de área de trabalho não persistente em pool.

Para implantar o recurso de camada de personalização do usuário, instale-o e configure-o usando as etapas detalhadas no artigo. Antes disso, o recurso não estará disponível.

Suporte a aplicativos

Além das exceções a seguir, 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 empresariais, 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 repositório 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 os aplicativos diretamente na imagem mestre.

Aplicativos que exigem uma conta de usuário ou administrador local

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 persistirão além da sessão.

> **Importante:**
>
> Adicione os usuários ou grupos locais necessários na imagem mestre.

Requisitos

O recurso da 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 arquivos do Azure com autenticação do AD no local ativada

Você pode implantar o recurso de camada de personalização de usuário nas seguintes versões do Windows com sistema operacional implantado como uma única sessão. 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 multissessão (arquivos do Azure suportados)
- Windows Server 2016 (arquivos do Azure suportados)
- Windows Server 2019 (arquivos do Azure suportados)

Para o Citrix Virtual Apps and Desktops 7, o uso de arquivos do Azure com camadas de personalização de usuário é suportado no Windows Server 2019, Windows Server 2016v e no cliente Windows 10.

> **Nota:**
>
> Se você estiver usando um SO de servidor, somente o Server VDI é aceito. 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 a máquina precisa ser reinicializada para reiniciar os discos. Você não pode usar a camada de personalização do usuário com sistemas operacionais de servidor multissessão, apenas com sistemas de servidor de sessão única. A camada de personalização do usuário funciona apenas com áreas de trabalho não persistentes.

Desinstale o recurso da camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

Configurar o compartilhamento de arquivos

O recurso da camada de personalização do usuário requer o armazenamento SMB (Server Message Block) do Windows. Para criar um compartilhamento de arquivos do Windows, siga as etapas habituais para o sistema operacional Windows em que você está.

Para obter mais informações sobre como usar os Arquivos do Azure com catálogos baseados no Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

Recomendações, em Recommendations

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 instruções da Microsoft para preparar a imagem em um ambiente VDI. Consulte este artigo do Microsoft TechNet para obter mais informações.

Tamanho da camada do usuário

Uma camada de usuário é um disco thin provisionado que se expande à medida que o espaço em disco é utilizado. O tamanho padrão permitido para uma camada de usuário é 10 GB, o mínimo que recomendamos.

> **Nota:**
>
> Durante a instalação, se o valor for definido como zero (0), o tamanho da camada de usuário padrão será definido como 10 GB.

Se quiser alterar o tamanho da camada do usuário, insira um valor diferente na política **User Layer Size** do Studio. Consulte, na **Etapa 5: Criar políticas personalizadas de grupo de entrega**, **Opcional: clique em Select 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 Windows para definir uma cota no compartilhamento de arquivos da camada do usuário.

Use uma das seguintes ferramentas de cota da Microsoft para definir uma cota fixa no diretório da camada de usuário chamado **Users**:

- Gerenciador de Recursos do Servidor de Arquivos (FSRM)
- Gerente de cota

> **Nota:**
>
> Aumentar a cota afeta as novas camadas de usuário e expande as existentes. Diminuir a cota afeta apenas as novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

Implantar uma camada de personalização de usuário

Ao implantar o recurso de personalização do usuário, você define as políticas no Studio. Depois, 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 de usuário, os serviços permanecem inativos e não interferem nas atividades de criação.

Se você definir as políticas na imagem mestre, os serviços tentam realizar a execução e montar uma camada de usuário dentro da imagem mestre. A imagem mestre poderá exibir comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, execute as seguintes etapas nesta ordem:

- Etapa 1: verifique a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Passo 2: prepare sua imagem mestre.
- Etapa 3: crie um catálogo de máquinas.
- Etapa 4: crie um grupo de entrega.
- Etapa 5: crie políticas personalizadas do 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 login.

Etapa 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

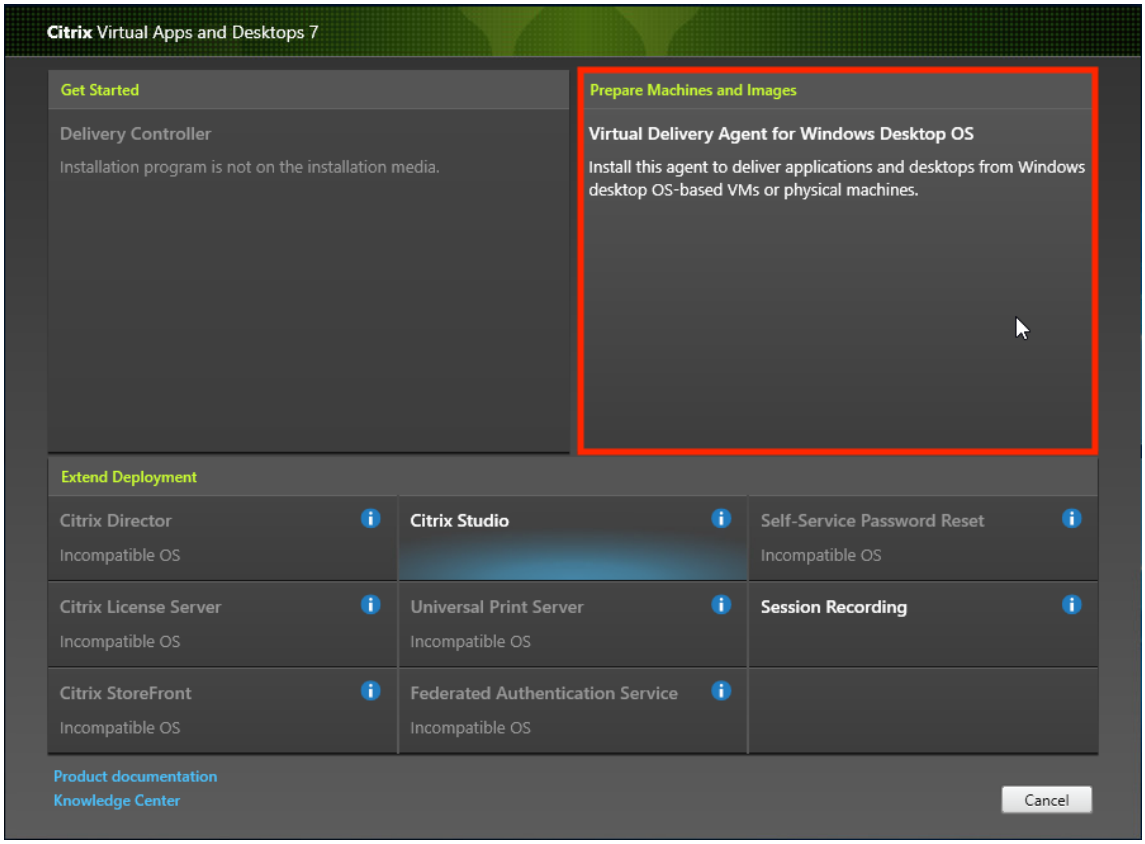
Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops está disponível para usar com o novo recurso. Para obter detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

Etapa 2: Prepare sua imagem mestre

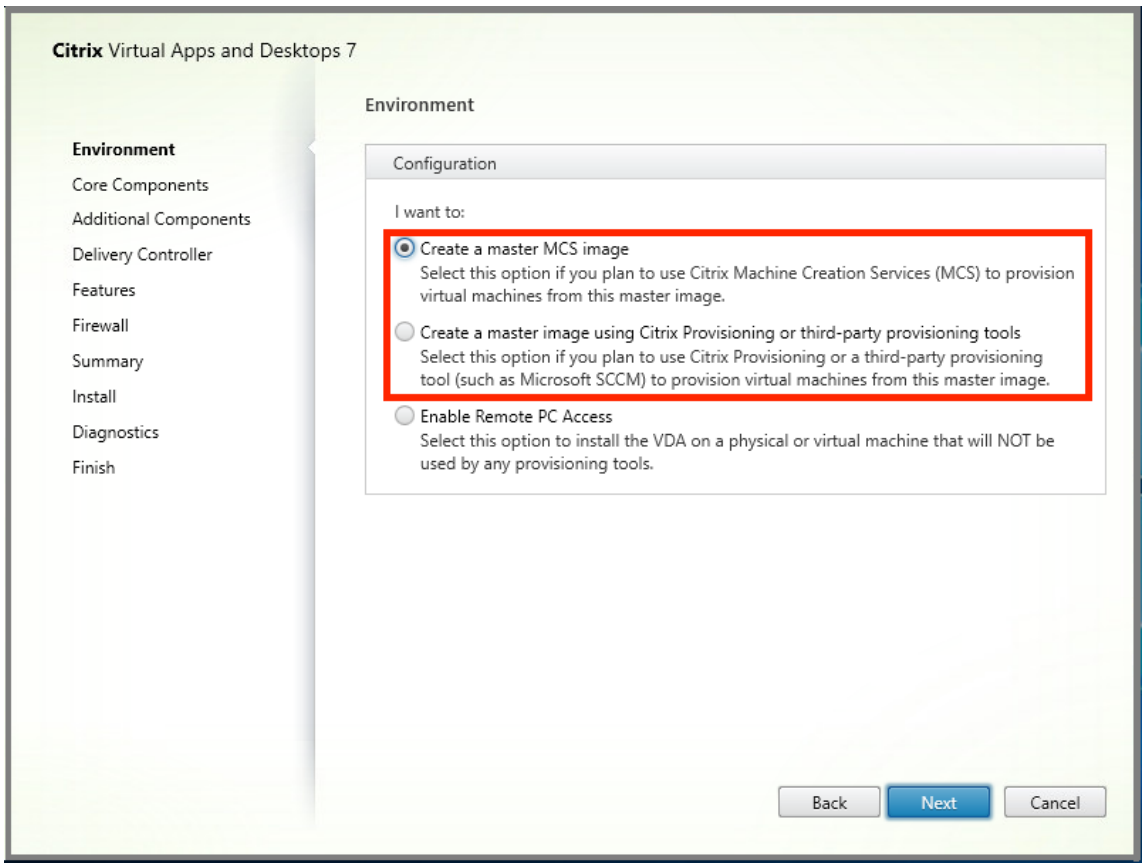
Para preparar a sua imagem mestre:

1. Localize a imagem mestre. Instale os aplicativos empresariais da sua organização e outros aplicativos que os usuários geralmente acham úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Lembre-se de incluir o componente opcional **User personalization layer**. Para obter detalhes, consulte as opções de linha de comando para instalar um VDA.
3. Se 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. Quando instalar a nova versão, certifique-se de selecionar e instalar o componente opcional **Citrix User Personalization Layer** como se segue:

    a) Clique no bloco **Virtual Delivery Agent for Windows Desktop OS**:

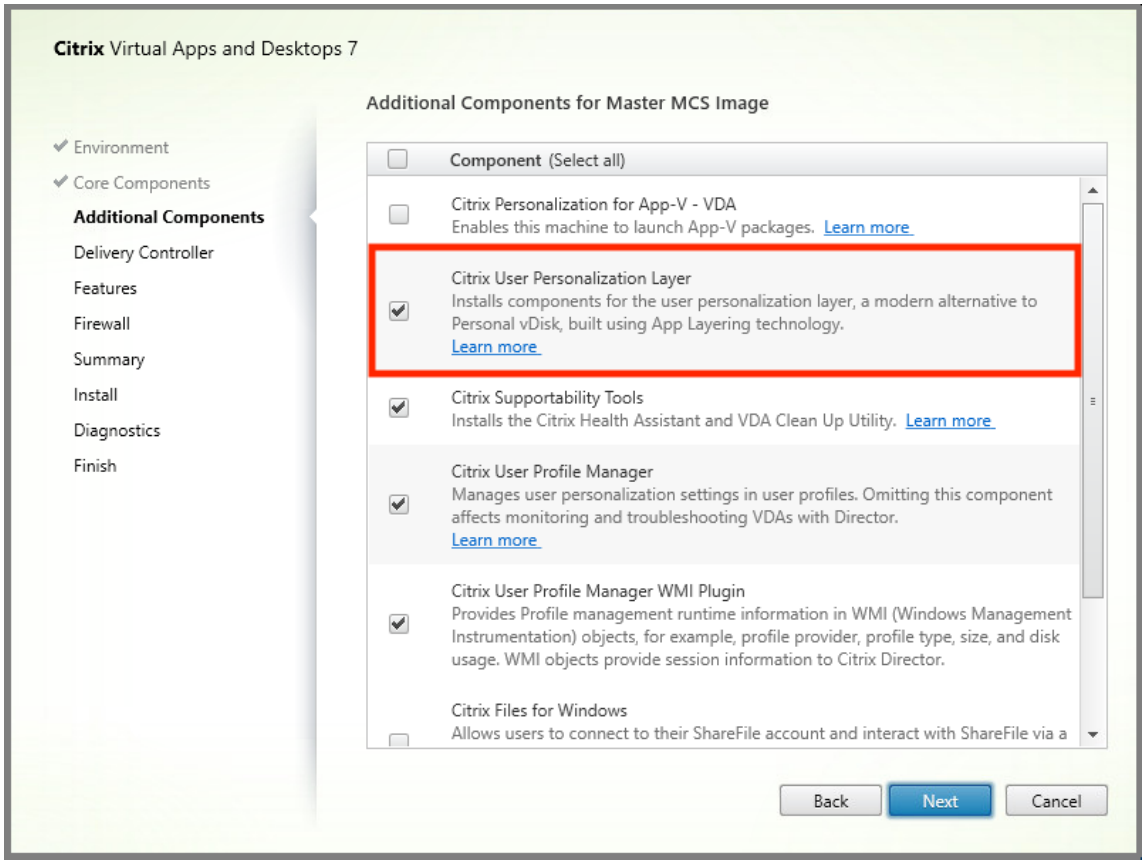


a) **Environment:** selecione **Create a master MCS image** ou **Create a master image using Citrix Provisioning or third-party provisioning tools**.



a) **Core Components:** clique em **Next**.

b) **Additional Components:** selecione **Citrix User Personalization Layer**.



a) Clique nas telas de instalação restantes, configurando o VDA conforme necessário, e clique em **Install**. A imagem é reinicializada uma ou mais vezes durante a instalação.

4. Deixe **Windows updates** desativado. O instalador da camada de personalização do usuário desativa as atualizações do Windows na imagem. Deixe as atualizações desativadas.

A imagem está pronta para você carregar no Studio.

> **Nota:**
>
> Se deseja simplesmente atualizar a camada de personalização do usuário (UPL), você pode fazer isso com uma versão mais recente da UPL e o pacote autônomo. Você não precisa atualizar o VDA.

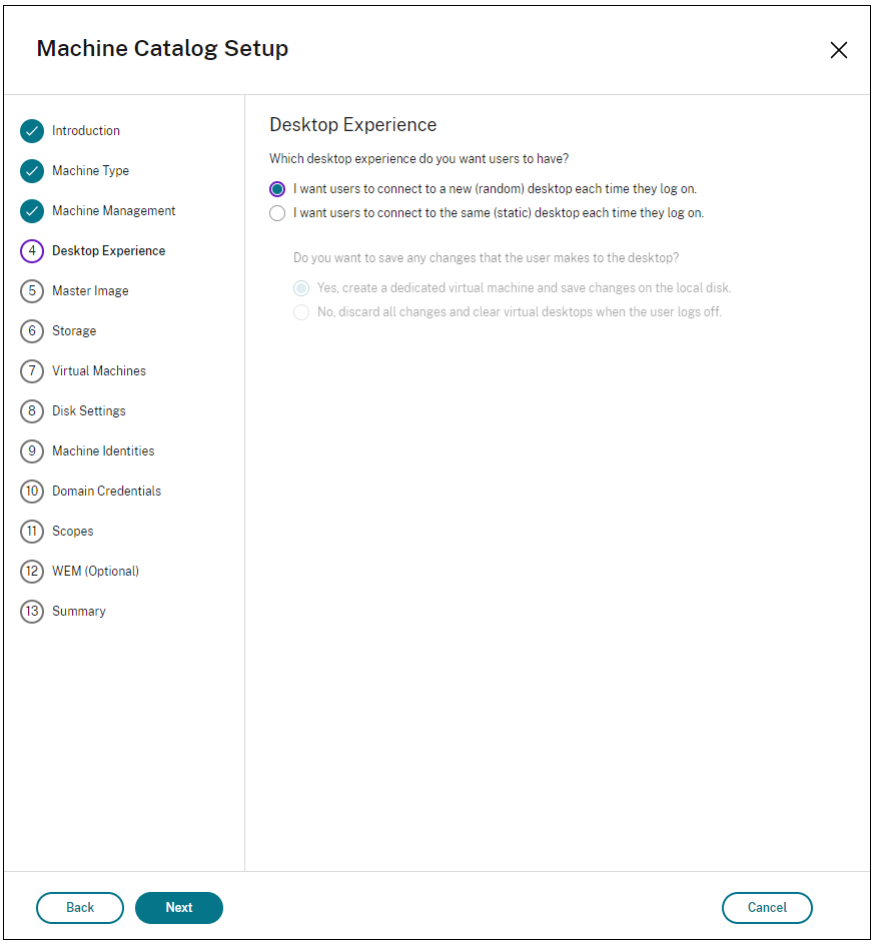
Etapa 3: Crie um catálogo de máquinas

No Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

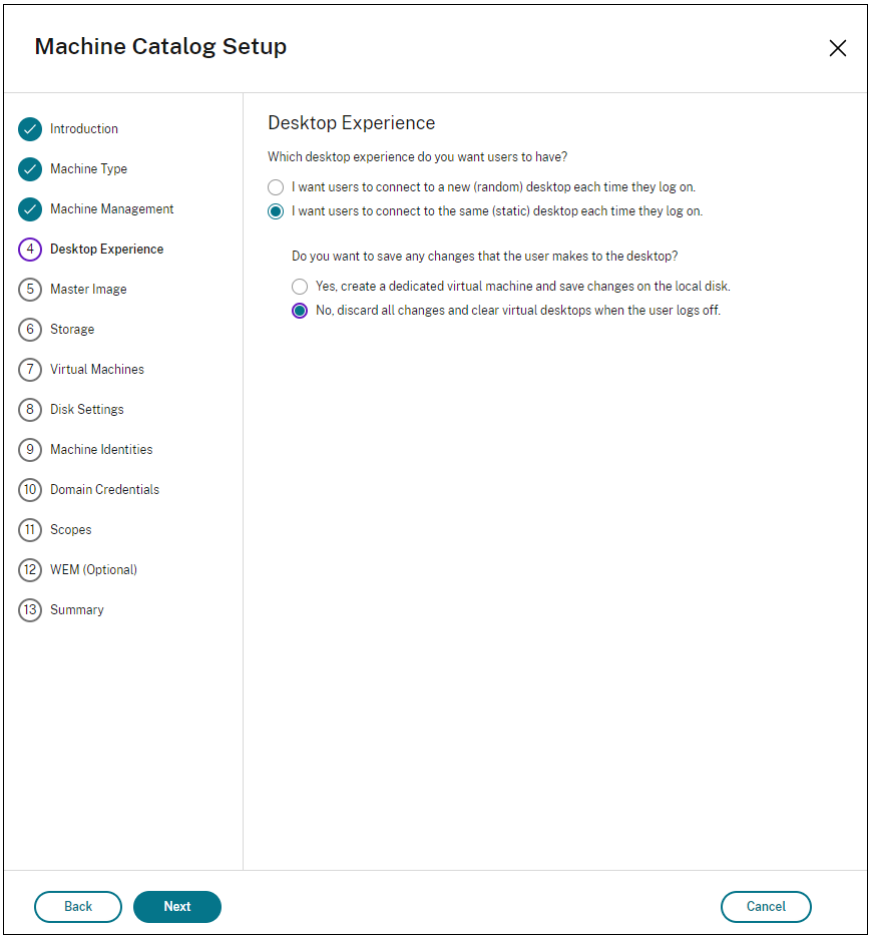
1. Selecione **Operating System** e defina como **Single session OS**.
2. Selecione **Machine Management** e defina como **Machines that are power managed**. Por exemplo, máquinas virtuais ou PCs blade.

3. Selecione **Desktop Experience** e defina o tipo de catálogo como **pooled-random** ou **pooled-static**, conforme os exemplos a seguir:

   - **Pooled-random:**



   - **Pooled-static:** se você selecionar pooled-static, configure áreas de trabalho para descartar todas as alterações e limpar as áreas de trabalho virtuais quando o usuário fizer logoff, conforme mostra a captura de tela a seguir:



> **Nota:**
>
> A camada de personalização do usuário não oferece suporte a catálogos estáticos em pool configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se estiver usando o MCS, selecione **Master Image** e o instantâneo da imagem criada na seção anterior.
5. Configure as propriedades de catálogo restantes conforme necessário para o seu ambiente.

Etapa 4: Crie 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.

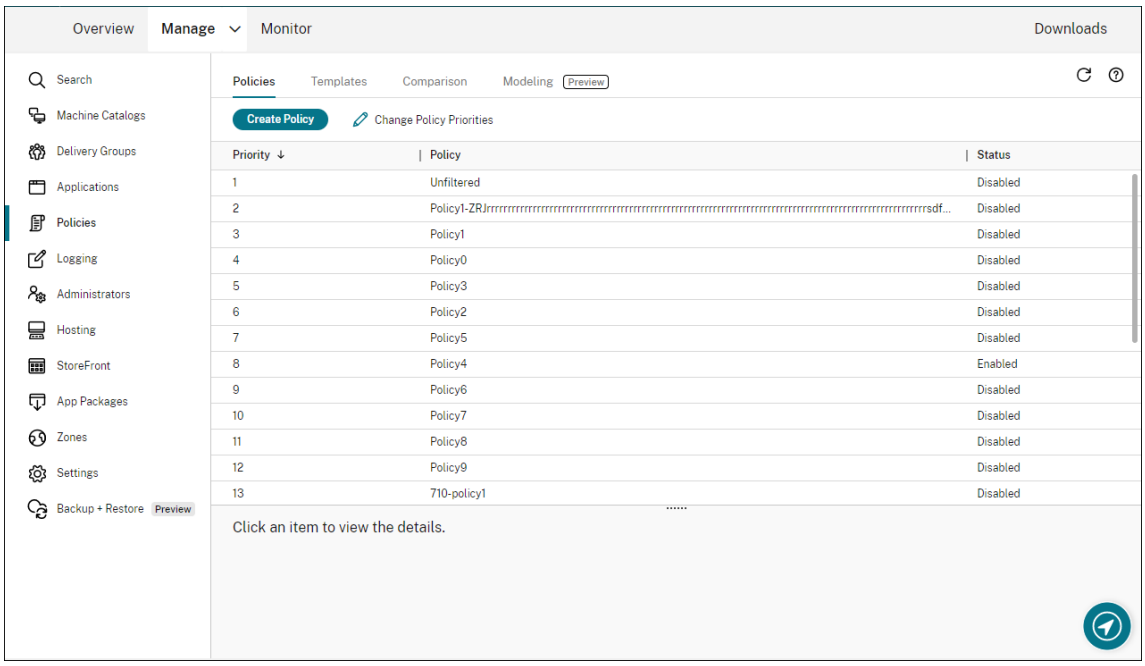
Etapa 5: Crie políticas personalizadas do grupo de entrega

Para habilitar a montagem de camadas de usuário em Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Em que ponto da rede acessar as camadas do usuário.
- Quanto permitir que os discos da camada do usuário cresçam.

Para definir os parâmetros como políticas Citrix personalizadas no Web Studio e atribuí-las ao seu grupo de entrega.

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.



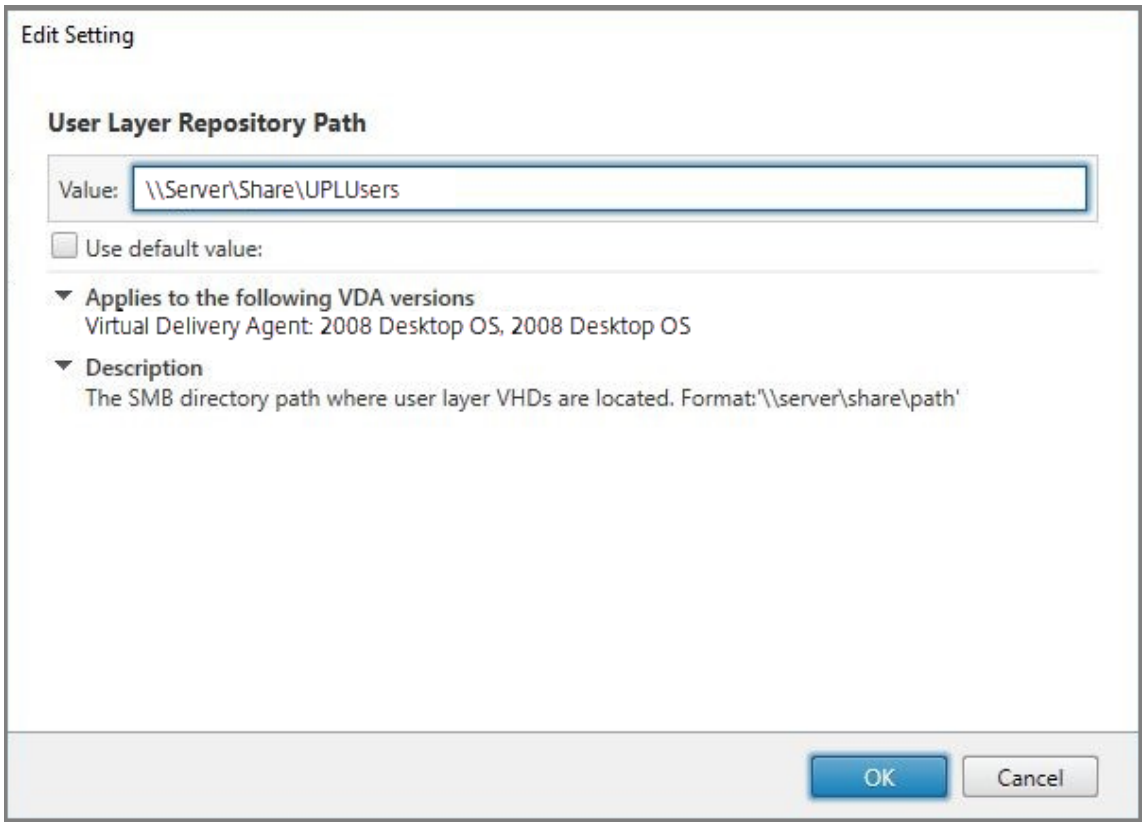
2. Selecione **Create Policy** na barra de ações. A janela Create Policy é exibida.
3. Digite ‘user layer’no campo de pesquisa. As três políticas a seguir aparecem na lista de políticas disponíveis:

   - User Layer Exclusions
   - User Layer Repository Path
   - User Layer Size GB

   > **Nota:**
   >
   > Aumentar o tamanho afeta as novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas as novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

4. Marque a caixa de seleção ao lado de **User Layer Repository Path** e clique em **Edit**. É exibida a janela Edit Setting.
5. Insira um caminho no campo **Value** e clique em **Save**:

   - **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`

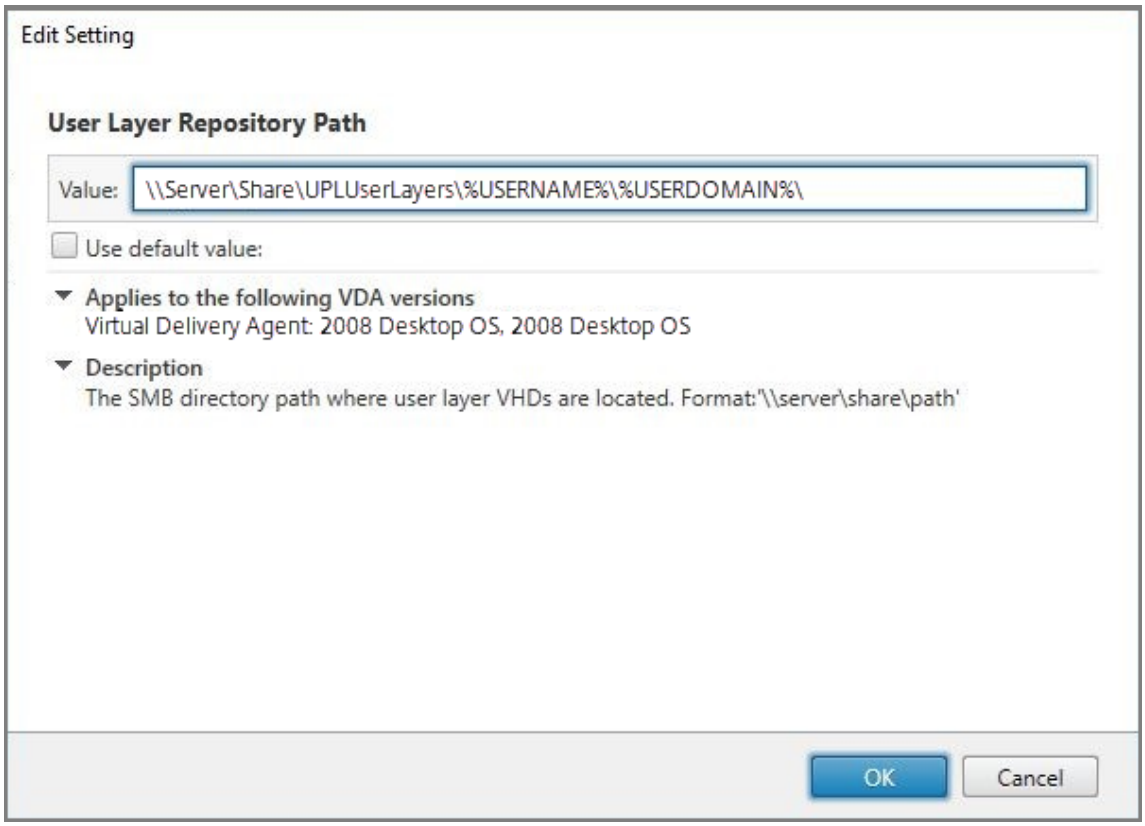


Você pode personalizar o caminho usando as variáveis `%USERNAME%` e `%USERDOMAIN%`, variáveis de ambiente da máquina e atributos do Active Directory (AD). Quando expandidas, essas variáveis resultam em caminhos explícitos.

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\`

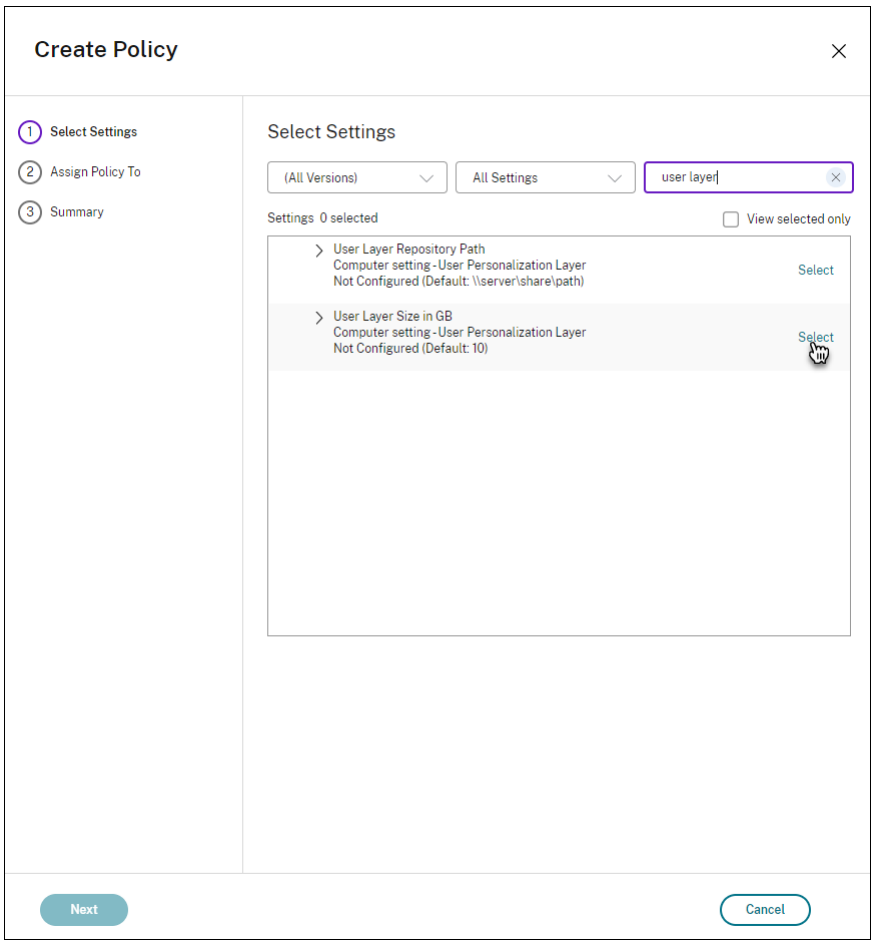
`CoolCompanyDomain\A_OK`



Exemplo de atributos personalizados do AD:

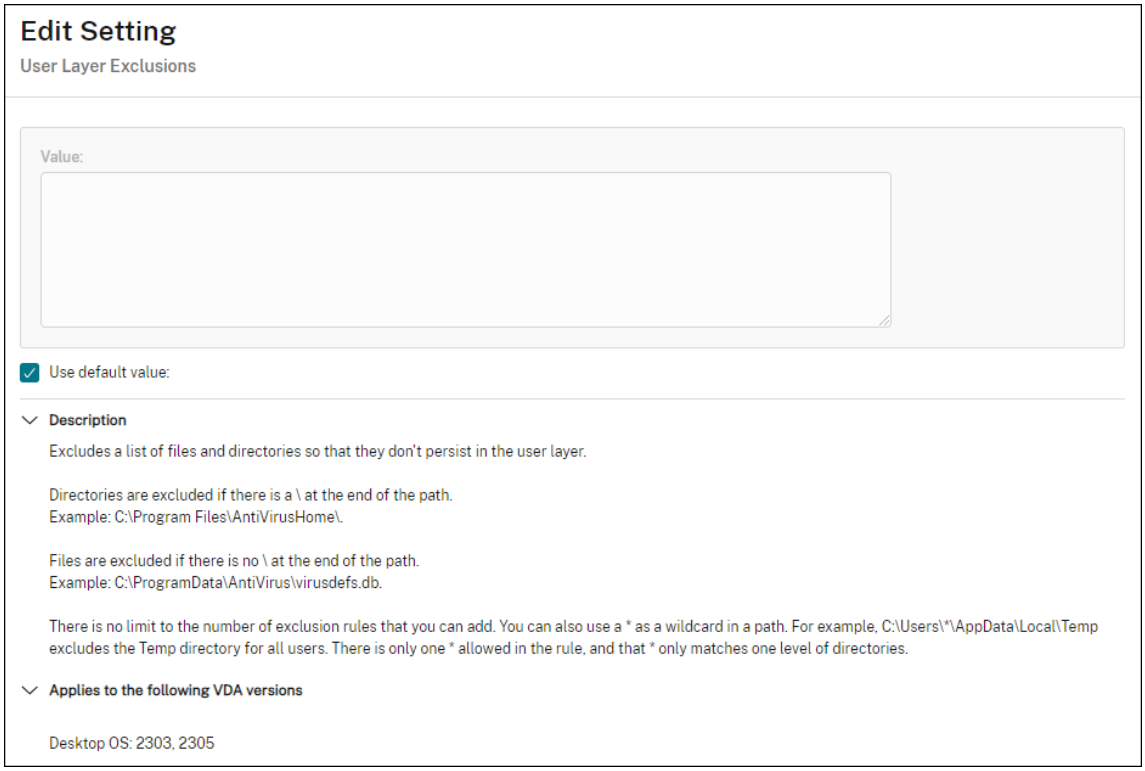
- Formato do caminho: `\\Server-name-or-address\share-name\AD-attribute`
- Exemplo de caminho: `\\Server\share\\#sAMAccountName#`
- Exemplo de caminhos resultantes: `\\Server\share\JohnSmith` (se #sAMAccount-Name # for resolvido para JohnSmith para o usuário atual)

6. Opcional: marque a caixa de seleção ao lado de **User Layer Size in GB** e clique em **Edit**:

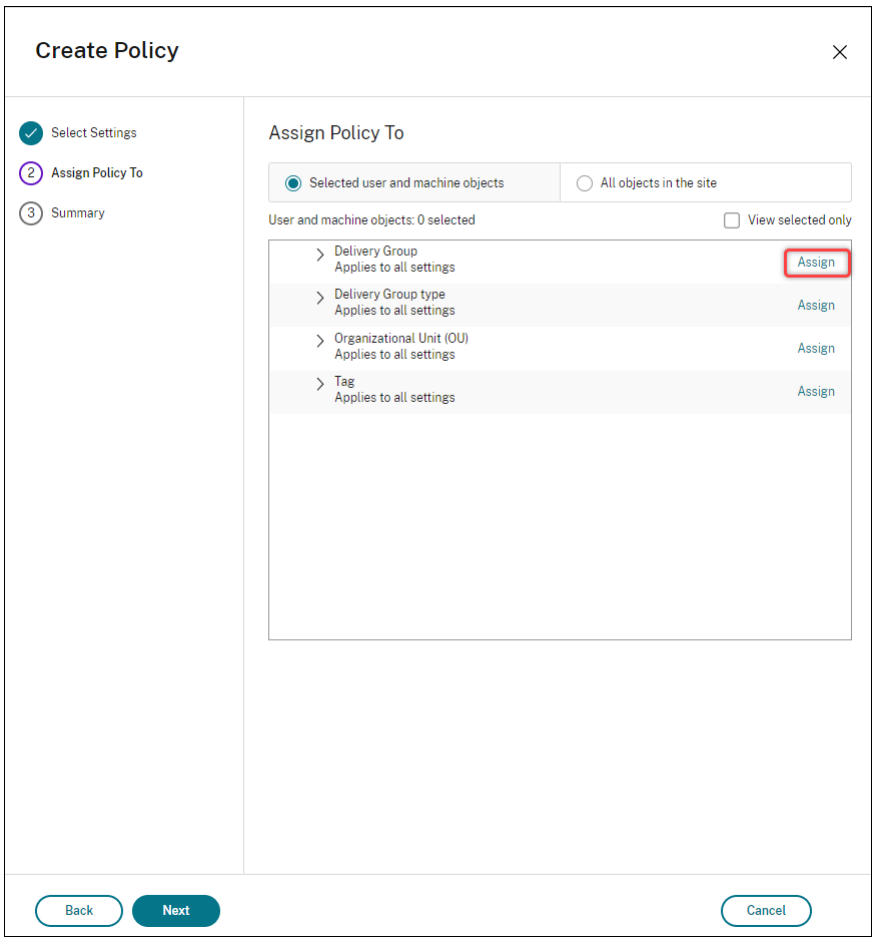


A janela Edit Settings é exibida.

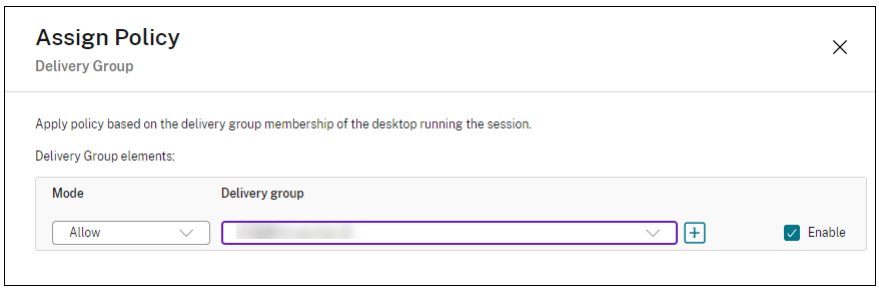
7. Opcional: altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode crescer. Clique em **Salvar**.
8. Opcional: marque a caixa de seleção ao lado de **User Layer Exclusions** e clique em **Edit**.



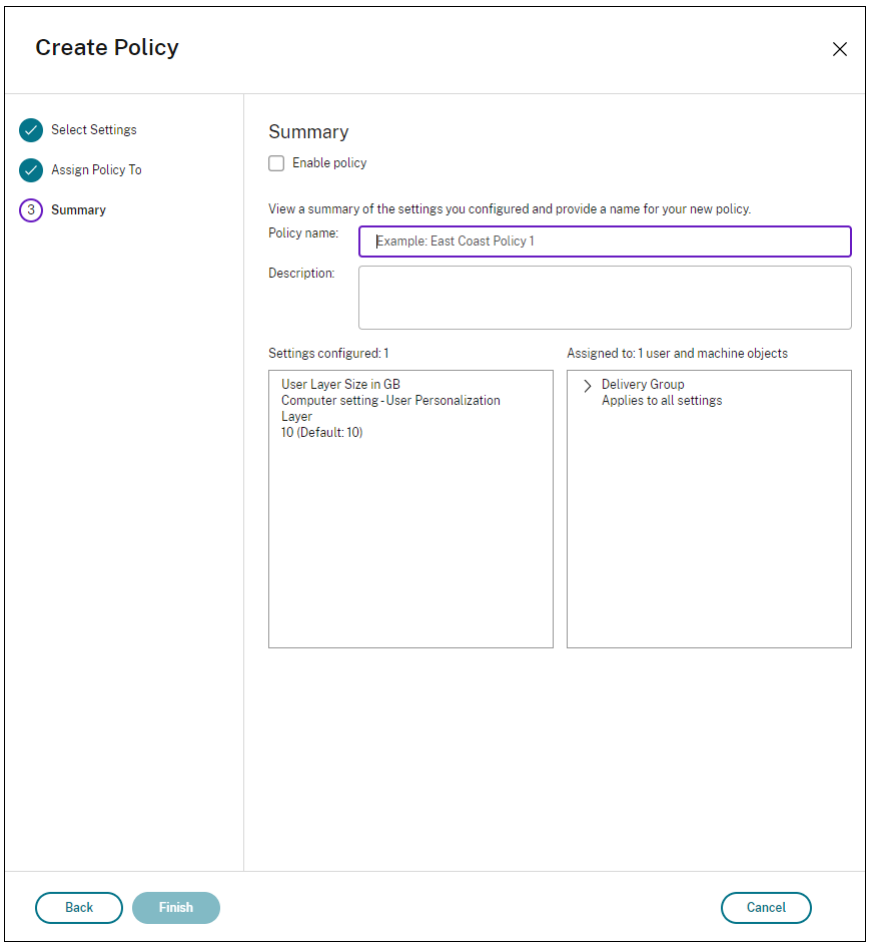
9. Opcional: especifique os arquivos e pastas a serem excluídos e clique em **Save**. Para obter mais informações, consulte a documentação do Citrix App Layering.
10. Clique em **Next** para configurar usuários e máquinas aos quais você deseja atribuir. Clique no link **Assign de Delivery Group**, em destaque nesta imagem:



11. No menu **Delivery Group**, selecione o grupo de entrega criado na seção anterior. Clique em **OK**.



12. Digite um nome para a política. Clique na caixa de seleção para ativar a política e clique em **Finish**.



Configurar parâmetros 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 do parâmetro	Valor	Aplica-se a
Creator Owner	Modify	Somente subpastas e arquivos
Owner Rights	Modify	Somente subpastas e arquivos
Users or group	Create Folder/Append Data; Traverse Folder/Execute File; List Folder/Read Data; Read Attributes	Somente pasta selecionada
System	Full Control	Pasta, subpastas e arquivos selecionados

Nome do parâmetro	Valor	Aplica-se a
Domain Admins, e Admin do grupo selecionado	Full Control	Pasta, subpastas e arquivos selecionados

Mensagens de 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.<!--
  NeedCopy-->
  ```

- **Camada do 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.<!--NeedCopy-->
  ```

- **Sistema não redefinido após a saída do usuário**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

Arquivos de log para usar ao solucionar 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
<!--NeedCopy-->
```

Limitações

Tenha em mente as seguintes limitações ao instalar e usar o recurso de camada de personalização do usuário.

- *Não* tente implantar o software de camada de personalização do usuário em uma camada dentro do App Layering. Implante camadas de personalização do usuário no Citrix Virtual Apps and

Desktops ou ative camadas de usuário em um modelo de imagem no App Layering, 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 da máquinas com uma imagem executando uma nova instalação de sistema operacional (inclusive a mesma versão do Windows 10). A prática recomendada é aplicar atualizações ao sistema operacional dentro da mesma imagem mestre usada ao criar o catálogo de máquinas.
- *Não* use drivers de tempo de inicialização nem outros tipos de personalização de inicialização antecipada.
- *Não* migre dados 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 sistema operacional mestre diferente.
- Quando um usuário faz logout de uma sessão e, em seguida, faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Centro de Software da Microsoft lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Não disponível** na segunda máquina.

  Para descobrir o verdadeiro status do aplicativo, instrua o usuário a selecionar o aplicativo no Centro de Software e clicar em **Instalar**. Em seguida, o SCCM atualiza o status para o valor verdadeiro.
- Ocasionalmente, o Centro de Software é interrompido imediatamente após iniciar 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 XenDesktop VDI. Além disso, certifique-se de que o serviço `ccmexec` está em execução antes de iniciar o Centro de Software.
- Nas Políticas de Grupo (Configurações do Computador), as configurações da camada do usuário substituem as configurações aplicadas à imagem mestre. Portanto, as alterações feitas às configurações do computador usando um GPO nem sempre estão apresentadas ao usuário no próximo login da sessão.

  Para contornar esse problema, crie um script de logon de usuário que emita o comando:

  ```
  gpupdate /force
  ```

  Por exemplo, um cliente define o seguinte comando para executar em cada login de usuário:


```
gpudate /Target:Computer /force
```

Para obter melhores resultados, aplique alterações às configurações do computador diretamente na camada do usuário, após o usuário ter 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 apresentarão problemas.
- Os certificados personalizados não persistem quando o UPL está habilitado em um ambiente Azure AD 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.

Upgrade de VDAs

July 28, 2023

Introdução

A Citrix mantém todos os componentes do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) em sua implantação, exceto VDAs.

Antes de iniciar uma atualização do VDA:

- Leia este artigo inteiro, para saber o que esperar.
- Leia a política de ciclo de vida do Citrix DaaS.

Para atualizar um VDA, baixe um instalador de VDA e execute-o na máquina ou na imagem. Você pode usar a interface gráfica ou de linha de comando do instalador. Para obter orientação, consulte:

- Instaladores de VDA
- Instalar VDAs usando a interface gráfica
- Instalar VDAs usando a linha de comando

Se o VDA foi originalmente instalado usando `VDAWorkstationCoreSetup.exe`:

- Você manterá essa configuração se atualizar o VDA com a versão mais recente do mesmo instalador.
- Se você executar `VDAWorkstationSetup.exe` nessa máquina, poderá ativar os recursos que não são suportados em `VDAWorkstationCoreSetup.exe`. Lembre-se de que alguns desses recursos podem estar ativados por padrão no instalador `VDAWorkstationSetup.exe`. Você também pode instalar o aplicativo Citrix Workspace.

> **Nota:**
>
> Ao atualizar um VDA para a versão 7.17 ou uma versão posterior suportada, ocorre a reinicialização da máquina durante o processo de atualização. Essa reinicialização não pode ser evitada. A atualização é retomada automaticamente após a reinicialização (a menos que você especifique `/noresume` na linha de comando).

Depois de atualizar o VDA, atualize as imagens e os catálogos que usam esse VDA.

Atualizar VDAs usando a interface Full Configuration

> **Importante:**
>
> - Uma boa prática que recomendamos é que você teste minuciosamente as atualizações do VDA antes de entrar em produção.
> - Você pode alternar entre o VDA CR e o VDA LTSR, desde que a mudança seja de uma versão anterior para uma versão posterior. Você não pode mudar de uma versão posterior para uma versão anterior porque isso é considerado um downgrade. Por exemplo, você não pode fazer o downgrade de 2212 CR para 2203 LTSR (qualquer CU), mas pode fazer o upgrade de 2112 CR para 2203 LTSR (qualquer CU).
> - Não há suporte para atualizações sob demanda (como hotfixes e patches entre as principais versões).

Usando a interface Full Configuration, você pode atualizar VDAs por catálogo ou por máquina. Você pode atualizá-los imediatamente ou em um horário agendado.

Para saber mais sobre o serviço de atualização do VDA, consulte Tech Brief: Citrix VDA Upgrade service. Você encontrará uma visão geral do serviço, informações detalhadas sobre como ele funciona e outros recursos úteis.

Pré-requisitos

- Plano de controle: Citrix DaaS
- Tipo de VDA: VDA com SO de sessão única ou multissessão
- Versão do VDA: 2109 ou posterior, ou 2203 LTSR ou posterior

  > **Nota:**
  >
  > Recomendamos usar o CR VDA mais recente ou o LTSR CU VDA mais recente.

- Tipo de provisionamento: máquinas persistentes (como máquinas provisionadas por MCS, máquinas de acesso ao PC remoto, Citrix HDX Plus para Windows 365). Consulte Tipos de máquinas compatíveis.

- Os VDAs devem ter o VDA Upgrade Agent instalado e o serviço deve estar em execução.
- Você ter permissões para atualizar VDAs.
- A atualização do VDA estar configurada com a trilha CR ou LTSR adequada em Full Configuration.
- Os VDAs não estarem em uso. (Os usuários devem se desconectar deles.)

> **Nota:**
>
> Os upgrades são ignorados para quaisquer VDAs que estejam em uso ou em estado desconectado. Recomendamos agendar uma janela de atualização e solicitar que os usuários se desconectem dos VDAs.

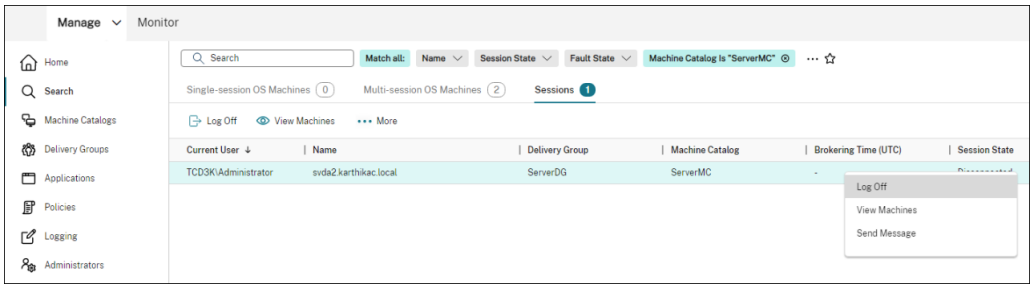
- Os VDAs não estarem no modo de manutenção. (O VDA pode ser colocado em modo de manutenção por um administrador. O VDA também pode ser colocado automaticamente no modo de manutenção se tiver excedido o máximo permitido de tentativas de registro.)
- URLs relevantes adicionadas à lista de permissões se a filtragem de URL estiver em vigor. Consulte Requisito para atualização do VDA.
- Os VDAs devem pertencer a um grupo de entrega e estar registrados no DaaS.
- O nível funcional é definido corretamente para que o recurso de atualização do VDA esteja disponível para uso. Consulte Versões do VDA e níveis funcionais.
- O VDA de destino suporta o sistema operacional do VDA atual.

Problemas conhecidos

Problema 1: Falha ao atualizar VDAs LTSR para versões de atualização cumulativa (CU) LTSR
As tentativas de atualizar VDAs LTSR para versões de atualização cumulativa (CU) LTSR podem falhar. Embora o processo de atualização pareça ter sido concluído com êxito na Full Configuration, a versão instalada do VDA não muda e o status volta para **Upgrade Available** após um ou dois minutos. O problema ocorre com VDAs que têm o VDA Upgrade Agent versão 7.35.0.7 ou anterior instalado.

Para contornar o problema, faça login no VDA e atualize o VDA Upgrade Agent para a versão 7.37.0.7 ou posterior (usando o instalador do VDA versão 2303 ou posterior). A partir da versão 7.37.0.7, o VDA Upgrade Agent oferece suporte à atualização automática para que agentes de versões anteriores executadas nos VDAs possam atualizar automaticamente para a versão mais recente. Com esse recurso de atualização automática, o serviço de atualização do VDA verifica a versão do VDA relatada pelo agente e, em seguida, agenda as atualizações para dentro de uma hora para atualizar automaticamente o agente para a versão mais recente. Esse recurso de atualização automática reduz seu esforço de manutenção.

Para que o agente no VDA seja atualizado automaticamente, certifique-se de fazer logoff das sessões para que o serviço de atualização do VDA possa iniciar as atualizações automáticas. Você pode fazer logoff das sessões em Full Configuration.



Se o agente falhar na atualização automática, faça login no VDA e atualize o agente manualmente da seguinte forma:

1. Execute o seguinte cmdlet para exibir o VDA Upgrade Agent no Painel de controle > Desinstalar ou alterar um programa.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $\_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
     Service - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $\_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
     Service - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Instale o VDA Upgrade Agent mais recente. Para realizar uma instalação silenciosa, use o seguinte cmdlet:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

Você pode identificar a versão do VDA Upgrade Agent usando o cmdlet ou um script. Consulte Solução de problemas.

Problema 2: Proxy não suportado Atualmente, o VDA Upgrade Agent não oferece suporte a configurações de proxy. Essa limitação pode causar problemas de conectividade quando o agente tenta estabelecer conexões por meio de um servidor proxy.

Você pode aplicar uma solução alternativa para resolver o problema. Siga as etapas abaixo:

1. Localize o arquivo de configuração do VDA Upgrade Agent em: `C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`.

2. Abra o arquivo de configuração usando um editor de texto.
3. Adicione as seguintes linhas no final do arquivo, substituindo `ProxyServerName` pelo nome real do servidor proxy:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
        ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Reinicie o serviço Citrix VDA Upgrade Agent para aplicar a configuração atualizada.

Fluxo de trabalho geral

Um fluxo de trabalho geral para atualizar VDAs usando a interface Full Configuration é o seguinte:

1. Ative a atualização de VDA para um catálogo.
   - Você pode ativar a atualização do VDA ao criar um catálogo.
   - Você pode ativar a atualização do VDA ao editar um catálogo.
2. Atualize os VDAs por catálogo ou por máquina. Para obter mais informações, consulte Configurar o upgrade automático para VDAs.

> **Nota:**
>
> Ao programar atualizações de VDA para um catálogo, esteja ciente de que todas as máquinas do catálogo serão incluídas no escopo de atualização. Portanto, recomendamos fazer backup dessas máquinas antes de iniciar a atualização.

Solução de problemas

Se ocorrerem falhas de atualização, você pode usar os seguintes logs para solucionar problemas sozinho ou fornecer os logs ao entrar em contato com o Suporte Técnico Citrix para obter assistência.

- Logs de instalação para instalação inicial do VDA em `%temp%/Citrix/XenDesktop Installer`
- Logs de atualização em `C:\Windows\Temp\Citrix\XenDesktop Installer`

Para verificar as versões do VDA Upgrade Agent, use o seguinte cmdlet: `Get-VusComponentVersion -ComponentType VUS`. Ele lista todos os VDAs e suas versões do VDA Upgrade Agent.

Para obter os nomes do VDA, use o seguinte cmdlet: `Get-BrokerMachine -UUID "<version number>"`, onde `<version number>` está a versão do VDA Upgrade Agent que você obtém do cmdlet `Get-VusComponentVersion`.

Para verificar as versões do VDA Upgrade Agent no nível de catálogo, você pode usar o seguinte script:

> **Nota:**
>
> O script serve como exemplo e talvez precise ser adaptado para se adequar ao seu ambiente específico. Recomendamos que você teste o script minuciosamente 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 $_
 }

```



```
<!--NeedCopy-->
```

Logs relacionados ao VDA Upgrade Agent Você também pode coletar logs relacionados ao VDA Upgrade Agent. Os logs que você pode coletar incluem:

- **Rastreamentos do Citrix Diagnostic Facility (CDF)**.
- **Logs de eventos do Windows**. Informações gravadas no Log de Eventos do Windows. Veja os logs em **Event Viewer > Applications and Services Logs > Citrix VDA Upgrade Agent Service**.

Se necessário, você pode modificar o arquivo de configuração do VDA Upgrade Agent para que os logs sejam gravados continuamente em um arquivo. Para habilitar o registro em log em um arquivo, siga estas etapas:

1. Vá até a pasta `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Abra o arquivo `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Mude 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:**
>
> - A ativação do registro em log em um arquivo grava logs continuamente, potencialmente consumindo espaço de armazenamento. Lembre-se de desativar o registro em log depois que o problema for resolvido. Para desativar o registro em log, primeiro defina `LogToFile` como `0` e reinicie o serviço Citrix VDA Upgrade Agent.
> - Quando `LogToFile=1` estiver definido, os logs serão gravados somente no arquivo. Eles não aparecerão nos rastreamentos de CDF.

Solucionar falhas de download de atualização do VDA Siga as etapas abaixo para solucionar e resolver falhas de download relacionadas ao recurso de atualização do VDA:

1. Confirme que as URLs relevantes foram adicionadas à lista de permissões se a filtragem de URL estiver em vigor. Consulte Requisito para atualização do VDA.
2. Depois de adicionar as URLs necessárias à lista de permissões, tente reagendar a atualização do VDA.

Você pode ativar o rastreamento de CDF ou definir `LogToFile` como 1 para capturar logs detalhados para análise. Se o problema de falha no 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 o seguinte:

- **Opção 1**: redefina as listas de controle de acesso (ACLs) na pasta usando o comando a seguir. (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 agende a atualização do VDA.

Solucionar 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 tenham sido 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 OCSP (Online Certificate Status Protocol), necessárias para a verificação da revogação. Consulte Requisito para atualização do VDA.
2. Depois de adicionar as URLs necessárias à lista de permissões, tente reagendar a atualização do VDA.

Sugerimos ativar o rastreamento de CDF ou configurar `LogToFile` como 1 para capturar registros 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 VDA Upgrade Agent depende das chamadas do sistema Windows para validar certificados e realizar verificações de revogação. Os erros acima indicam que o agente não consegue estabelecer uma conexão com as URLs da CRL ou do OCSP.

Observe que o VDA Upgrade Agent atualmente não oferece suporte a configurações de proxy. As chamadas de saída de CRL e OCSP feitas pela CryptoAPI não reconhecem as configurações de proxy, o que pode resultar em falhas.

Se o seu ambiente tiver uma configuração de proxy, você poderá configurar o proxy do sistema no VDA para facilitar as chamadas de saída de CRL. Siga as etapas abaixo para configurar o proxy do sistema:


```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

Upgrade de VDAs usando o PowerShell

Você pode configurar as atualizações do VDA usando o SDK do Remote PowerShell. Para obter mais informações sobre o SDK do Remote PowerShell, consulte Citrix DaaS Remote PowerShell SDK.

A seguir estão os cmdlets do PowerShell:

- **Get-VusCatalog**

  Use esse cmdlet para obter detalhes de um catálogo como `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), `Upgrade scheduled` e `StateId` (status de `Upgrade scheduled`).

- **Get-VusMachine**

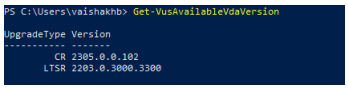
  Use esse cmdlet para obter detalhes de uma máquina como `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) e `StateId` (status de `Upgrade scheduled`).

- **Get-VusComponentVersion**

  Use esse cmdlet para verificar se os VDAs relataram as versões dos componentes. Use `MachineId` para filtrar os VDAs. `MachineId` é o UUID de `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Use esse cmdlet para verificar a versão mais recente do CR/LTSR lançada pelo VDA Update Service.

- **Set-VusCatalogUpgradeType**

  Use esse cmdlet para definir o tipo de upgrade de um catálogo para CR ou LTSR. O tipo de upgrade só pode ser definido no nível do catálogo de máquinas.

- **New-VusMachineUpgrade**

  Use esse cmdlet para configurar upgrades do VDA no nível da máquina.

- **New-VusCatalogSchedule**

  Use esse cmdlet para programar upgrades do VDA no nível do catálogo de máquinas.

Exemplos de cmdlets no nível da máquina

- Defina o tipo de upgrade.

  Exemplo:

  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Use `Get-VusMachine` para verificar `UpgradeState` das máquinas em um catálogo.

  Exemplo:

  - `Get-VusMachine -CatalogName test-catalog`

```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  :
LastStateChange  :
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    :
SessionSupport   : SingleSession
StateId          :
StatusMessage    :
UpgradeState     : UpgradeAvailable
UpgradeType      : LTSR
UpgradeVersion   :

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  :
LastStateChange  :
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    :
SessionSupport   : SingleSession
StateId          :
StatusMessage    :
UpgradeState     : UpgradeAvailable
UpgradeType      : LTSR
UpgradeVersion   :
```

  Se você perceber que `UpgradeState` é `Unknown`, um possível motivo é que o Citrix VDA Upgrade Agent instalado no VDA não relatou a versão ao VDA Update Service. Você pode usar o cmdlet `Get-VusComponentVersion` para verificar se o VDA relatou versões do componente.

  - `Get-VusComponentVersion -MachineId ""`


```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Se nenhum resultado for exibido, verifique o seguinte:

- O VDA faz parte de um catálogo e grupo de entrega.
- O VDA Upgrade Agent está instalado no VDA e em execução. Se necessário, tente reiniciar o agente.

Nota: Se não houver resultados, colete os rastreamentos do Citrix Diagnostic Facility ao reiniciar o VDA Upgrade Agent e solucione os problemas.

- Agende atualizações do VDA. Antes de começar, esteja ciente do seguinte:

  - `DurationInHours`: permite que você forneça a duração em horas do processo de upgrade. Os VDAs serão colocados no modo de manutenção. O instalador do VDA será baixado e a atualização será realizada. Forneça uma duração mais longa se houver muitos VDAs a serem atualizados.
  - `UpgradeNow`: use essa opção para agendar um upgrade imediatamente ou definir `ScheduledTimeInUtc`.
  - `ScheduledTimeInUtc`: permite que você agende um upgrade para uma data e hora específicas.

  Exemplo:

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  Você pode usar `MachineUuid`, `MachineUid` e `MachineName` para agendar a atualização do VDA.

```
PS C:\Windows\system32> New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 2


DurationInHours    : 2
MachineName        : test-machine-1
MachineUUID        : d664614a-cd37-44d6-b1f0-6f6b70f8299c
MachineUid         : 35
ScheduledTimeInUtc : 6/23/2023 11:35:00 AM
UpgradeVersion     : 2203.0.3000.3300
```

- Verifique o status do upgrade.

  Exemplo:

  - `Get-VusMachine -MachineName test-machine-1`


```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

Exemplos de cmdlet no nível de catálogo

- Defina o tipo de atualização no nível do catálogo de máquinas.

  Exemplo:
  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Use `Get-VusCatalog` para verificar `UpgradeState` das máquinas em um catálogo:

  Exemplo:
  - `Get-VusCatalog -Name test-catalog`


```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog

CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Se você perceber que `UpgradeState` é `Unknown`, um possível motivo é que o Citrix VDA Upgrade Agent instalado no VDA não relatou a versão ao VDA Update Service. Você pode usar o cmdlet `Get-VusComponentVersion` para verificar se o VDA relatou versões do componente.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Se nenhum resultado for exibido, verifique o seguinte:

  - O VDA faz parte de um catálogo e grupo de entrega.
  - O VDA Upgrade Agent está instalado no VDA e em execução. Se necessário, tente reiniciar o agente.

Nota: Se não houver resultados, colete os rastreamentos do Citrix Diagnostic Facility ao reiniciar o VDA Upgrade Agent e solucione os problemas.

- Agende atualizações do VDA. Antes de começar, esteja ciente do seguinte:

  - `DurationInHours`: permite que você forneça a duração em horas do processo de upgrade. Os VDAs no catálogo serão colocados no modo de manutenção. O instalador do

VDA será baixado e a atualização será realizada em cada VDA. Forneça uma duração maior se o catálogo contiver muitos VDAs.

- `UpgradeNow`: use essa opção para agendar um upgrade imediatamente ou definir `ScheduledTimeInUtc`.
- `ScheduledTimeInUtc`: permite que você agende um upgrade para uma data e hora específicas.

Exemplo:

```
- New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc
  ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd
  /yyyy hh:mm tt', $null))-DurationInHours 4
```

Você pode usar `CatalogName`, `Uid` e `Uuid` para agendar a atualização.

```
PS C:\Windows\system32> New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 4


CatalogName          : test-catalog
CatalogUUID          : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
CatalogUid           : 30
DurationInHours      : 4
LastStateChangeInUtc : 6/23/2023 12:08:14 PM
ScheduledTimeInUtc   : 6/23/2023 12:00:00 PM
State                : UpgradeScheduled
UpgradeVersion       : 2203.0.3000.3300
```

- Verifique o status do upgrade. Use o cmdlet `Get-VusCatalog` ou `Get-VusMachine` para verificar periodicamente o status do upgrade do VDA. Use `MachineUuid`, `MachineUid` e `MachineName` para filtrar os VDAs.

  Exemplo:

  ```
  - Get-VusCatalog -Name test-catalog
  ```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           : 0
DurationInHours             : 4
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades       : 100
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeInProgress
SuccessfulUpgrades          : 0
TotalMachines               : 2
Uid                         : 30
UpgradeState                : UpgradeScheduled
UpgradeType                 : LTSR
UpgradeVersion              : 2203.0.3000.3300
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```


Use `Get-VusMachine` para ver o status de atualização do VDA de cada máquina em um catálogo.

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

Se o VDA tiver o Personal vDisk instalado

Se o componente Personal vDisk (PvD) já tiver sido instalado em um VDA, esse VDA não poderá ser atualizado para a versão 1912 LTSR ou posterior até que você remova o componente.

Essa instrução se aplica mesmo que você nunca tenha usado o PvD. Veja como o componente PvD pode ter sido instalado em versões anteriores:

- Na interface gráfica do instalador do VDA, o PvD era uma opção na página **Additional Components**. O 7.15 LTSR e versões 7.x anteriores habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou ativou explicitamente a opção em alguma versão), o PvD foi instalado.
- Na linha de comando, a opção `/baseimage` instalou o PvD. Se você especificou essa opção ou usou um script que continha essa opção, o PvD foi instalado.

O que fazer

Se o instalador de VDA não detectar o componente PvD no VDA instalado atualmente, a atualização prosseguirá como de costume.

Se o instalador detectar o componente PvD no VDA atualmente instalado:

- **Interface gráfica:** a atualização pausa. Uma mensagem pergunta se você deseja que o componente não suportado seja removido automaticamente. Quando você clica em **OK**, o componente é removido automaticamente e a atualização prossegue.
- **CLI:** o comando falha se o instalador detectar o componente PvD. Para evitar a falha do comando, inclua a seguinte opção no comando: `/remove_pvd_ack`.

Se você quiser continuar usando o PvD em suas máquinas Windows 10 (1607 e anteriores, sem atualizações), o VDA 7.15 LTSR é a versão mais recente suportada. Esteja ciente de que o programa de suporte estendido para XenApp e XenDesktop 7.15 LTSR não se aplica aos VDAs usados com o Citrix DaaS. Para obter mais informações, consulte o Extended Support Customer Guide no Citrix Support Knowledge Center.

Sistemas operacionais anteriores

O artigo Requisitos do sistema lista os sistemas operacionais Windows suportados pelos VDAs com a versão atual.

- Para VDAs LTSR, consulte o artigo de requisitos do sistema para a sua versão LTSR.
- Para Linux VDAs, consulte a documentação do Linux Virtual Delivery Agent.

Para computadores Windows com sistemas operacionais que não têm mais suporte para instalação do VDA mais recente, você tem as seguintes opções.

Para ambientes não WVD:

- Refaça a imagem da máquina para uma versão compatível do Windows e instale o novo VDA.
- Se a nova imagem da máquina não for uma opção, mas você quiser atualizar o sistema operacional, desinstale o VDA antes de atualizar o sistema operacional. Caso contrário, o VDA estará em um estado sem suporte. Depois de atualizar o sistema operacional, instale o novo VDA.
- Se a máquina tiver a versão 7.15 LTSR instalada (e você tentar instalar uma versão mais recente), uma mensagem informará que você está usando a versão mais recente suportada.
- Se a máquina tiver uma versão anterior à 7.15 LTSR instalada, uma mensagem o levará até CTX139030 para obter informações. Você pode baixar VDAs 7.15 LTSR no site da Citrix.

Migrar a configuração para o Citrix Cloud

December 21, 2022

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.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

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.

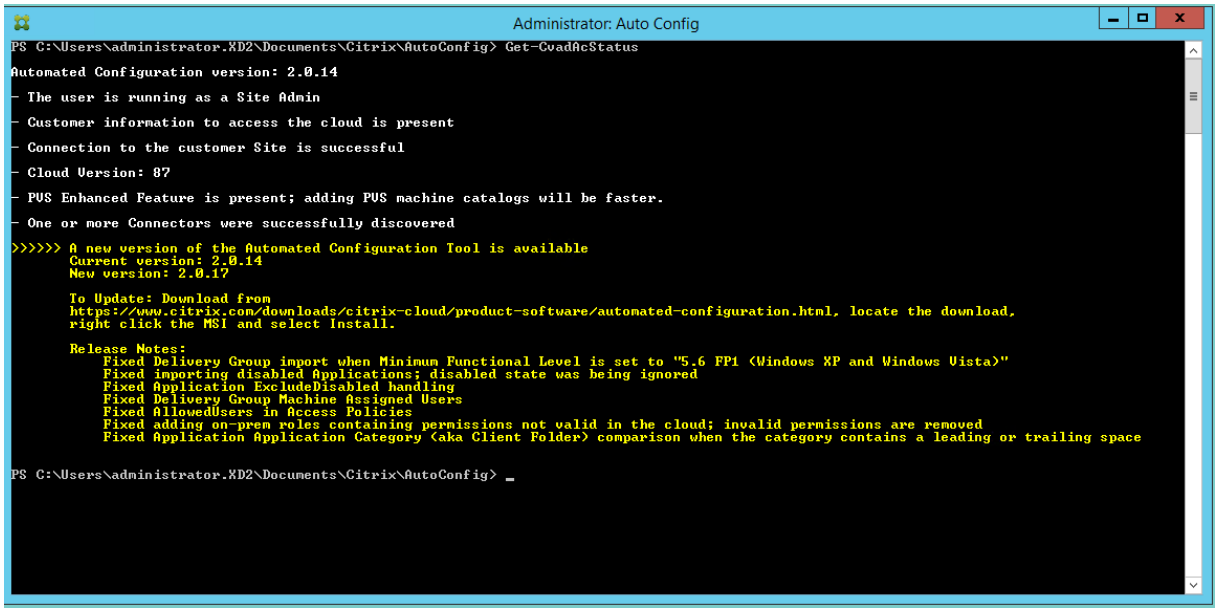
Baixar a Configuração Automatizada

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.

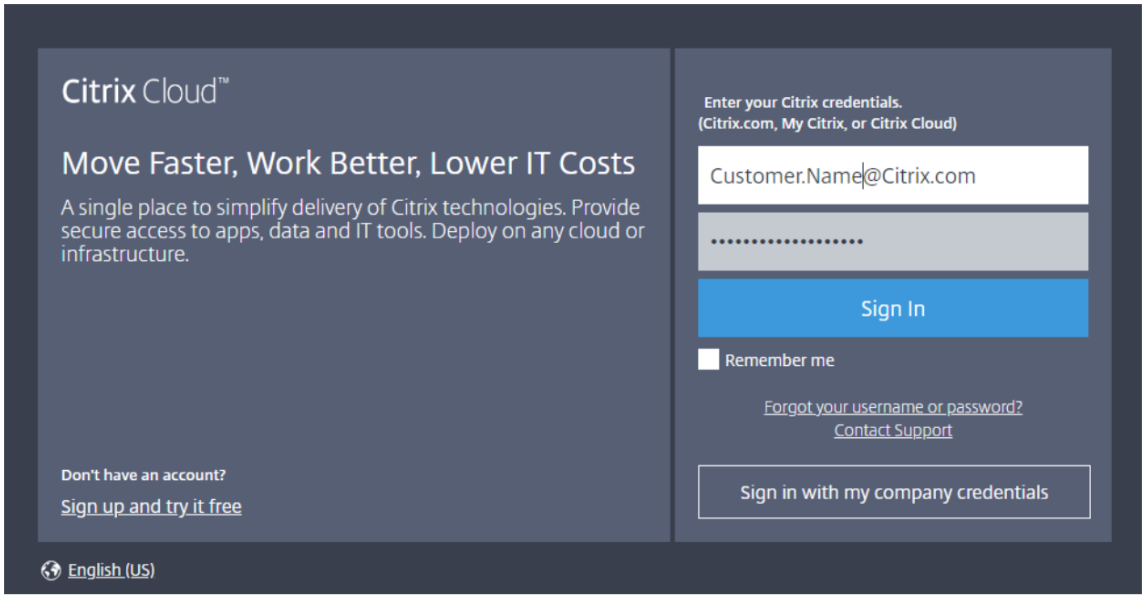
Geração do ID do consumidor, o ID do cliente e a chave secreta

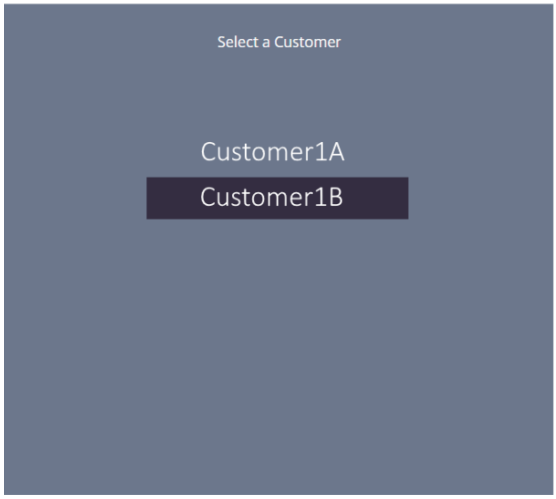
Antes de iniciar a migração usando a Configuração Automatizada, você precisa do seu ID de consumidor do Citrix Cloud e deve criar um ID de cliente e uma chave secreta para importar sua configuração para o Citrix Cloud. Todos os cmdlets que acessam a nuvem exigem esses valores.

As etapas a seguir permitem recuperar o ID de consumidor e criar o ID do cliente e a chave secreta.

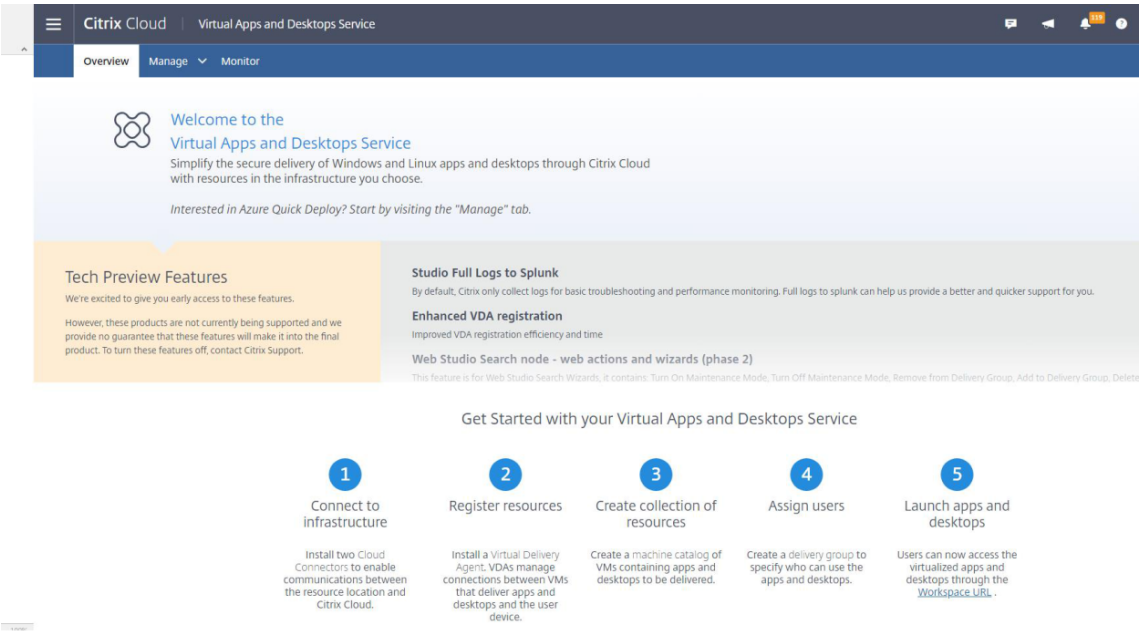
Para recuperar a **ID do consumidor**:

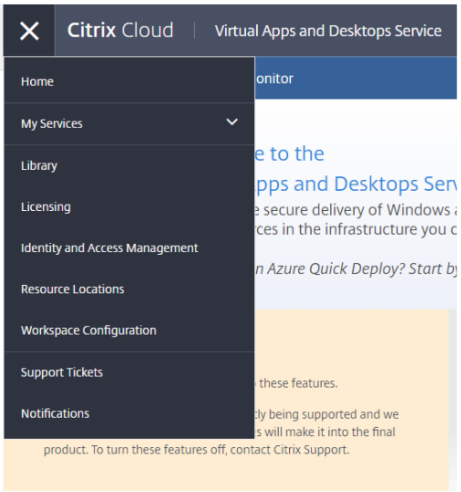
1. Faça login na sua conta do Citrix Cloud e selecione o consumidor.



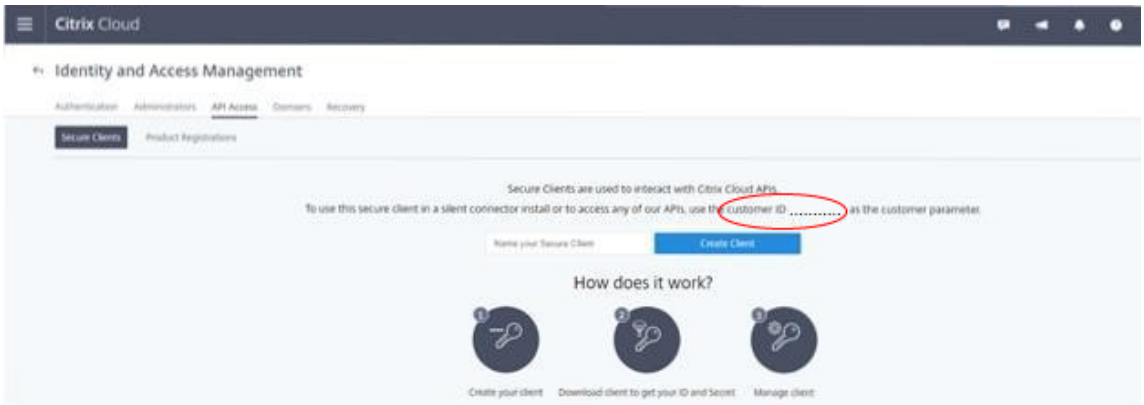


2. Clique no menu de hambúrguer e selecione **Identity and Access Management** no menu suspenso.



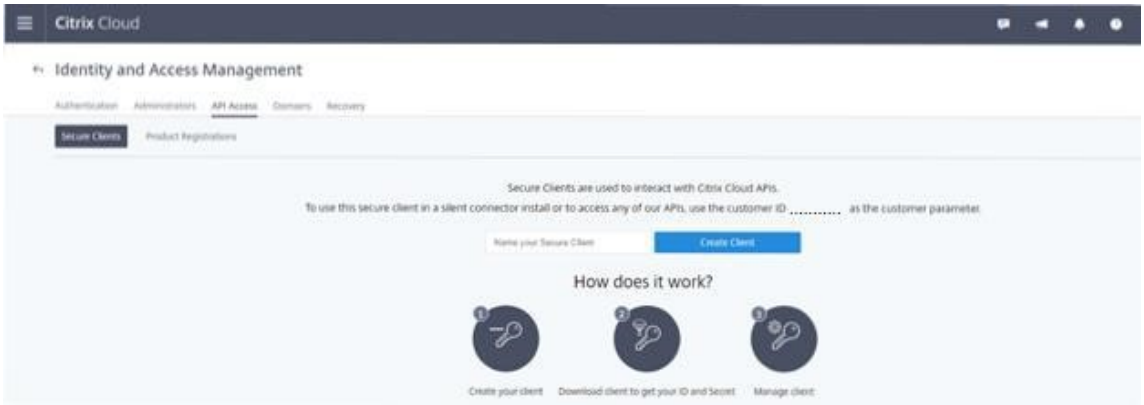


3. A **ID do consumidor** está localizada na página **Identity and Access Management**.

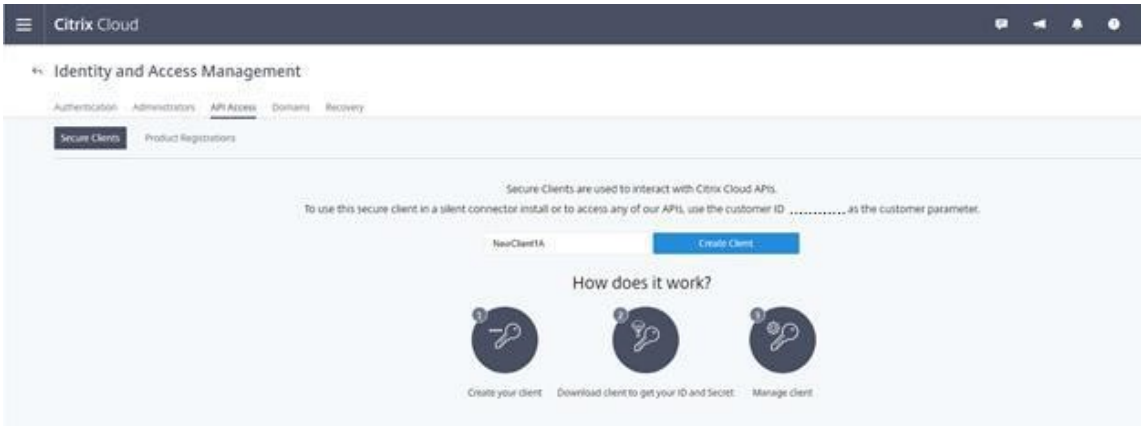


Para recuperar o **ID do cliente** e a **chave secreta**:

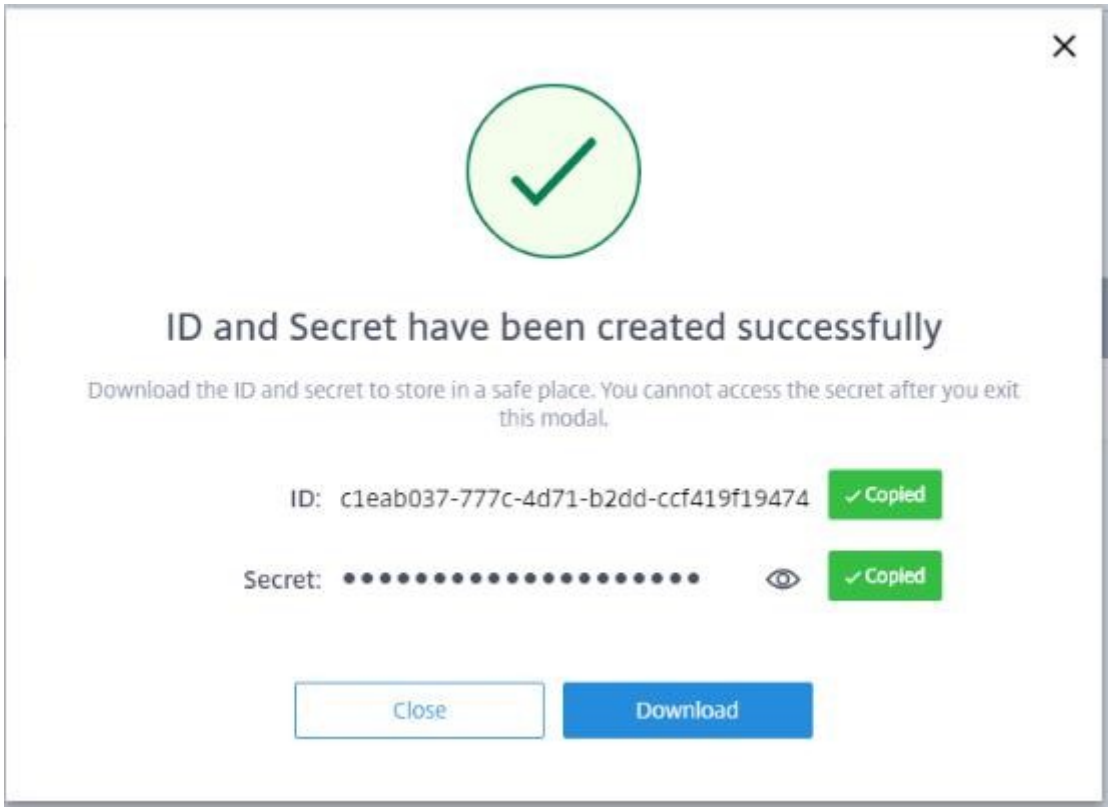
1. Na página **Identity and Access Management**, clique na guia **API Access**.



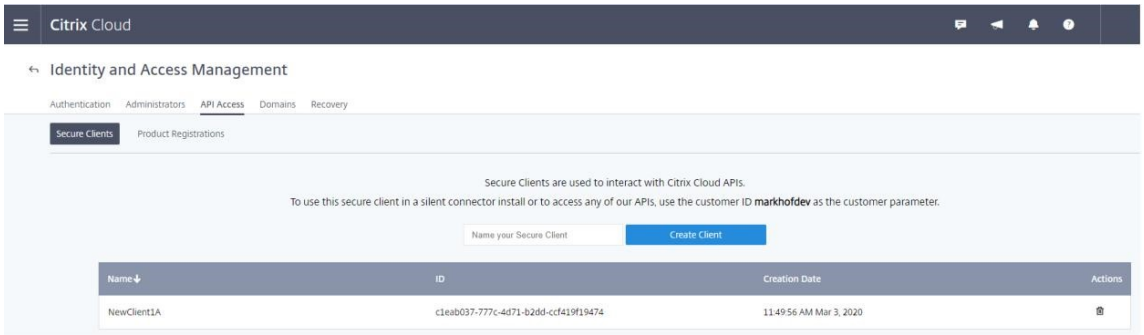
2. Digite um nome na caixa. Esse nome é usado para diferenciar entre vários IDs de cliente e chaves secretas. Clique em **Create Client** para criar o ID do cliente e a chave secreta.



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 Customer-Info.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:

```
1            Zone-1: Cloud-RL-1
2
3            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-CvadAcSiteActiveStateClo` 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.

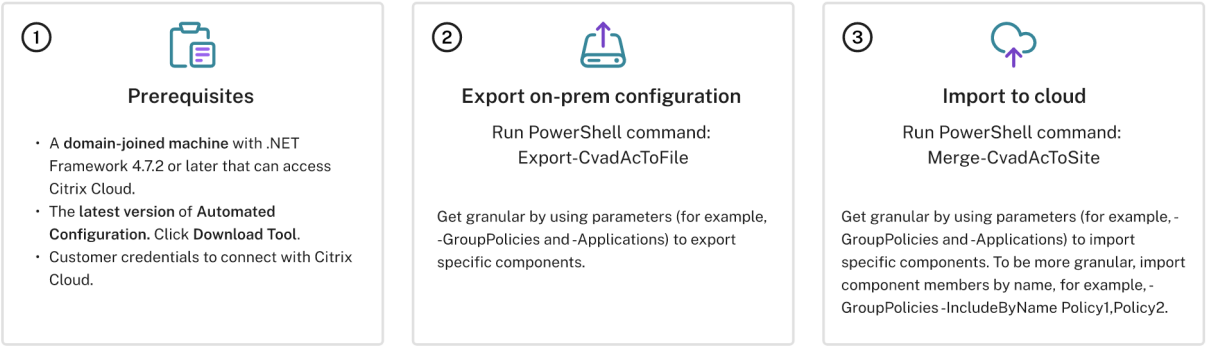
Quando a migração for concluída, se você quiser excluir esse catálogo do site local, selecione sair da VM e da conta do AD. Caso contrário, eles serão excluídos e o site da nuvem será deixado apontando para a VM excluída.

Migração do local para a nuvem

November 9, 2023

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

November 9, 2023

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.

```yaml
    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_"
```



```
14        StoreFrontPrefix: "East_"
15        TagPrefix: "East_"
16        AdminScopeSuffix: "_east"
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "" # Important: leave this empty
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
             is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        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.

```yml
        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_"
```



```
9         ApplicationUserPrefix: "East_"
10        DeliveryGroupPrefix: "East_"
11        GroupPolicyPrefix: "East_"
12        HostConnectionPrefix: "East_"
13        MachineCatalogPrefix: "East_"
14        StoreFrontPrefix: "East_"
15        TagPrefix: "East_"
16        AdminScopeSuffix: "_east"
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
             is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        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”
```

Migração da nuvem para a nuvem

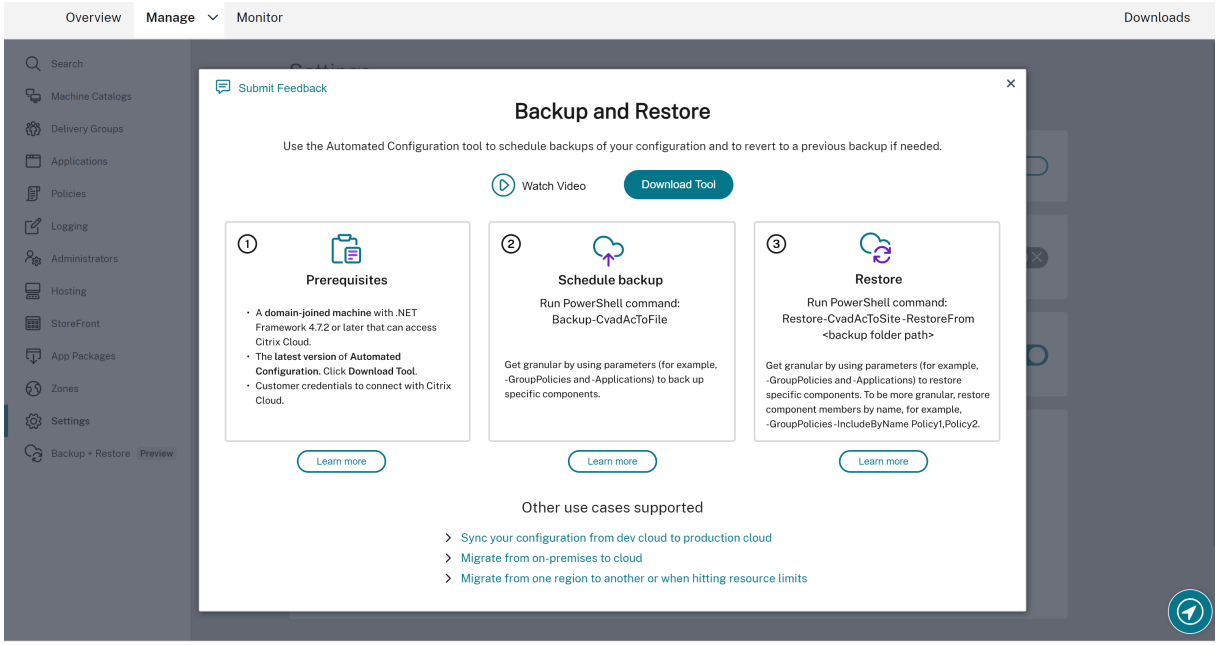
June 24, 2022

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.

Cmdlets da ferramenta de configuração automatizada

November 9, 2023

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`
		`Merge-CvadAcToSite`
		`New-CvadAcToSite`
		`Sync-CvadAcToSite`
		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`.

Cmdlets de nuvem para nuvem	`Backup-CvadAcToFile`	Faz backup de toda a configuração do seu site na nuvem.
		`Restore-CvadAcToSite`
		`Remove-CvadAcFromSite`
		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`.

Outros cmdlets básicos	`Compare-CvadAcToSite`	Compara os arquivos .yml locais com a configuração da nuvem.

Categoria	Cmdlet	Descrição
Cmdlets relacionados a pré-requisitos	New-CvadAcCustomerInfoFile	Criar um arquivo de informações do consumidor.
		Set-CvadAcCustomerInfoFile
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
		Test-CvadAcConnectionWithSite
		Find-CvadAcConnector
		Get-CvadAcCustomerSites
		New-CvadAcTemplateToFile
		Show-CvadAcDocument
		Find-CvadAcInFile
Cmdlets de ativação do site	Set-CvadAcSiteActiveStateOnPrem	Define o estado do site local como ativo ou inativo.
		Set-CvadAcSiteActiveStateCloud
Mesclagem de vários cmdlets de sites locais	New-CvadAcSiteMergingInfo	Cria um conjunto de informações de prefixo/sufixo de mesclagem de sites.
		Set-CvadAcSiteMergingInfo

	`Remove-CvadAcSiteMergingInfo`

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 Controlador de Entrega.		Cadeia de caracteres
`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`

Nome	Descrição	Obrigatório?	Tipo
`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
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

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*.		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 `$false`
`AddOnly`	Quando definido como `$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 importados têm precedência.		SwitchParameter
`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 `$false` para remover componentes.		`$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`

Nome	Descrição	Obrigatório?	Tipo
`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 importados têm precedência.		SwitchParameter
`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
`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`
`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
`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`

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`
`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 importados têm precedência.		SwitchParameter

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

Nome	Descrição	Obrigatório?	Tipo
`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 `$false` para suprimir a exibição do log.		`$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

- `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
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters

Nome	Descrição	Obrigatório?	Tipo
`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 `$false`
`AddOnly`	Quando definido como `$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 importados têm precedência.		SwitchParameter
`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

Nome	Descrição	Obrigatório?	Tipo
`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 `$false`
`AddOnly`	Quando definido como `$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 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

Nome	Descrição	Obrigatório?	Tipo
`SecurityCsvFileSpec`	A especificação de arquivo totalmente qualificada que aponta para o arquivo SecurityClient.csv baixado do Citrix Identity and Access Management. O CustomerID deve ser especificado quando esse parâmetro é usado.		Cadeia de caracteres

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
`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

Nome	Descrição	Obrigatório?	Tipo
`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 CustomerID deve ser especificado quando esse parâmetro é usado.		Cadeia de caracteres

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 con-

sumidor (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 ferramenta não estiver sendo executada em um Delivery Controller.		Cadeia de caracteres

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 consumidor para substituir o local e o nome padrão. Esse parâmetro é ignorado quando é fornecido o parâmetro `CustomerId`.		Cadeia de caracteres
`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
`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 ativo. Os caracteres curinga '*'e '?'são suportados em nomes.		Lista de cadeias de caracteres
`Unique`	Indicar apenas membros encontrados exclusivamente.		SwitchParameter

Nome	Descrição	Obrigatório?	Tipo
`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

Nome	Descrição	Obrigatório?	Tipo
`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

- `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 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 suportados em nomes.		Lista de cadeias 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 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 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

- `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<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
                {
```



```
3
4                    public Dictionary<string, Dictionary<string,
                        ActionResultValues >> EvaluationResults;
5                    public int                  Added;
6                    public int                  Updated;
7                    public int                  Deleted;
8                    public int                  NoChange;
9                    public int                  TotalChanged;
10                   public EvaluationResults     OverallResult;
11                   public string               CloudBackupFolder;
12                   public string               SourceBackupFolder;
13                }
14
15               Where:
16               public enum ActionResultValues
17              {
18
19                   Add,
20                   Update,
21                   Delete,
22                   Identical,
23                   DoNothing
24                }
25
26               public enum EvaluationResults
27               {
28
29                   Success,
30                   Failure,
31                   Skipped
32                }
```

`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

December 21, 2022

> **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)
`StopImmediately`	O processamento é interrompido quando um erro é encontrado.

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 Auto-Config. 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 CvadAc-Security.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.

Migre cargas de trabalho entre locais de recursos usando o Image Portability Service

December 6, 2023

O Image Portability Service simplifica o gerenciamento de imagens entre plataformas. 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.

O fluxo de trabalho do Image Portability começa quando você usa o Citrix Cloud para iniciar a migração de uma imagem da sua localização local para a sua assinatura da nuvem pública. Depois de preparar a sua imagem, o Image Portability Service ajuda você a transferir a imagem para a sua assinatura da nuvem pública e prepará-la para execução. Por fim, o Citrix Provisioning ou o Machine Creation Services provisionam a imagem na sua assinatura da nuvem pública.

Componentes

Os componentes do Image Portability Service incluem:

- Serviços do Citrix Cloud
- Citrix Credential Wallet
- Dispositivo Citrix Connector
- Máquina virtual Compositing Engine
- Scripts de exemplo do PowerShell

Serviços do Citrix Cloud

A API do Citrix Cloud Services é um serviço de API REST que interage com o Image Portability Service. Usando o serviço da API REST, você pode criar e monitorar trabalhos do Image Portability. Por exemplo, você faz uma chamada de API para iniciar um trabalho do Image Portability, como exportar um disco e, em seguida, faz chamadas para obter o status do trabalho.

Citrix Credentials Wallet

O serviço Citrix Credentials Wallet gerencia com segurança as credenciais do sistema, permitindo que o Image Portability Service interaja com os seus ativos. Por exemplo, ao exportar um disco do vSphere para um compartilhamento SMB, o Image Portability Service requer credenciais para abrir uma conexão com o compartilhamento SMB para gravar o disco. Se as credenciais estiverem armazenadas no Credential Wallet, o Image Portability Service pode recuperar e usar essas credenciais.

Esse serviço oferece a capacidade de gerenciar totalmente suas credenciais. A API do Cloud Services atua como um ponto de acesso, permitindo que você crie, atualize e exclua credenciais.

Compositing Engine

O Compositing Engine é o trabalhador central do Image Portability Service. O Compositing Engine (CE) é uma única máquina virtual criada no início de um trabalho de exportação ou preparação do Image Portability. Essas VMs são criadas no mesmo ambiente em que o trabalho está ocorrendo. Por exemplo, ao exportar um disco do vSphere, o CE é criado no servidor vSphere. Da mesma forma, ao executar um trabalho de preparação em Azure, AWS ou Google Cloud, o CE é criado no Azure, na AWS ou no Google, respectivamente. O CE monta o seu disco nele mesmo e, em seguida, faz as manipulações necessárias no disco. Após a conclusão do trabalho de preparação ou exportação, a VM CE e todos os seus componentes são excluídos.

Dispositivo Connector

O dispositivo Connector, que executa o software do provedor para gerenciar recursos IPS, é executado em seu ambiente (no local e na sua assinatura do Azure, da AWS ou do Google Cloud) e atua como um controlador de trabalhos individuais. Ele recebe instruções de trabalho do serviço de nuvem e cria e gerencia as máquinas virtuais do Compositing Engine. A máquina virtual do dispositivo Connector atua como um ponto único e seguro de comunicação entre os serviços de nuvem e seus ambientes. Implante um ou mais dispositivos Connector em cada uma das suas localizações do recurso (no local, Azure, AWS ou Google Cloud). Um dispositivo Connector é implantado em cada localização do recurso para segurança. Ao colocar o dispositivo Connector e o Compositing Engine juntos, a postura de segurança da implantação aumenta muito, pois todos os componentes e comunicações são mantidos dentro da sua localização do recurso.

Módulos PowerShell

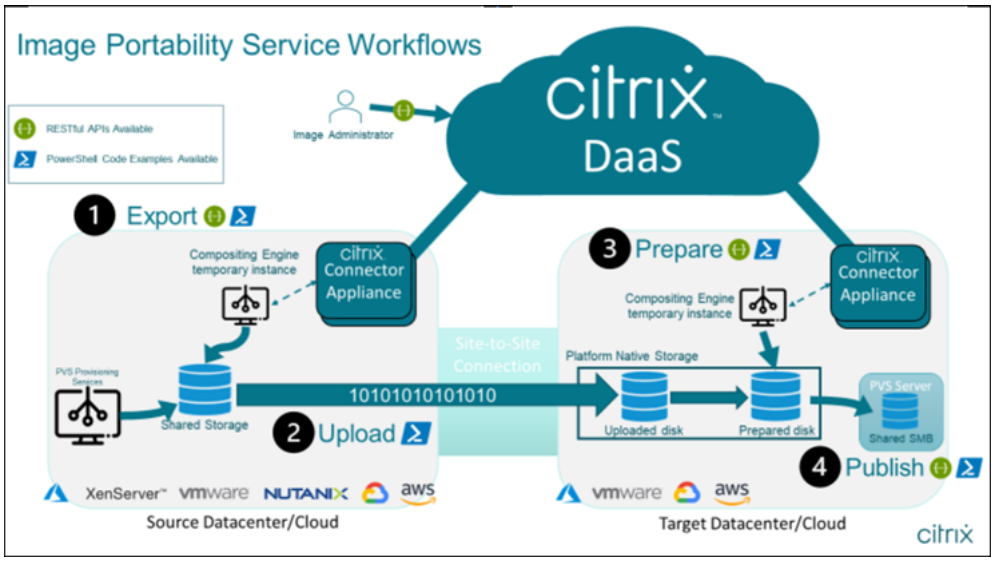
Fornecemos uma coleção de módulos do PowerShell para uso em scripts como ponto de partida para desenvolver sua própria automação personalizada. Os módulos fornecidos são suportados como são, mas você pode modificá-los, se necessário, para sua implantação.

A automação do PowerShell usa os parâmetros de configuração fornecidos para compor uma chamada REST para o serviço da API do Citrix Cloud para iniciar o trabalho e, em seguida, fornecer atualizações periódicas à medida que o trabalho avança.

Se deseja desenvolver sua própria solução de automação, você pode fazer chamadas para o serviço de nuvem diretamente usando sua linguagem de programação preferida. Consulte o portal da API para obter informações detalhadas sobre como configurar e usar os pontos de extremidade REST e os módulos do PowerShell do Image Portability Service.

Fluxos de Trabalho

O Image Portability Service usa um fluxo de trabalho multifásico para preparar uma imagem de catálogo mestre a partir da localização do recurso local para sua assinatura de nuvem pública. O serviço exporta a imagem da plataforma de hipervisor local e você a carrega para a sua assinatura de nuvem pública (nosso utilitário de upload do PowerShell fornecido pode ajudar a automatizar isso). Em seguida, o Image Portability prepara a imagem para ser compatível com a sua plataforma de nuvem pública. Por fim, a imagem é publicada e está pronta para ser implantada como um novo catálogo de máquinas na localização do recurso na nuvem.



Esses fluxos de trabalho de alto nível são baseados na configuração de provisionamento de origem e destino da imagem (Machine Creation ou Citrix Provisioning). O fluxo de trabalho escolhido determina quais etapas de trabalho do Image Portability são necessárias.

Consulte a tabela a seguir para entender quais trabalhos são necessários para cada um dos fluxos de trabalho IPS suportados.

Fluxo de trabalho (origem para destino)	Exportar	Carregar	Preparar	Publicar
MCS para MCS	S	S	S	N
PVS para MCS*	N	S	S	N
PVS para PVS no Azure/Google Cloud*	N	S	S	S

Fluxo de trabalho (origem para destino)	Exportar	Carregar	Preparar	Publicar
MCS para PVS no Azure/Google Cloud	S	S	S	S

*Presume que você tem a imagem original como um Citrix Provisioning vDisk e não precisa exportá-la diretamente do hipervisor da plataforma de origem.

Requisitos

Para começar a usar o Image Portability, você deve atender aos seguintes requisitos.

Uma imagem do Catálogo de máquinas Citrix

O IPS requer o uso de imagens que tenham uma das seguintes configurações testadas:

- Windows Server 2016, 2019 e 2022H2
- Windows 10 ou 11
- Provisionado usando Machine Creation Services ou Citrix Provisioning
- Citrix Virtual Apps and Desktops VDA versão 1912CU6, 1912CU7, 2203CU1, 2203CU2, 2212, 2303 ou 2305
- Serviços de Área de Trabalho Remota ativados para acesso ao console no Azure

O Image Portability Service é compatível com os seguintes hipervisores e plataformas na nuvem:

Plataformas de origem:

- VMware vSphere 7.0 e 8.0
- Citrix Hypervisor/XenServer 8.2
- Nutanix Prism Element 3.x
- Microsoft Azure
- Google Cloud Platform

Plataformas de destino:

- VMware vSphere 8.0

- Microsoft Azure
- AWS
- Google Cloud Platform

Um dispositivo Citrix Connector

Você precisa de um dispositivo Citrix Connector instalado e configurado em cada localização do recurso em que planeja usar o Image Portability. Por exemplo, se você usar o Image Portability para mover uma imagem do vSphere para o Azure, a AWS e o Google Cloud, precisará de pelo menos quatro dispositivos Citrix Connector:

Consulte Implantar dispositivos Connector para obter instruções detalhadas.

Um compartilhamento de arquivos (Windows) SMB

Você precisa de um **compartilhamento de arquivos SMB** do Windows para armazenamento temporário de dados durante trabalhos de exportação hospedados na localização do recurso no local onde você está usando o Image Portability Service. Certifique-se de que o espaço livre disponível no compartilhamento seja pelo menos o dobro do tamanho configurado do sistema de arquivos da imagem.

Uma máquina para executar scripts do PowerShell

Certifique-se de que a máquina executando os scripts do PowerShell tenha o seguinte:

- PowerShell versão 5.1.
- Uma conexão de rede rápida para o compartilhamento de arquivos SMB. Pode ser a mesma máquina que está hospedando o compartilhamento de arquivos.
- Uma conexão de rede rápida com as plataformas de nuvem pública em que você planeja usar o recurso Image Portability. Por exemplo, Azure, AWS ou Google Cloud.

  Consulte a seção Preparar uma máquina para o PowerShell para obter detalhes sobre como baixar e configurar os módulos do Image Portability da Galeria do PowerShell.

Seu ID de cliente do Citrix Cloud

Certifique-se de ter uma assinatura do Citrix DaaS válida.

Para continuar, você precisa de acesso ao Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Se você não tiver acesso, entre em contato com seu representante da Citrix.

Consulte a documentação de Introdução a APIs para obter instruções sobre como criar e configurar um cliente de API para usar com o Image Portability.

Configuração e permissões necessárias do Azure

Para que o Image Portability Service execute ações no seu recurso do Azure, você precisa conceder permissões a determinados recursos do Azure para a entidade de serviço do Azure usada pelo Image Portability Service. Para obter a lista detalhada, consulte Permissões necessárias do Microsoft Azure.

Você pode atribuir a função de **Colaborador** à entidade de serviço no recurso associado. Ou, para atribuir as permissões mínimas necessárias, você pode criar funções personalizadas com as permissões necessárias e atribuí-las à entidade de serviço com o escopo dos recursos apropriados.

Consulte a documentação do Azure para configurar funções de segurança para a sua entidade de serviço do Azure e para criar funções personalizadas.

Configuração e permissões necessárias do Google Cloud

Para que o Image Portability Service execute ações no seu projeto do Google Cloud, você concede permissões a determinados recursos para a entidade de serviço do Google Cloud usada pelo Image Portability Service.

Para ver a lista detalhada, consulte Permissões necessárias do Google Cloud.

Você pode atribuir essas permissões usando as seguintes funções:

- Cloud Build Editor
- Compute Admin
- Storage Admin
- Service Account User

Consulte a documentação do Google Cloud para obter mais informações sobre como configurar as permissões da conta de serviço.

Configuração e permissões necessárias da Amazon Web Services

Para executar fluxos de trabalho do Image Portability Service com uma conta da Amazon Web Services (AWS), a respectiva identidade do Identity and Access Management (IAM) deve ter as permissões corretas.

Para ver a lista detalhada, consulte as Permissões necessárias da AWS.

Instalar o Image Portability Service

Para instalar o Image Portability Service você deve:

- Implantar dispositivos Connector
- Preparar uma máquina para o PowerShell
- Adicionar credenciais ao Credential Wallet

Implantar dispositivos Connector

O Image Portability exige que os dispositivos Citrix Connector criem trabalhos do Image Portability. Os dispositivos Connector ajudam a proteger as interações com seus ambientes locais e na nuvem pública. Os dispositivos Connector se comunicam de volta com o Image Portability Service para informar sobre o status do trabalho e a integridade geral do serviço.

Para implantar e configurar o dispositivo Connector em seu ambiente, siga as etapas em Dispositivo Connector para Cloud Services.

Observe a configuração de hardware e o acesso à porta de rede necessários para o dispositivo ao planejar sua implantação.

Quando seu dispositivo é implantado e registrado, os componentes necessários para habilitar o Image Portability são instalados automaticamente.

Preparar uma máquina para o PowerShell

Para ajudá-lo a começar a usar o Image Portability, criamos módulos do PowerShell que você pode personalizar e usar com o serviço.

As seções a seguir descrevem como preparar uma máquina para executar os scripts do PowerShell. Esses scripts são apenas alguns exemplos. Modifique ou aprimore-os para atender às suas necessidades.

> **Nota:**
>
> Após a instalação inicial, use o **Update-Module** para atualizar o módulo do PowerShell.

Requisitos do PowerShell Para usar os scripts do PowerShell, você precisa do seguinte:

- Um computador Windows para executar os scripts do PowerShell que conduzem os trabalhos do Image Portability. O computador:
  - Tem a versão mais recente do PowerShell.

- Tem uma conexão de rede de 10 Gb/s ou melhor para o compartilhamento de arquivos SMB no local e uma conexão rápida com a sua nuvem pública (Azure, AWS ou Google Cloud, por exemplo).
- Pode ser o mesmo computador que hospeda o compartilhamento de arquivos.
- É um computador executando o Windows 10, Windows Server 2019 ou Windows Server 2022, com os patches mais recentes da Microsoft.
- Pode se conectar à Galeria do Microsoft PowerShell para baixar as bibliotecas do PowerShell necessárias.

Dependendo da sua versão do Windows, talvez seja necessário desativar o suporte ao TLS 1.0/1.1. Consulte a documentação de suporte do Microsoft PowerShell Gallery TLS para obter mais informações.

Por padrão, o PowerShell não se autentica automaticamente por meio de um servidor proxy. Verifique se você configurou a sua sessão do PowerShell para usar o seu servidor proxy, de acordo com a Microsoft, e as práticas recomendadas do fornecedor do proxy.

Se você vir erros ao executar os scripts do PowerShell relacionados a uma versão ausente ou antiga do PowerShellGet, será necessário instalar a versão mais recente da seguinte maneira:

```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

Instale bibliotecas e módulos O Image Portability Service utiliza bibliotecas da Galeria do Microsoft PowerShell para conduzir operações de portabilidade.

> **Importante:**
>
> Após a instalação inicial, use o **Update-Module** para instalar novas versões.

1. Execute o seguinte comando do PowerShell para baixar os módulos mais recentes:

```
Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Scope CurrentUser
<!--NeedCopy-->
```

   - Para alterar a variável de ambiente PATH:

     Pressione **Y** e **Enter** para aceitar.
   - Para instalar o provedor NuGet:

     Pressione **Y** e **Enter** para aceitar.
   - Se informado sobre um repositório não confiável:

     Pressione **A** (Sim para todos) e **Enter** para continuar.

2. Confirme se todos os módulos necessários foram baixados executando o comando:

```
Get-InstalledModule -Name Citrix.*
<!--NeedCopy-->
```

Esse comando retorna uma saída semelhante à seguinte:

Nome	Repositório	Descrição
Citrix.Image.Uploader	PSGallery	Comandos para carregar um VHD(x) para uma conta de armazenamento do Azure, AWS ou GCP e obter informações sobre um VHD(x)
Citrix.Workloads.Portability	PSGallery	Cmdlet autônomo para o trabalho de imagem do Citrix Image Portability Service

Atualize os módulos para a versão mais recente Execute o seguinte comando para atualizar o script para a versão mais recente.

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

Instale o SDK do PowerShell remoto do Citrix Virtual Apps and Desktops O Image Portability Service requer o SDK do PowerShell remoto do Citrix Virtual Apps and Desktops para criar e gerenciar trabalhos de portabilidade no Citrix Cloud.

Baixe e instale o SDK do PowerShell remoto no seu computador.

Instale componentes de terceiros específicos da plataforma O módulo PowerShell do Image Portability Service não instala dependências de terceiros. Portanto, você pode limitar a instalação apenas às plataformas que deseja. Se você estiver usando uma das plataformas a seguir, siga as instruções relevantes para a instalação das dependências da plataforma:

VMware Se você estiver criando trabalhos do Image Portability que se comunicam com o seu ambiente VMware, execute o seguinte comando para instalar os módulos do VMware PowerShell necessários.


```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

Amazon Web Services Se você estiver criando trabalhos do Image Portability na AWS, baixe e instale a Interface de linha de comando da AWS e execute estes comandos para instalar os módulos necessários do AWS PowerShell:

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

Azure Se você estiver criando trabalhos do Image Portability no Azure, baixe e instale os utilitários de linha de comando do Azure e execute esses comandos para instalar os módulos necessários do Azure PowerShell:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

Google Cloud Se você estiver criando trabalhos do Image Portability no Google Cloud, baixe e instale o SDK do Google Cloud no seu computador.

Desinstale scripts e módulos Execute os seguintes comandos para desinstalar os módulos usados pelo software Image Portability.

> **Nota:**
>
> Scripts e componentes de terceiros não são removidos automaticamente ao desinstalar módulos IPS.

Para desinstalar os módulos:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images
    .Uploader" | Uninstall-Module
<!--NeedCopy-->
```

Adicionar credenciais ao Credential Wallet

Para cenários de automação de ponta a ponta, você pode configurar o Image Portability Service para autenticar de forma não interativa com o Citrix Cloud, a sua nuvem pública e os recursos locais. Além

disso, o Image Portability Service usa credenciais armazenadas no Citrix Credential Wallet sempre que as nossas APIs são autenticadas diretamente com os seus recursos locais e na nuvem pública. Definir credenciais conforme descrito nesta seção é uma etapa necessária para executar trabalhos de exportação, preparação e publicação.

Ao executar trabalhos, o Image Portability Service requer acesso a recursos que você pode controlar. Por exemplo, para que o Image Portability Service exporte um disco de um servidor vSphere para um compartilhamento SMB, o serviço precisa de acesso de login para os dois sistemas. Para proteger essas informações de conta, o Image Portability Service usa o serviço Citrix Credential Wallet. Esse serviço armazena suas credenciais na carteira com um nome definido pelo usuário. Quando quiser executar um trabalho, forneça o nome da credencial a ser usada. Além disso, essas credenciais podem ser atualizadas ou excluídas da carteira a qualquer hora.

As credenciais geralmente são armazenadas para estas plataformas:

- Microsoft Azure
- AWS
- Google Cloud
- Compartilhamento SMB
- VMware vSphere
- Nutanix AHV
- XenServer

Para gerenciar credenciais, consulte Credentials Management na seção Image Portability Service APIs do Developer API Portal.

Usar o Image Portability Service

Preparar imagens nas localizações de recursos locais para sua assinatura de nuvem pública requer a criação de trabalhos do Image Portability no Citrix Cloud. Você pode criar um trabalho para fazer chamadas diretas de API para o serviço no seu script ou programa, ou usando os módulos do PowerShell de exemplo que desenvolvemos para automatizar chamadas de API. Consulte Image Portability Service Developer API Portal para obter informações sobre o uso de APIs REST e módulos do PowerShell para criar trabalhos IPS.

Publicar catálogos de máquinas usando o Citrix Provisioning

O Image Portability Service (IPS) é usado com o Machine Creation Services (MCS) no Azure, na AWS e no Google Cloud, ou com o Citrix Provisioning (PVS) no Azure ou no Google Cloud. Você pode combinar as soluções PowerShell e REST descritas neste guia com as ferramentas da sua plataforma, as APIs da sua plataforma ou os SDKs do Citrix DaaS para criar um fluxo de trabalho completo e automatizado

para criar um catálogo de máquinas com base na imagem preparada. Dependendo da plataforma de nuvem escolhida, podem ser necessárias etapas intermediárias entre a conclusão de um trabalho de preparação de IPS e a criação de um catálogo ou atribuição a um alvo de PVS.

AWS Os trabalhos de preparação do IPS na AWS produzem um volume. O Machine Creation Services exige uma Amazon Machine Image (AMI) durante a criação do catálogo. Para gerar uma AMI da imagem migrada, primeiro você precisa criar um instantâneo da imagem do volume resultante e depois criar uma AMI com base nesse instantâneo. Isso pode ser feito com a interface de linha de comando (CLI) da AWS:

```
> aws ec2 create-snapshot --volume-id <VolumeId>
> aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```

O <VolumeId> é a saída do trabalho de preparação do IPS. A AMI resultante pode ser usada como uma imagem mestre do MCS.

Um exemplo de script do PowerShell para automatizar essa parte do fluxo de trabalho é fornecido no módulo Citrix.Workloads.Portability como um script chamado `New-ImsAwsImage.ps1`.

Azure No Azure, o IPS produz discos gerenciados que podem ser usados diretamente como imagens mestre do MCS. Para atribuir a imagem resultante aos destinos PVS, o IPS fornece uma operação de "publish"para copiar o disco gerenciado para um arquivo VHD(x) na sua loja PVS.

Google Cloud Os trabalhos de preparação do IPS no Google Cloud produzem um disco. O MCS exige um modelo de instância do Google Cloud. O processo de criação de um modelo de instância MCS a partir de um disco é abordado em detalhes em Preparar uma instância de VM mestre e um disco permanente.

Para destinos PVS no Google Cloud, o IPS fornece uma operação de "publish"para copiar o disco para um arquivo VHD(x) na sua loja PVS.

Automatizar a configuração do VDA

Ao preparar uma imagem gerenciada pela Citrix que se originou no local, você pode reconfigurar o VDA na imagem para dar suporte ao ambiente de destino para o qual a imagem está sendo preparada. O Image Portability Service pode aplicar alterações de configuração do VDA em tempo real durante

a fase de preparação do fluxo de trabalho. Há três parâmetros de configuração que definem como o VDA opera na imagem migrada: **InstallMisa**, **InstallPvs** e **XdReconfigure**. Defina esses parâmetros ao criar trabalhos IPS da seguinte forma:

```
InstallMisa = $true
<!--NeedCopy-->
```

Configurar o **InstallMisa** como **true** permite que o Image Portability Service instale quaisquer componentes do VDA ausentes que seriam necessários para provisionar a imagem usando o MCS.

Configurar o **InstallMisa** como **true** também requer a configuração do **CloudProvisioningType** como **Mcs**.

```
InstallPvs = '2206'
<!--NeedCopy-->
```

A versão do servidor PVS com a qual a imagem é usada: (string, default $null). Por exemplo: 2206, 7.33 ou 2203cu1 (necessário se o tipo de provisionamento for PVS).

Defina **InstallPvs** para a versão do servidor PVS em que a imagem está sendo implantada. Quando **InstallPvs** é definido, o Image Portability Service (IPS) instala automaticamente a versão especificada do software do dispositivo de destino PVS na imagem durante os trabalhos de preparação. O IPS suporta as duas compilações mais recentes (versão básica ou atualizações cumulativas) para os dois últimos lançamentos de Long-Term Service Release (LTSR) e Current Releases (CR).

A configuração do **InstallPvs** também exige que o **CloudProvisioningType** seja configurado como **Pvs**.

Para **InstallMisa** e **InstallPvs**, observe o seguinte:

- Somente as versões recentes de LTSR e CR do VDA suportam esse recurso.
- Se os componentes necessários já estiverem presentes para o VDA instalado, nenhuma alteração será feita, mesmo que os parâmetros sejam configurados.
- Para versões suportadas do VDA, o Image Portability instala a versão apropriada dos componentes necessários, mesmo que os componentes necessários do VDA não estejam presentes.
- Para versões não suportadas do VDA, a reconfiguração falha e uma mensagem é registrada no log se os componentes necessários do VDA não estiverem presentes. O trabalho de preparação é concluído mesmo que a reconfiguração do VDA não seja concluída.

XdReconfigure requer um dos seguintes valores: **controllers** ou **site_guid**. Alguns exemplos de parâmetros de configuração usando cada valor:

Usando **controllers**:

```
XdReconfigure = @(
    [pscustomobject]@{
```



```
3
4           ParameterName = 'controllers'
5           ParameterValue = 'comma-separated-list-of-your-cloud-connectors
               -fqdns'
6        }
7
8  )
9  <!--NeedCopy-->
```

onde o **ParameterValue** é a lista de FQDNs dos novos DDCs para onde você deseja apontar o VDA. Vários DDCs podem ser especificados no formato separado por vírgulas.

Usando **site_guid**:

```
1  XdReconfigure = @(
2      [pscustomobject]@{
3
4          ParameterName = 'site_guid'
5          ParameterValue = 'active-directory-site-guid'
6       }
7
8  )
9  <!--NeedCopy-->
```

XdReconfigure também aceita valores que são suportados ao executar o instalador da linha de comando do VDA com a opção de instalação **/reconfigure**, por exemplo, **XenDesktopVdaSetup.exe /reconfigure**. Alguns exemplos desses valores: **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors** e **wem_server**. Para obter uma lista completa das opções de linha de comando de reconfiguração do VDA, consulte a documentação do VDA do Citrix DaaS.

> **Nota:**
>
> Você pode usar `-DryRun` enquanto executa seus comandos para validar sua configuração e as configurações de rede do seu dispositivo conector.

Referência

Esta seção detalha as informações de referência técnica, com base em suas necessidades.

Permissões exigidas pelo Image Portability Services

Esta seção detalha as permissões exigidas pelo Image Portability Service em cada uma das plataformas suportadas, local e na nuvem.

Permissões necessárias do Connector Appliance O Connector Appliance precisa acessar as seguintes URLs para preparar imagens no Image Portability Service:


```
*.layering.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

Permissões necessárias do VMware vCenter As seguintes permissões do vCenter são necessárias para executar o trabalho de disco de exportação IPS em um ambiente VMware. Essas permissões podem ser encontradas em **Roles** na seção **Access Control** do painel de administração do vCenter.

```
-  Cryptographic operations
    -  Direct Access

-  Datastore
    -  Allocate space
    -  Browse datastore
    -  Low level file operations
    -  Remove file

-  Folder
    -  Create folder
    -  Delete folder

-  Network
    -  Assign network

-  Resource
    -  Assign virtual machine to resource pool

-  Virtual machine
    -  Change Configuration
        -  Add existing disk
        -  Add new disk
        -  Remove disk

    -  Edit Inventory
        -  Create from existing
        -  Create new
        -  Remove

    -  Interaction
        -  Power off
        -  Power on
<!--NeedCopy-->
```

Permissões necessárias do Microsoft Azure O Image Portability exige que a sua conta de serviço do Azure tenha as seguintes permissões.

Quando o grupo de recursos a ser usado para o Compositing Engine é especificado (ou seja, na propriedade *resourceGroup* em uma solicitação REST ou no parâmetro *-AzureVmResourceGroup* ao usar os comandos Citrix.Workloads.Portability PowerShell), as seguintes permissões são necessárias no escopo do grupo de recursos.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/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.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
<!--NeedCopy-->
```

Quando o grupo de recursos a ser usado para o Compositing Engine não é especificado, as seguintes permissões são necessárias no escopo da assinatura.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```


As permissões a seguir são necessárias no escopo do grupo de recursos de destino especificado (ou seja, o grupo de recursos especificado na propriedade *targetDiskResourceGroupName* em uma solicitação REST ou no parâmetro *-TargetResourceGroup* ao usar o PowerShell).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

As permissões a seguir são necessárias no escopo do grupo de recursos de rede virtual especificado (ou seja, o grupo de recursos especificado na propriedade *virtualNetworkResourceGroupName* em uma solicitação REST ou no parâmetro *-AzureVirtualNetworkResourceGroupName* ao usar o PowerShell).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> **Importante:**
>
> A opção `ceVmSku` de trabalhos “prepare”e “prepareAndPublish”controla o tipo de VM do Azure para a qual o disco gerenciado resultante é adequado. Você deve selecionar uma ceVMSku com a mesma família e versão das VMs que você pretende provisionar a partir da imagem de saída. O valor padrão de `Standard_D2S_v3` é adequado para ser executado em todas as máquinas da família v3 D. Com a v4 e as SKUs de VM mais recentes, a Microsoft tornou opcional o disco de recurso temporário conectado às VMs. Isso afeta o posicionamento correto de pagefile. Se você pretende usar uma SKU de VM *sem* um disco de recurso temporário para as máquinas que você provisiona usando a imagem de saída, certifique-se de que sua ceVmSku também não tenha um disco de recurso temporário. Se a ceVmSku for um tipo com um disco de recurso temporário, o IPS move o pagefile do Windows para esse disco. Você recebe uma caixa de diálogo de aviso em cada login se usar um disco preparado dessa forma em uma SKU que não tenha um disco de recurso temporário. Se a ceVmSku não tiver um disco temporário, o pagefile será configurado no volume raiz do sistema. Isso poderá resultar em cobranças de E/S não intencionais se você usar uma imagem preparada dessa forma em uma SKU que inclua um disco de recurso temporário.

Permissões necessárias do Google Cloud O Image Portability exige que a sua conta de serviço do Google Cloud tenha as seguintes permissões:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
```



```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Permissões necessárias da AWS O Image Portability requer que você anexe um documento de política JSON com a seguinte configuração ao usuário do IAM (Identity and Access Management):

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
```



```
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--NeedCopy-->
```

> **Nota:**
>
> Se desejar, você pode reduzir ainda mais o escopo do Recurso, conforme necessário.

Permissões necessárias da Nutanix AHV Image Portability exige que você seja Cluster Admin na configuração da Nutanix AHV.

Permissões necessárias do XenServer O Image Portability exige que você tenha, no mínimo, a função “VM Admin”para o pool em que o host XenServer está.

Trabalho em rede O Image Portability Service (IPS) cria uma VM funcional chamada Compositing Engine (CE) para realizar operações de imagem. Todos os Connector Appliances no local de recursos associado devem ser capazes de se comunicar com o CE via HTTP.
Toda comunicação entre um Connector Appliance (CA) e o CE é iniciada pelo CA, exceto por uma única exceção no caso do vSphere, em que ocorre a comunicação HTTPS bidirecional entre o CE e o CA.

Em ambientes de nuvem (Azure, AWS, Google Cloud), o CE é criado com um endereço IP privado. Portanto, o CE deve estar na mesma rede virtual que o CA ou em uma rede virtual acessível a partir do CA.

Além disso, para trabalhos que envolvem arquivos em um compartilhamento SMB (por exemplo, trabalhos de exportação), o CE deve estar em uma rede com conectividade com o compartilhamento SMB.

Consulte a documentação da API do Image Portability Service para obter detalhes sobre como especificar a rede a ser usada para o CE em cada plataforma compatível.

Para trabalhos "prepare", o sistema operacional contido na imagem é inicializado (no CE) para realizar a especialização e outras tarefas. Se a imagem contiver agentes de gerenciamento ou de segurança que telefonam para um servidor de controle, esses processos podem interferir no processo de preparação.

Se a opção de cancelamento de ingresso no domínio for especificada, a conectividade da rede poderá afetar os resultados. Se a VM do Compositing Engine puder acessar o controlador de domínio do Active Directory pela rede, o cancelamento do ingresso removerá a conta do computador do domínio. Isso interrompe a associação de domínio da VM de origem da qual a imagem foi extraída.

Portanto, recomendamos isolar a rede fornecida para a operação a partir de outros recursos da rede. Isso pode ser feito por meio do isolamento da sub-rede ou com regras de firewall. Consulte Isolamento de rede para obter detalhes.

Em alguns ambientes de hipervisor locais, o hipervisor pode ser configurado com um certificado de servidor TLS, que não é confiável pelo conjunto de autoridades de certificação raiz confiáveis da AC ou não corresponde ao nome do host do servidor. Em tais situações, o **IPS fornece propriedades de solicitação de trabalho** que podem ser usadas para contornar o problema. Consulte Certificados TLS para obter detalhes.

Proxies de rede Se o tráfego de rede entre a autoridade de certificação e a Internet passar por um proxy que executa a introspecção de TLS, pode ser necessário adicionar a Autoridade de Certificação Raiz do proxy (ou seja, o certificado que o proxy usa para assinar os certificados TLS que ele gera) ao conjunto de autoridades de certificação raiz da AC. Consulte Registrar seu Connector Appliance no Citrix Cloud para obter mais informações.

Isolamento de rede

- Azure

  No Azure, o CE é criado por padrão com um grupo de segurança de rede (NSG) anexado à sua NIC se a entidade de serviço do Azure usada na operação tiver as permissões necessárias do Azure [1].

  Esse NSG está configurado para bloquear todo o tráfego de entrada/saída do CE, exceto:

  - saída SMB (porta 445)

  - entrada HTTPS (porta 443)
  - o necessário para os serviços internos do Azure.

  O uso do NSG pode ser forçado definindo a propriedade *networkIsolation* na solicitação de trabalho como *true*. Nesse caso, o trabalho falha se a entidade de serviço usada na operação não tiver as permissões necessárias. O uso do NSG pode ser desativado definindo a propriedade *networkIsolation* como *false*.

- AWS

Na AWS, para obter o isolamento da rede do CE, você pode criar um grupo ou grupos de segurança de rede que bloqueiam todo o tráfego indesejado e, na solicitação de trabalho, atribuir os grupos de segurança à instância do CE usando o parâmetro de solicitação *securityGroupIds*, que usa uma lista de IDs de grupos de segurança como valor.

- Google Cloud

No Google Cloud, para obter o isolamento da rede do CE, você pode criar regras de firewall que bloqueiam todo o tráfego indesejado e depois aplicá-las ao CE por meio de marcações de rede. O IPS cria o CE com a marcação de rede *compositing-engine* e você pode atribuir a ela outras marcações de rede usando o parâmetro de solicitação de trabalho *networkTags*, que usa uma lista de tags como um valor.

Certificados TLS Se o certificado do servidor do hipervisor for assinado por uma autoridade que não confia na autoridade de certificação, há duas abordagens alternativas que podem ser usadas para resolver o problema.

1. Especifique na solicitação de trabalho um certificado adicional da Autoridade de Certificação Raiz para usar na verificação do certificado. Esse certificado deve ser a Autoridade de Certificação Raiz usada para assinar o certificado do servidor do hipervisor.
2. Especifique na solicitação de trabalho a impressão digital SHA-1 do certificado do servidor do hipervisor. Nesse caso, a validação do certificado é feita verificando se a impressão digital SHA-1 do certificado retornado pelo hipervisor corresponde à fornecida na solicitação de trabalho. Observe que esse método pode não funcionar se houver um proxy de interceptação de TLS entre o CE e o hipervisor.

Os parâmetros de solicitações de trabalho acima, fornecidos respectivamente abaixo para cada plataforma, são:

- vSphere

  1. vCenterSslCaCertificate
  2. vCenterSslFingerprint

- Nutanix

    1. prismSslCaCertificate
    2. prismSslFingerprint

- XenServer

    1. xenSslCaCertificate
    2. xenSslFingerprint

Consulte a documentação da API do Image Portability Service para obter mais detalhes.

Os erros de validação do certificado também podem ocorrer quando ocorre uma incompatibilidade entre o nome do host do servidor do hipervisor e o nome do host em seu certificado. Nesse caso, a correspondência de nomes de host pode ser desativada definindo o seguinte parâmetro como *true* na solicitação de trabalho:

- vSphere
    - vCenterSslNoCheckHostname
- Nutanix
    - prismSslNoCheckHostname
- XenServer
    - xenSslNoCheckHostname

Documentação relacionada

- Documentação da API do Image Portability Service
- Dispositivo Connector para Cloud Services
- Documentação do Google Cloud
- Contas de serviço do Google Cloud
- Registro e autenticação do aplicativo Microsoft Azure

1. If Se um grupo de recursos explícito estiver sendo usado para a operação, as seguintes permissões no escopo do grupo de recursos:
   - Microsoft.Network/networkSecurityGroups/join/action
   - Microsoft.Network/networkSecurityGroups/read
   - Microsoft.Network/networkSecurityGroups/write

   Otherwise the following permissions at the scope of the subscription if no explicit resource group is being used:

   - Microsoft.Network/networkSecurityGroups/delete
   - Microsoft.Network/networkSecurityGroups/join/action

- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkSecurityGroups/write

Impressão

June 24, 2022

Gerenciar impressoras em seu ambiente é um processo de vários estágios:

1. Familiarize-se com os conceitos de impressão, se não estiver ainda.
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 se aplica melhor ao seu ambiente.
3. Configure seu ambiente de impressão selecionando um método de provisionamento de impressora e criando políticas para implantar seu design de impressão. Atualize políticas quando novos funcionários ou servidores forem adicionados.
4. Teste uma configuração de impressão piloto antes de implantá-la para os usuários.
5. Faça a manutenção do seu ambiente de impressão Citrix gerenciando drivers de impressora e otimizando o desempenho de impressão.
6. Solucione os problemas que possam surgir.

Para obter informações completas sobre a impressão em um ambiente Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), comece com Impressão. A partir desse artigo, você pode passar para:

- Exemplo de configuração de impressão
- Práticas recomendadas
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

Instalar o Servidor de Impressão Universal em seus servidores de impressão

1. Cada servidor de impressão deve ter 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**.

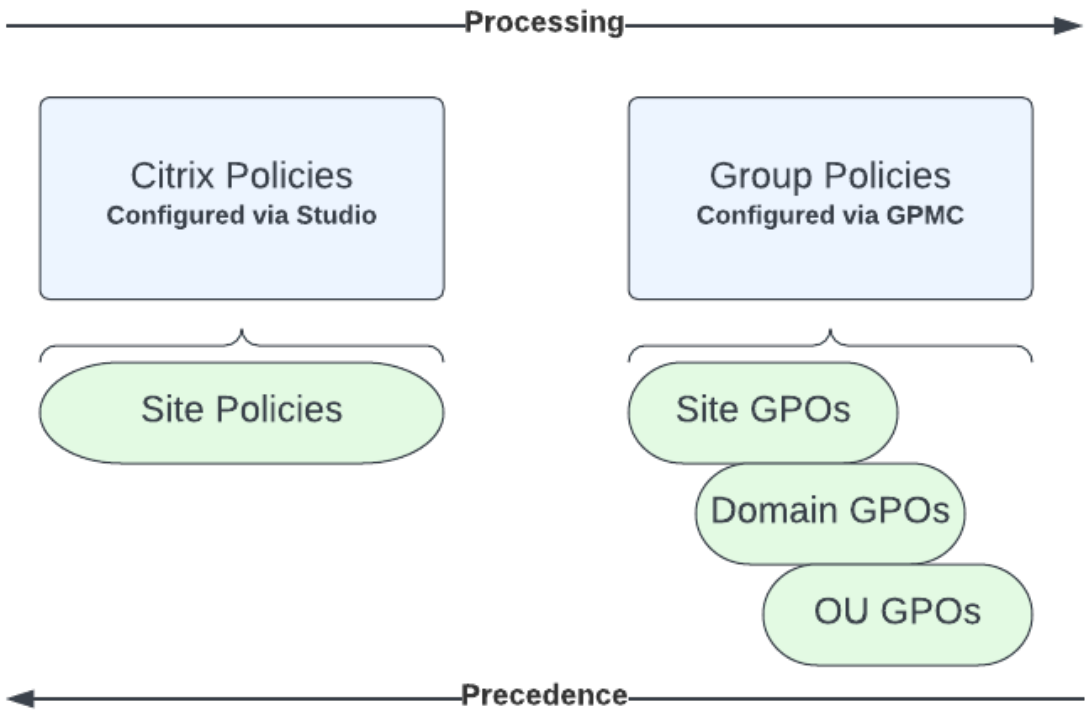
Depois de instalar o servidor de impressão universal, configure-o usando as orientações em Provisionar impressoras.

Políticas

April 14, 2023

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.

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 objetos) para políticas. Se você não atribuir políticas especificamente aos filtros, as configurações serão aplicadas a todas as sessões do usuário.



Você pode aplicar políticas em diferentes níveis da rede. As configurações da política colocadas no nível do GPO da Unidade Organizacional têm a maior precedência na rede. As políticas no nível do

GPO do Domínio substituem as políticas no nível do Objeto de Política de Grupo do Site. O nível do Objeto da Política de Grupo do Site substitui todas as 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 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 (GPMC) da Microsoft 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 para Modelagem para ajudar os administradores a comparar os parâmetros de configuração em 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 desativada substitui uma configuração ativada com classificação inferior. As configurações de política não definidas são ignoradas e não substituem as configurações de classificação inferior.

As políticas do Web Studio também podem ter conflitos com 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 login 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 do site
   c) Políticas de domínio
   d) Políticas da UO (unidade organizacional)

> **Nota:**
>
> - Pode ser que nem todas as políticas estejam presentes nos quatro níveis. Para a maioria dos clientes, somente as políticas do site são usadas. As políticas locais exigem que o usuário faça login no VDA para editar as políticas. Portanto, essas políticas quase nunca são usadas.
> - Não oferecemos suporte à mistura de políticas Windows e Citrix no mesmo GPO.

Para obter informações completas sobre as políticas da Citrix, consulte o seguinte:

- Trabalhar com políticas
- Modelos de política
- Criar políticas

- Priorizar, modelar, comparar e solucionar problemas de políticas
- Configurações de política padrão
- Referência a configurações de política

> **Nota:**
>
> As referências às configurações da política do Citrix DaaS são iguais às configurações da política do Citrix Virtual Apps and Desktops. Portanto, você também pode consultar a seção de Referência a configurações de política na documentação do Citrix Virtual Apps and Desktops do Citrix DaaS.

Trabalhar com políticas

May 30, 2023

Configurar políticas Citrix para controlar o acesso do usuário e os ambientes de sessão. As políticas da Citrix são o método mais eficiente de controlar as configurações de conexão, segurança e largura de banda. Você pode criar políticas para grupos específicos de usuários, dispositivos ou tipos de conexão. Cada política pode conter várias configurações.

Ferramentas para trabalhar com políticas Citrix

- Studio –as políticas criadas usando o Studio são armazenadas no banco de dados do site, e as atualizações são enviadas para o VDA no caso de ocorrer qualquer das seguintes situações:
  - Quando o VDA se registra no Controller
  - Quando um usuário inicia uma sessão
- Console de gerenciamento de política de grupo –se o seu ambiente de rede usa o Active Directory e você tem permissão para gerenciar a política de grupo, você pode usar o Console de Gerenciamento de Política de Grupo (GPMC) para criar e editar políticas para o seu site. No console, você pode configurar Objetos de Política de Grupo (GPOs) com as configurações e filtros desejados. Essas políticas terão prioridade sobre as políticas configuradas no Studio. Para obter mais informações, consulte CTX238166.

Ordem e precedência de processamento de políticas

As configurações de política de grupo são processadas na seguinte ordem:

1. GPO do site Citrix DaaS (armazenado no banco de dados do site)
2. GPOs de nível de domínio
3. Unidades organizacionais

No entanto, se configurações diferentes forem aplicadas à mesma política em dois objetos de política de grupo, as configurações da política processadas pela última vez substituirão as configurações processadas anteriormente. Essa configuração significa que as configurações de política têm precedência na seguinte ordem:

1. Unidades organizacionais
2. GPOs de nível de domínio
3. GPO do site Citrix DaaS (armazenado no banco de dados do site)

Ao usar várias políticas, você pode priorizar políticas que contêm configurações conflitantes. Para obter mais informações, consulte Priorizar, modelar, comparar e solucionar problemas de políticas.

Fluxo de trabalho para políticas Citrix

O processo para configurar políticas é o seguinte:

1. Crie a política.
2. Defina as configurações de política.
3. Atribua a política aos objetos da máquina e do usuário.
4. Priorize a política.
5. Verifique a política efetiva executando o assistente de modelagem de políticas de grupo Citrix.

> **Nota:**
>
> Abra o assistente de Modelagem de Política de Grupo Citrix navegando até a guia **Policies > Modeling** e clicando em **Launch Modeling Wizard** no painel **Actions**. A guia **Modeling** está disponível no Web Studio hospedado no Citrix Cloud por solicitação do cliente.

Navegue pelas políticas e configurações da Citrix

As configurações de política são classificadas em categorias com base na funcionalidade ou recurso que afetam. Por exemplo, a seção Profile Management inclui configurações de política para o Profile Management.

- As configurações do computador (configurações de política aplicáveis a máquinas) definem o comportamento das áreas de trabalho virtuais e são aplicadas quando uma área de trabalho virtual é iniciada. Essas configurações se aplicam mesmo quando não há sessões de usuário ativas na área de trabalho virtual.

- As configurações do usuário definem a experiência do usuário. As configurações do usuário são aplicadas quando um usuário se conecta ou se reconecta

Para acessar políticas, configurações ou modelos, selecione **Policies** no painel de navegação do Web Studio.

- A guia **Policies** lista todas as políticas. Quando você seleciona uma política, as guias na parte inferior exibem:
  - Overview –lista nome, prioridade, status ativado/desativado e descrição
  - Settings –lista todos de parâmetros configurados
  - Assigned To –lista o grupo de entrega. Você pode editar ou remover as configurações atribuídas. Aplique a política com base na associação ao grupo de entrega da área de trabalho executando a sessão. Para obter mais informações, consulte Criar políticas.
- A guia **Templates** lista os modelos personalizados e fornecidos pela Citrix que você criou. Quando você seleciona um modelo, as guias na parte inferior exibem:
  - Description (motivo para você querer usar o modelo)
  - Settings (lista de parâmetros configurados). Para obter mais informações, consulte Modelos de políticas.
  - A guia **Comparison** permite comparar as configurações em uma política ou modelo com as configurações de outras políticas ou modelos. Por exemplo, você pode verificar a definição de valores para garantir a conformidade com as práticas recomendadas. Para obter mais informações, consulte Priorizar, modelar, comparar e solucionar problemas de políticas.
  - Na guia **Modeling**, você pode simular cenários de conexão com as políticas Citrix. Para obter mais informações, consulte Priorizar, modelar, comparar e solucionar problemas de políticas.

  Para pesquisar uma configuração em uma política ou modelo:

  1. Selecione a política ou o modelo.
  2. Selecione a guia **Edit policy** ou **Edit Template**.
  3. Na página **Select Settings**, comece a digitar o nome da configuração.

  Você pode refinar sua pesquisa selecionando:

  - Uma categoria (por exemplo, Bandwidth)
  - A caixa de seleção **View selected only**
  - Para pesquisar somente as configurações que foram adicionadas à política selecionada.
- Para pesquisar uma configuração dentro de uma política:

  1. Selecione a política.

2. Selecione a guia **Settings** e digite o nome da configuração.

Uma política, uma vez criada, é independente do modelo usado. Você pode usar o campo **Description** em uma nova política para rastrear o modelo de origem usado.

Modelos de política

November 17, 2022

Os modelos são uma fonte para criar políticas a partir de um ponto de partida predefinido. Os modelos Citrix integrados, otimizados para ambientes específicos ou condições de rede, podem ser usados como:

- Uma fonte para criar suas próprias políticas e modelos para compartilhar entre sites.
- Uma referência para facilitar a comparação dos resultados entre implantações, pois você pode citar os resultados, por exemplo, "…ao usar o modelo Citrix x ou y…".
- Um método para comunicar políticas com o suporte da Citrix ou terceiros confiáveis. Você pode fazer isso importando ou exportando modelos.

Modelos Citrix incorporados

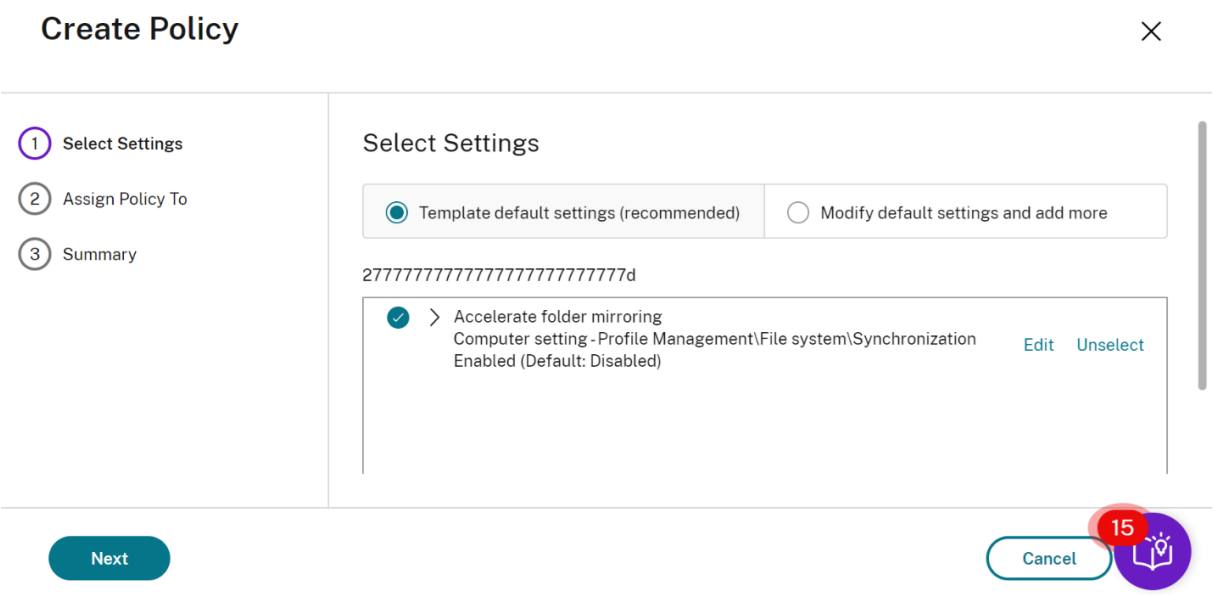
Os seguintes modelos de política estão disponíveis:

- **Very High Definition User Experience**. Este modelo impõe as configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde as políticas múltiplas são processadas por ordem de precedência.
- **High Server Scalability**. Aplique este modelo para economizar nos recursos do servidor. Este modelo equilibra a experiência do usuário e a escalabilidade do servidor. Ele oferece uma boa experiência de usuário, aumentando o número de usuários que você pode hospedar em um único servidor. Este modelo não usa um codec de vídeo para compressão de gráficos e impede a renderização multimídia do lado do servidor.
- **High Server Scalability-Legacy OS**. Este modelo de alta escalabilidade do servidor aplica-se apenas aos VDAs com Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo se baseia no modo gráfico legado, que é mais eficiente para os sistemas operacionais.
- **Optimized for NetScaler SD-WAN.** Aplique este modelo para usuários que trabalham em filiais com o NetScaler SD-WAN para otimizar a entrega do Citrix Virtual Desktops. (NetScaler SD-WAN é o novo nome de CloudBridge).

- **Optimized for WAN**. Este modelo é destinado a trabalhadores por tarefa 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 negocia a experiência de reprodução de vídeo e alguma escalabilidade do servidor para eficiência otimizada da largura de banda.
- **Optimized for WAN-Legacy OS**. Este modelo aplica-se apenas a VDAs com Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo se baseia no modo gráfico legado, que é mais eficiente para os sistemas operacionais.
- **Security and Control**. Use esse modelo em ambientes com baixa tolerância ao risco, para minimizar os recursos habilitados por padrão no Citrix Daas. Esse modelo inclui configurações que desabilitam o acesso ao seguinte:
  - Impressão
  - Área de transferência
  - Dispositivos periféricos
  - Mapeamento da unidade
  - Redirecionamento de portas
  - Aceleração flash nos dispositivos de usuários

  A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade do usuário por servidor.

Embora recomendemos usar os modelos Citrix integrados com suas configurações padrão, há configurações que não têm um valor recomendado específico. Por exemplo, **Overall session bandwidth limit**, incluído no otimizado para modelos WAN. Nesse caso, o modelo expõe a configuração para que o administrador entenda que essa configuração provavelmente se aplica ao cenário.



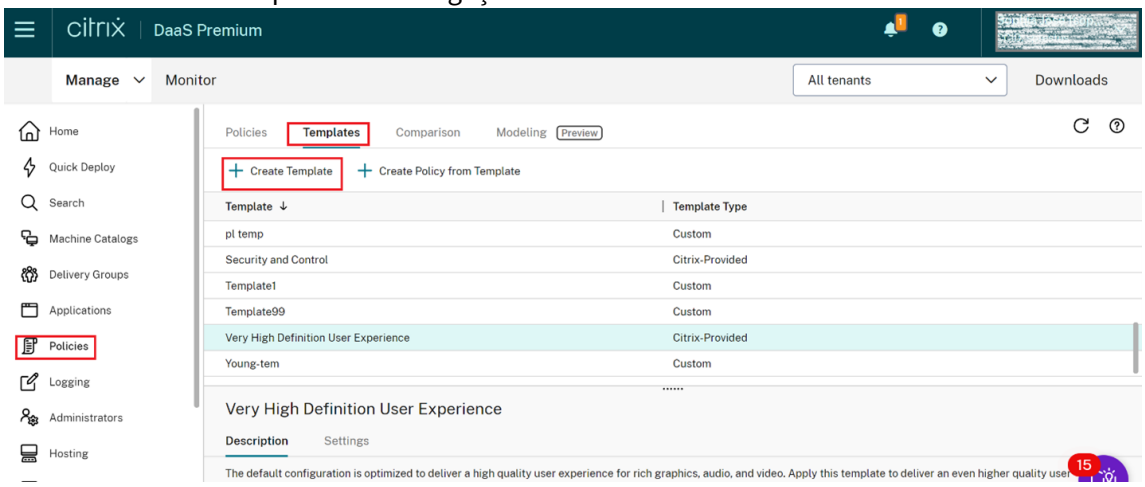
Considere que você está trabalhando com uma implantação (gerenciamento de políticas e VDAs) anterior a XenApp e XenDesktop 7.6 FP3. Além disso, exigem modelos High Server Scalability e Optimized for WAN. Nesse caso, use as versões SO Legado desses modelos quando se aplicarem.

> **Nota:**
>
> O Citrix cria e atualiza modelos internos. Não é possível modificar ou excluir esses modelos.

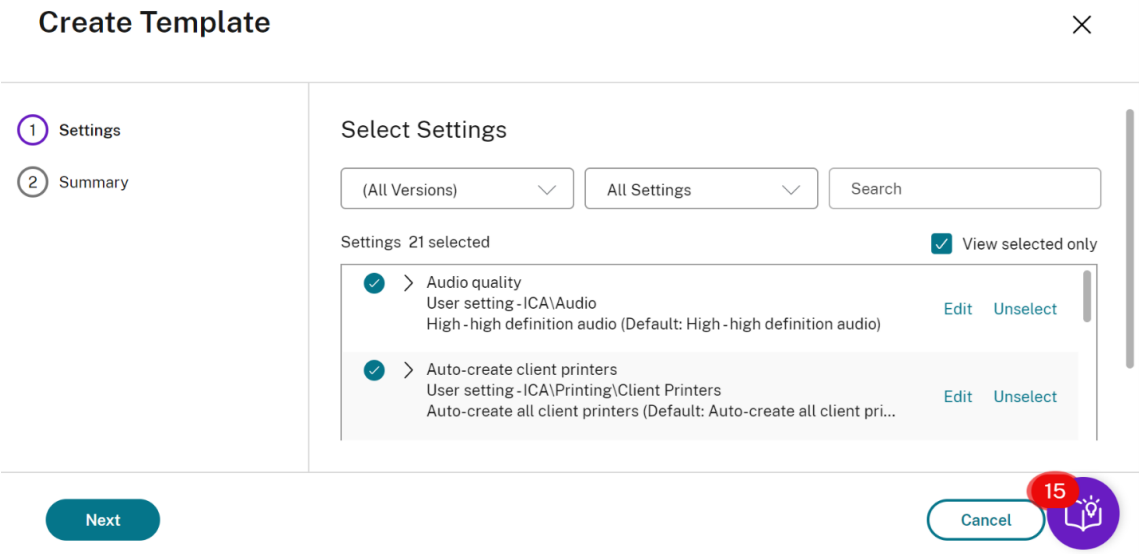
Criar e gerenciar modelos usando o Web Studio

Para criar um modelo baseado em um modelo:

1. Selecione **Policies** no painel de navegação do Web Studio.



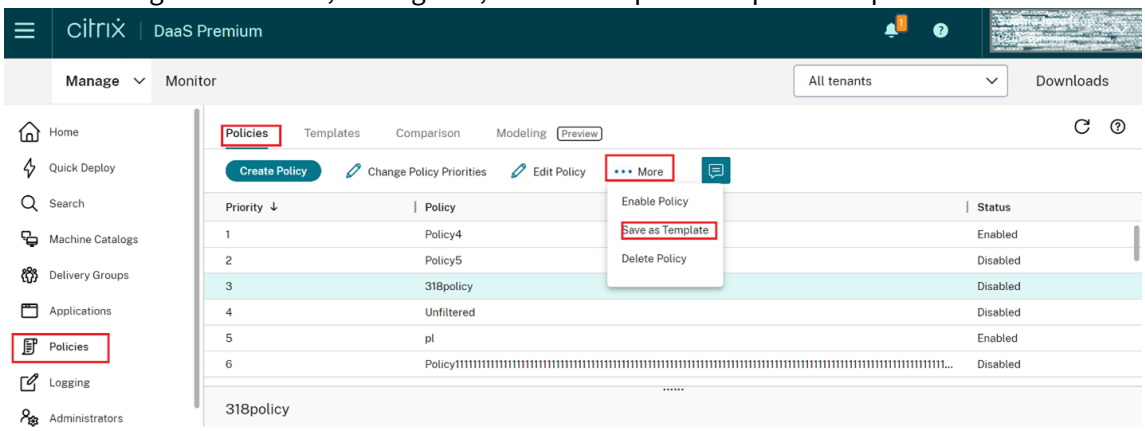
2. Selecione a guia **Templates** e, em seguida, selecione o modelo a partir do qual você criará o modelo.
3. Selecione a guia **Create Template**. A tela **Select Settings** é exibida.



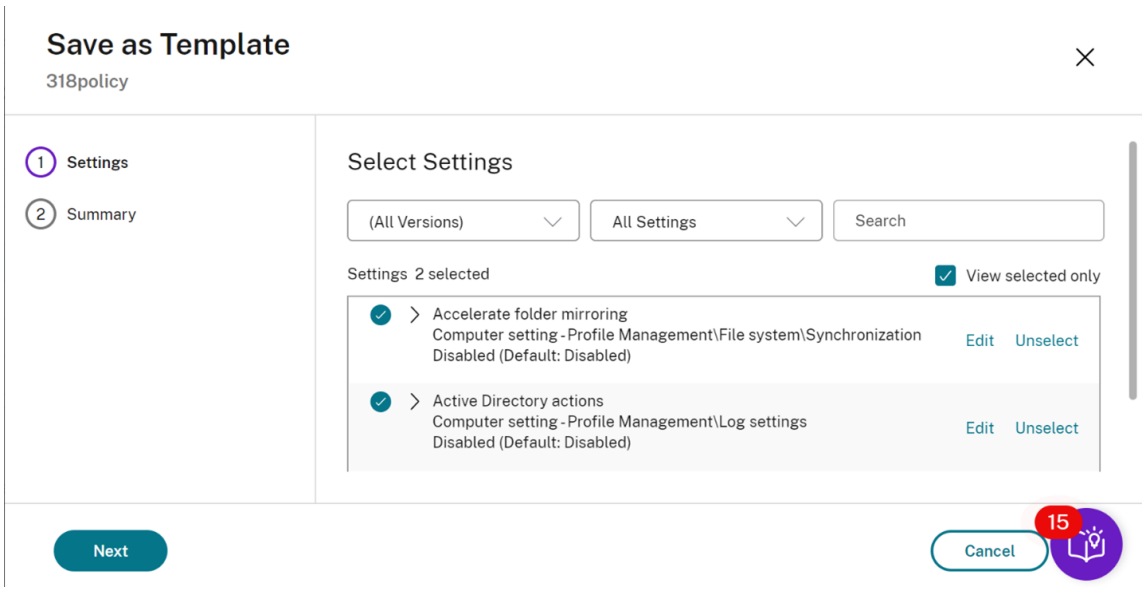
4. Selecione e defina as configurações de política que devem ser incluídas no modelo.
5. Clique em **Next**. A tela **Summary** é exibida.
6. Insira um nome para o modelo.
7. Clique em **Finish**. O novo modelo é exibido na guia Templates

Para criar um modelo baseado em uma política:

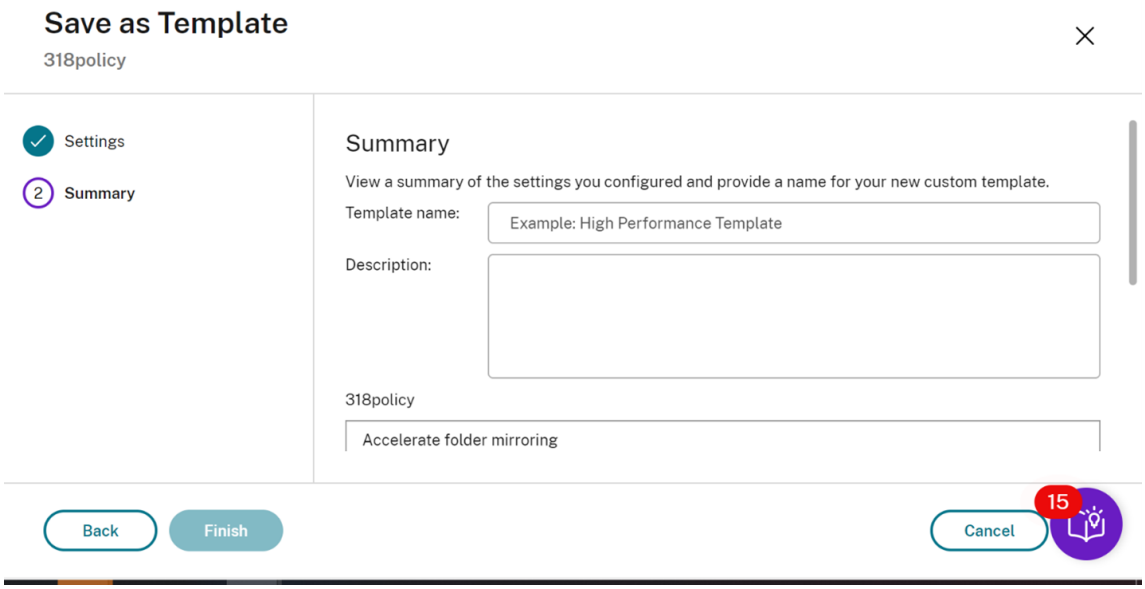
1. Selecione **Policies** no painel de navegação do Web Studio.
2. Selecione a guia **Policies** e, em seguida, selecione a política a partir da qual criar o modelo.



3. Clique na guia **More**.
4. Selecione **Save as Template**. A tela **Select Settings** é exibida.



5. Selecione e defina quaisquer novas configurações de política a serem incluídas no modelo.
6. Clique em **Next**. A tela **Summary** é exibida.



7. Insira um nome e uma descrição para o modelo e clique em **Finish**.

Criar políticas

November 9, 2023

Antes de criar uma política, decida qual grupo de usuários ou dispositivos ela poderá afetar. Você poderá criar uma política que é baseada na função de trabalho do usuário, tipo de conexão, disposi-

tivo do usuário ou localização geográfica.

Se você já criou uma política que se aplica a um grupo, considere editar essa política em vez de criar outra política. Depois de editar a política, defina as configurações apropriadas. Evite criar uma política exclusivamente para habilitar uma configuração específica ou para excluir a política da aplicação a determinados usuários.

Ao criar uma política, você pode baseá-la nas configurações em um modelo de política e personalizar as configurações conforme necessário. Você também pode criá-la sem usar um modelo e adicionar todas as configurações necessárias.

No Citrix Studio, as novas políticas criadas são definidas como desativadas, a menos que a caixa de seleção **Enable policy** esteja explicitamente marcada.

Durante a criação da política e ao definir as configurações, o sistema oferece a opção de visualizar o tipo das configurações. Você pode visualizar os seguintes tipos de configurações:

- All settings –Exibir todas as configurações de todas as versões do VDA
- Current settings only –Exibir configurações somente para as versões atuais do VDA
- Legacy settings only –Exibir configurações somente para as versões do VDA preteridas

Para visualizar as configurações ao definir as configurações:

1. Faça login no DaaS Premium.
2. No painel de navegação à esquerda, clique em **Políticas**.
3. Na guia **Policies**, clique em **Create Policy**.
4. Na tabela **Select Settings**, clique no menu suspenso ao lado de **Settings**.
5. Selecione uma das seguintes opções no menu suspenso:
    - All settings –Exibir todas as configurações de todas as versões do VDA
    - Current settings only –Exibir configurações somente para as versões atuais do VDA
    - Legacy settings only –Exibir configurações somente para as versões do VDA preteridas
6. A tabela Settings lista as configurações disponíveis com base na etapa anterior.

Configurações de política

As configurações de política podem estar ativadas, desativadas ou não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que elas não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

Ao definir as configurações para criar ou editar uma política, se todos os grupos de entrega estiverem desativados, o sistema exibirá um sinal de notificação de aviso **None of the elements in this filter is enabled**. Se pelo menos um grupo de entrega estiver ativado, o sistema não exibirá o sinal de aviso.

Para ver o aviso ao criar uma política:

1. Faça login no DaaS Premium.
2. No painel de navegação à esquerda, clique em **Políticas**.
3. Na guia **Policies**, clique em **Create Policy**.
4. Na tabela **Select Settings**, selecione qualquer configuração e clique em **Next**.
5. Na tabela **Assign Policy To**, selecione um filtro no menu suspenso.
6. Desmarque a caixa de seleção **Enable** e clique em **Save**.

> **Nota:**
>
> Nem todos os filtros permitem desmarcar a caixa de seleção **Enable**.
> Na tabela **Filters**, o filtro exibe o aviso.

Para ver o aviso ao editar uma política:

1. Faça login no DaaS Premium.
2. No painel de navegação à esquerda, clique em **Políticas**.
3. Na guia **Policies**, selecione qualquer uma das políticas listadas e clique em **Edit Policy**.
4. Na página **Edit Policy**, clique em **Assign Policy To** no painel de navegação à esquerda.
5. Na tabela **Filter**, selecione ou clique em **Edit** no filtro necessário:
   - Se um filtro não tiver o botão **Edit**, selecione o filtro.
   - Se um filtro tiver o botão de edição, clique em **Edit**.
6. Desmarque a opção **Enable** e clique em **Save**.

> **Nota:**
>
> Nem todos os filtros permitem desmarcar a caixa de seleção **Enable**.
> Na tabela **Filters**, o filtro exibe o aviso.

Algumas configurações de política podem estar em um dos seguintes estados:

```
- Allowed or Prohibited allows or prevents the action controlled by
  the setting. Sometimes users are allowed or prevented from managing
  the setting's action in a session. For example, if the menu
  animation setting is set to Allowed, users can control menu
  animations in their client environment
- Enabled or Disabled turns the setting on or off. If you disable a
  setting, it is not enabled in lower-ranked policies.
```

Além disso, algumas configurações controlam a eficácia das configurações dependentes. Por exemplo, o redirecionamento da unidade cliente controla se os usuários têm permissão para acessar as unidades nos respectivos dispositivos. Essa configuração e a configuração **Client network drives**

devem ser adicionadas à política para permitir que os usuários acessem suas unidades de rede. Se a configuração de **Client drive redirection** estiver desativada, os usuários não poderão acessar suas unidades de rede, mesmo que a configuração de **Client network drives** esteja ativada.

Em geral, as alterações de configuração de política que afetam as máquinas entram em vigor quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon. Alterações de configuração de política que afetam os usuários entram em vigor na próxima vez que os usuários efetuarem logon.

Para algumas configurações de política, você pode inserir ou selecionar um valor ao adicionar a configuração a uma política. Você pode limitar a configuração do parâmetro selecionando Use default value. Essa seleção desativa a configuração do parâmetro e permite que somente o valor padrão da configuração seja usado quando a política é aplicada. Essa seleção é independente do valor que foi inserido antes de selecionar Use default value.

Como prática recomendada:

- Atribua políticas a grupos em vez de a usuários separadamente. Se você atribuir políticas a grupos, as atribuições serão atualizadas automaticamente quando você adicionar ou remover usuários do grupo.
- Desabilite políticas não utilizadas. Políticas sem configurações adicionadas criam processamento desnecessário.

Atribuições de política

Ao criar uma política, você a atribui a determinados usuários e objetos de máquina. Essa política é aplicada às conexões de acordo com critérios ou regras específicas. Em geral, você pode adicionar quantas atribuições quiser a uma política, com base em uma combinação de critérios. Se você não especificar nenhuma atribuição, a política será aplicada a todas as conexões.

Se você não especificar nenhuma atribuição, ou especificar atribuições, mas desativá-las, a política será aplicada a **todas** as conexões.

> **Nota:**
>
> As atribuições de política também são conhecidas como filtros de política. Para obter informações adicionais, consulte os seguintes tópicos:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

A tabela a seguir lista as atribuições disponíveis:

Nome da atribuição	Aplica uma política baseada em
Controle de acesso	Condições de controle de acesso através das quais um cliente está se conectando. *Connection type* - se deve aplicar a política a conexões feitas com ou sem NetScaler Gateway. *NetScaler Gateway farm name* - Nome do servidor virtual NetScaler Gateway. *Access condition* - Nome da política de análise de ponto de extremidade ou política de sessão que deve ser usada.
Citrix SD-WAN	Se uma sessão de usuário é iniciada por meio do Citrix SD-WAN. **Observação:** você pode adicionar somente uma atribuição do Citrix SD-WAN a uma política.
Endereço IP do cliente	Endereço IP do dispositivo do usuário usado para se conectar à sessão: exemplos IPv4:12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; exemplos 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.
Grupo de entrega	Associação do Grupo de Entrega.
Tipo de grupo de entrega	Tipo de área de trabalho ou aplicativo: área de trabalho privada, área de trabalho compartilhada, aplicativo privado ou aplicativo compartilhado.
Unidade Organizacional (UO)	Unidade organizacional.
Marca	Marcas. **Nota:** Aplique esta política a todos os computadores com marcas. As marcas de aplicativo não estão incluídas.
Usuário ou Grupo	Nome do usuário ou do grupo.

Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas em ordem de prioridade e várias instâncias de todas as configurações são comparadas. Cada configuração é aplicada de acordo com a ordem de prioridades da política. Qualquer configuração de política desabilitada tem precedência sobre uma configuração

de classificação inferior que esteja ativada. As configurações de política que não estão configuradas são ignoradas.

> **Importante:**
>
> Ao configurar as políticas do Active Directory e do Citrix usando o console de gerenciamento de política de grupo, as atribuições e as configurações podem não ser aplicadas conforme esperado. Para obter mais informações, consulte CTX127461.

É fornecida uma política chamada "Unfiltered"por padrão.

- Se você usar o Web Studio para gerenciar políticas Citrix, as configurações adicionadas à política Unfiltered serão aplicadas a todos os servidores, áreas de trabalho e conexões em um site.
- Os sites e as conexões devem estar dentro do escopo dos objetos de política de grupo (GPO) que inclui a política. Por exemplo, a unidade organizacional (UO) de vendas contém um GPO chamado Vendas-EUA que inclui todos os membros da equipe de vendas dos Estados Unidos. O GPO Vendas-EUA é configurado com uma política Unfiltered que inclui várias configurações de política de usuário. Quando o gerente de vendas dos Estados Unidos faz logon no Site, as configurações na política Unfiltered são aplicadas automaticamente à sessão. Essa configuração ocorre porque o usuário é membro do GPO Vendas-EUA.

O modo de uma atribuição determina se a política é aplicada apenas a conexões que correspondem a todos os critérios de atribuição. Se o modo estiver definido como Allow (o padrão), a política será aplicada apenas a conexões que correspondam aos critérios de atribuição. Se o modo estiver definido como Deny, a política será aplicada se a conexão não corresponder aos critérios de atribuição. Os exemplos a seguir ilustram como os modos de atribuição afetam as políticas Citrix quando várias atribuições estão presentes.

- **Exemplo: Atribuições de tipo semelhante com modos diferentes** - Em políticas com duas atribuições do mesmo tipo, uma configurada como Allow (Permitir) e uma como Deny (Negar), a atribuição definida como Deny tem precedência, desde que a conexão satisfaça ambas as atribuições. Por exemplo:

  A política 1 inclui as seguintes atribuições:

  - Atribuição A especifica o grupo Vendas. O modo é definido como Allow.
  - Atribuição B especifica a conta do gerente de vendas. O modo é definido como Deny.

  Como o modo de Atribuição B está definido como Deny, a política não é aplicada quando o gerente de vendas faz logon no site, mesmo que o usuário seja membro do grupo Vendas.

- **Exemplo: Atribuições de diferentes tipos com modos semelhantes** - Em políticas com duas ou mais atribuições de diferentes tipos, definidas como Allow, a conexão deve satisfazer pelo menos uma atribuição de cada tipo para que a política seja aplicada. Por exemplo:

  A política 2 inclui as seguintes atribuições:

- Atribuição C é uma atribuição de usuário que especifica o grupo Vendas. O modo é definido como Allow.
- A atribuição D é uma atribuição de endereço IP do cliente que especifica 10.8.169.* (a rede corporativa). O modo é definido como Allow.

Quando o gerente de vendas faz logon no Site a partir do escritório, a política é aplicada porque a conexão satisfaz ambas as atribuições.

A política 3 inclui as seguintes atribuições:

- Atribuição E é uma atribuição de usuário que especifica o grupo Vendas. O modo é definido como Allow.
- Atribuição F é uma atribuição de controle de acesso que especifica as condições de conexão NetScaler Gateway. O modo é definido como Allow.

Quando o gerente de vendas faz logon no Site a partir do escritório, a política não é aplicada porque a conexão não atende à Atribuição F.

Conjuntos de políticas (prévia)

November 21, 2023

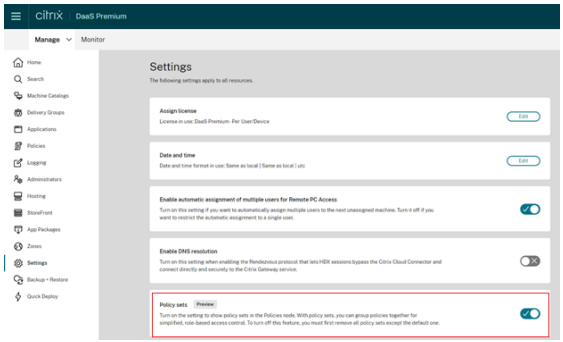
No Citrix DaaS , conjuntos de políticas são objetos que agregam políticas para permitir acesso simplificado e baseado em funções e de fácil gerenciamento. Você pode criar conjuntos de políticas para espelhar as divisões lógicas em sua equipe de administradores e empresa. Por exemplo, você pode criar um conjunto de políticas para cada região geográfica, unidade de negócios ou para um caso de uso específico. Depois de criados, escopos e grupos de entrega são atribuídos a conjuntos de políticas para que somente administradores autorizados possam gerenciar as políticas que se aplicam a seus usuários e máquinas relevantes.

Benefícios

- Controle de acesso baseado em funções para equipes de administradores distribuídas
- Fusões, aquisições e consolidações simplificadas
- Domínio de falha limitado
- Suporte multilocatário para políticas

Habilitar conjuntos de políticas

Na guia **Manage** do Citrix DaaS, vá para **Settings** e ative a configuração **Policy sets**.



> **Nota:**
>
> Você deve habilitar conjuntos de políticas antes de criar um conjunto de políticas.

Comparação de recursos

Antes de aplicar conjuntos de políticas	Depois de aplicar conjuntos de políticas
Políticas, configurações, filtros e prioridades de políticas para todo o site são configurados em um só lugar no Citrix Studio.	Políticas, configurações, filtros e prioridades de política são configurados separadamente para cada conjunto de políticas.
Se você gerencia uma política, deve gerenciar todas as políticas.	Administradores completos podem delegar para administradores de nível inferior a capacidade de gerenciar um determinado conjunto de políticas individualmente.
Políticas em ambientes grandes e distribuídos se tornam complexas e difíceis de gerenciar.	As políticas em ambientes grandes e distribuídos podem ser divididas e gerenciadas facilmente.

Como os conjuntos de políticas funcionam?

Visão geral

- Conjuntos de políticas são atribuídos a grupos de entrega
- Conjuntos de políticas têm um ou vários escopos
- Grupos de entrega sem nenhum conjunto de políticas atribuído recebem o conjunto de políticas padrão
- Um grupo de entrega só pode ter um conjunto de políticas atribuído a ele
- Vários grupos de entrega podem usar o mesmo conjunto de políticas
- Embora os conjuntos de políticas sejam atribuídos a grupos de entrega, as políticas mantêm seus filtros

Conjunto de políticas padrão

- Quando a configuração do conjunto de políticas está ativada, todas as políticas existentes são agrupadas dentro do conjunto de políticas padrão
- Cada grupo de entrega recebe o conjunto de políticas padrão, a menos que a equipe do administrador crie um conjunto de políticas e o atribua a um grupo de entrega.
- Assim que um grupo de entrega tenha um conjunto de políticas diferente atribuído a ele, ele não recebe mais políticas do conjunto de políticas padrão

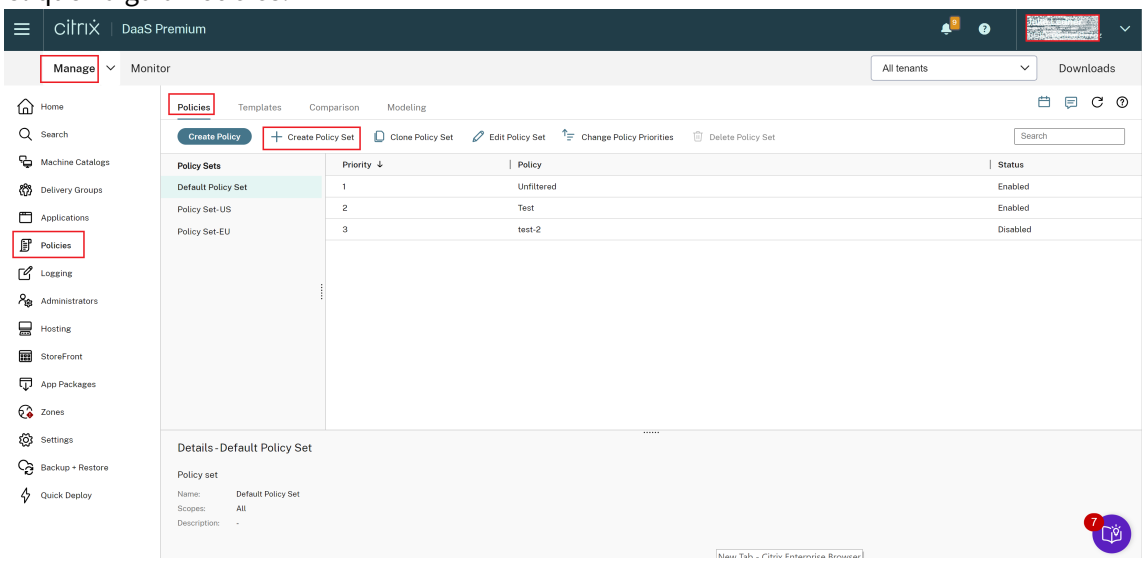
Criação de conjunto de políticas

Os conjuntos de políticas podem ser criados das duas maneiras a seguir:

- Create policy set –esta ação cria um conjunto de políticas vazio
- Clone policy set –esta ação cria um conjunto de políticas com base em um conjunto de políticas existente

Criar conjuntos de políticas

1. Na página de configuração do Citrix DaaS, clique na guia **Manage**.
2. Clique na guia **Policies**.



3. Selecione **Create Policy Set**. É exibida a guia **Introduction**.
4. Clique em **Next** ou clique na guia **Name and Description**.
5. Insira o nome e a descrição do conjunto de políticas.
6. Clique em **Next** ou clique na guia **Assignments**.
7. Selecione um ou mais grupos de entrega aos quais deseja atribuir o conjunto de políticas.
8. Clique em **Next** ou clique na guia **Scopes**.

9. Selecione os escopos do conjunto de políticas.
10. Clique em **Create**. O conjunto de políticas é criado com a atribuição e o escopo definidos.

Clonar conjuntos de políticas

1. Na página de configuração do Citrix DaaS, clique na guia **Manage**.
2. Clique na guia **Policies**.
3. Selecione **Clone Policy Set**.
4. Modifique o nome do conjunto de políticas.
5. Modifique ou crie atribuições para o conjunto de políticas e clique em **Next**.
6. Marque ou desmarque as políticas a serem incluídas no conjunto de políticas clonado.
7. Modifique o escopo da política.
8. Clique em **Create**. O conjunto de políticas é criado.

Editar conjuntos de políticas

1. Na página de configuração do Citrix DaaS, clique na guia **Manage**.
2. Clique na guia **Policies**.
3. Selecione **Edit Policy Set**.
4. Modifique o nome do conjunto de políticas e clique em **Next**.
5. Modifique ou crie atribuições para o conjunto de políticas e clique em **Next**.
6. Modifique o escopo da política.
7. Clique em **Create**.

Atribuição do conjunto de políticas

Os conjuntos de políticas são atribuídos aos grupos de entrega. Você pode configurar atribuições quando o conjunto de políticas é criado ou editado. Você também pode configurar atribuições quando os grupos de entrega são criados ou editados.

Escopos do conjunto de políticas

Os administradores podem definir o escopo do conjunto de políticas para que somente administradores autorizados possam exibi-lo ou editá-lo. Você pode configurar escopos quando o conjunto de políticas é criado ou editado.

Priorizar, modelar, comparar e solucionar problemas de políticas

June 6, 2023

Você pode usar políticas para personalizar seu ambiente para atender às necessidades dos usuários com base no seguinte:

- Funções de trabalho
- Localizações geográficas
- Tipos de conexão

Por exemplo, para maior segurança, crie restrições aos grupos de usuários que interagem regularmente com dados confidenciais.

Você também pode criar uma política que impede que os usuários salvem arquivos confidenciais em suas unidades de cliente locais. Você pode criar outra política para usuários do grupo de usuários que precisam acessar suas unidades locais. Você então classifica as duas políticas para controlar qual delas tem precedência. Ao usar várias políticas, você deve determinar:

- Como priorizar as políticas
- Como criar exceções
- Como visualizar a política eficaz quando as políticas entram em conflito

Priorizar políticas

Priorizar políticas permite que você defina a precedência das políticas quando elas contêm configurações conflitantes. A identificação de todas as políticas que correspondem às atribuições da conexão acontece quando um usuário faz login no sistema. As políticas identificadas e suas configurações associadas são classificadas em ordem de prioridade. Cada configuração é aplicada de acordo com a ordem de prioridades da política.

Você pode priorizar as políticas atribuindo a elas números de prioridade diferentes no **Web Studio**. Por padrão, uma nova política tem a prioridade mais baixa. Se houver conflitos entre as configurações de políticas, uma política com uma prioridade mais alta substituirá uma política com uma prioridade mais baixa. A política com o número de prioridade 1 é a política de maior prioridade. As configurações de política são mescladas de acordo com o seguinte:

- Prioridades das políticas
- Condições especificadas nos filtros das políticas

Para priorizar as políticas, siga estas etapas:

1. Selecione **Policies** no painel esquerdo.

2. Na guia **Policies**, selecione **Change Policy Priorities** na barra de ações. A página **Change Policy Priorities** é exibida.
3. Na lista de prioridades, use os seguintes meios para alterar a prioridade de uma política:
    - Arraste a política até a posição desejada.
    - Para movê-la para cima ou para baixo em uma posição, clique no ícone de seta para cima ou para baixo, respectivamente.
    - Para movê-la para a parte superior ou inferior da lista, clique no ícone de seta para cima ou para baixo, respectivamente.
    - Para alterar o número de prioridade, clique no ícone **Edit**, insira um número conforme necessário e clique em **Save**.
4. Clique em **Salvar**.

Exceções

Quando cria políticas e usa filtros para atribuí-las a grupos de usuários, dispositivos de usuários ou computadores, você pode notar que alguns membros do grupo exigem exceções a algumas configurações de política. Você pode criar exceções dos seguintes modos:

- Criando uma política apenas para os membros específicos do grupo que precisam das exceções e, em seguida, classificando a política mais alta do que a política para todo o grupo
- Usando o modo *Deny* para uma atribuição adicionada à política

Uma atribuição com o modo definido como *Deny* aplica uma política somente a conexões que não correspondem aos critérios de atribuição. Por exemplo, uma política inclui as seguintes atribuições:

- *Assignment A* é uma atribuição de endereço IP de cliente que especifica o intervalo `208.77.88.*`. O modo é definido como *Allow*.
- *Assignment B* é uma atribuição de usuário que especifica uma conta de usuário específica. O modo é definido como *Deny*.

A política se aplica a todos os usuários que fazem login no site com endereços IP no intervalo especificado em *Assignment A*. No entanto, a política não se aplica ao usuário que faz login no site com a conta de usuário especificada *Assignment B*.

> **Nota:**
>
> Durante a etapa **Assign Policy**, se você desmarcar a caixa de seleção enable, a atribuição será desativada para a política. Se a única atribuição da política estiver desativada, isso é o mesmo que não ter nenhuma atribuição, e, portanto, a política se aplica a todos os objetos no site.

Determine quais políticas se aplicam a uma conexão

Às vezes, uma conexão não responde como esperado porque várias políticas se aplicam. Se uma política de prioridade mais alta se aplicar a uma conexão, ela poderá substituir as configurações configuradas na política original. Você pode calcular o **Resultant Set of Policy** e determinar como as configurações finais de política são mescladas para uma conexão.

Você pode calcular o **Resultant Set of Policy** das seguintes maneiras:

- Use o **assistente Citrix Group Policy Modeling** para simular um cenário de conexão e discernir como as políticas Citrix podem ser aplicadas. Você pode especificar condições para um cenário de conexão, como:
  - Usuários
  - Valores de evidência de atribuição de políticas da Citrix
- Use o **Group Policy Results** para criar um relatório que descreve as políticas Citrix em vigor para um determinado usuário e Virtual Delivery Agent (VDA).

As configurações de política do site criadas usando o **Web Studio** não são incluídas no **Resultant Set of Policy** quando você executa o assistente **Citrix Group Policy Modeling** a partir do console **Group Policy Management**. Para confirmar que você obteve o conjunto **Resultant Set of Policy** mais abrangente, a Citrix recomenda iniciar o assistente **Citrix Group Policy Modeling** no **Web Studio**, a menos que você crie políticas usando apenas o console **Group Policy Management**.

Usar o assistente de modelagem de políticas

A modelagem de políticas ajuda você a simular políticas habilitadas com filtros para fins de planejamento e teste. Somente políticas habilitadas com filtros são modeladas. As políticas desabilitadas nunca são aplicadas e as políticas habilitadas sem filtros são sempre aplicadas.

Execute as etapas a seguir para abrir o assistente **Policy Modeling**:

1. Em Full Configuration, selecione **Policies**.
2. Selecione a guia **Modeling**.
3. Selecione **Policy Modeling** na barra de ações.
4. Leia a página de **introdução** e clique em **Next**.
5. Selecione usuários ou computadores. Você pode procurar contêineres ou usuários ou computadores específicos. Clique em **Next**.
6. Escolha sua evidência de filtro. Opcionalmente, você pode aprofundar mais a sua simulação inserindo detalhes adicionais, como **Delivery group**, **Tags**, **Client IP address** e outros. Clique em **Next**.
7. Revise o resumo de suas seleções e clique em **Run**.

Depois de clicar em **Run**, o assistente gera um relatório dos resultados da modelagem. Quando visualizar o relatório, você pode:

- Selecionar no menu suspenso o quer ver: **All settings**, **Computer settings** ou **User settings**.
- Usar a barra de pesquisa para procurar configurações específicas.
- Clicar em uma configuração específica para ver os detalhes dessa configuração. Por exemplo, se nem todas as configurações do usuário foram aplicadas a uma política específica, o painel **Details** mostra o motivo pelo qual as configurações não foram aplicadas.
- Clique em **Export** para exportar os resultados da modelagem no formato JSON, no formato HTML ou nos dois formatos.

Depois de executar a modelagem da política, mais opções ficam disponíveis para você. Você pode:

- **View Modeling Report**: abre o relatório de modelagem acima para que você possa exibi-lo novamente ou exportá-lo.
- **Rerun Policy Modeling**: permite que você execute novamente a modelagem da política com o mesmo conjunto de critérios selecionados anteriormente e gere novos resultados de modelagem. Isso é útil se algumas políticas tiverem sido alteradas e você quiser ver como as mudanças afetam o seu modelo atual.
- **Delete Modeling Report**: exclui o relatório de modelagem atual.

Comparar políticas e modelos

Você pode comparar as configurações em uma política ou modelo com as configurações de outras políticas ou modelos. Por exemplo, você pode querer verificar a definição de valores para manter a conformidade com as práticas recomendadas. Você também pode comparar as configurações em uma política ou modelo com as configurações padrão.

1. Selecione **Policies** no painel de navegação do **Web Studio**.
2. Clique na guia **Comparison** e clique em **Select**.
3. Escolha as políticas ou modelos que devem ser comparados. Para incluir valores padrão na comparação, marque a caixa de seleção **Compare to default settings**.
4. Depois de clicar em **Compare**, as configurações definidas são exibidas em colunas.
5. Para ver todas as configurações, selecione **Show All Settings**. Para retornar à exibição padrão, selecione **Show Common Settings**.

Solucionar problemas de políticas

Usuários, endereços IP e outros objetos atribuídos podem ter várias políticas que se aplicam simultaneamente. Esse cenário pode resultar em conflitos em que uma política pode não se comportar como esperado. Ao executar o assistente **Citrix Group Policy Modeling**, você pode descobrir que

nenhuma política é aplicada às conexões de usuário. Nesse cenário, as configurações da política não se aplicam aos usuários que se conectam a seus aplicativos e áreas de trabalho sob condições que correspondem aos critérios de avaliação da política. Essa situação acontece quando:

- Nenhuma política tem atribuições que correspondam aos critérios de avaliação da política.
- As políticas que correspondem à atribuição não têm nenhuma configuração definida.
- As políticas que correspondem à atribuição são desativadas.

Se você quiser aplicar as configurações de política às conexões que atendam aos critérios especificados, verifique se:

- As políticas que você deseja aplicar a essas conexões estão ativadas.
- As políticas que você deseja aplicar têm as configurações apropriadas definidas.

> **Nota:**
>
> No segundo salto em cenários de salto duplo, considere que um VDA com SO de sessão única se conecta ao VDA com SO multissessão. Nesse caso, as políticas da Citrix agem no VDA do SO de sessão única como se esse fosse o dispositivo do usuário. Por exemplo, considere que as políticas estão definidas para armazenar imagens em cache no dispositivo do usuário. Nesse exemplo, as imagens armazenadas em cache para o segundo salto em um cenário de salto duplo são armazenadas em cache na máquina VDA do SO de sessão única.

Director

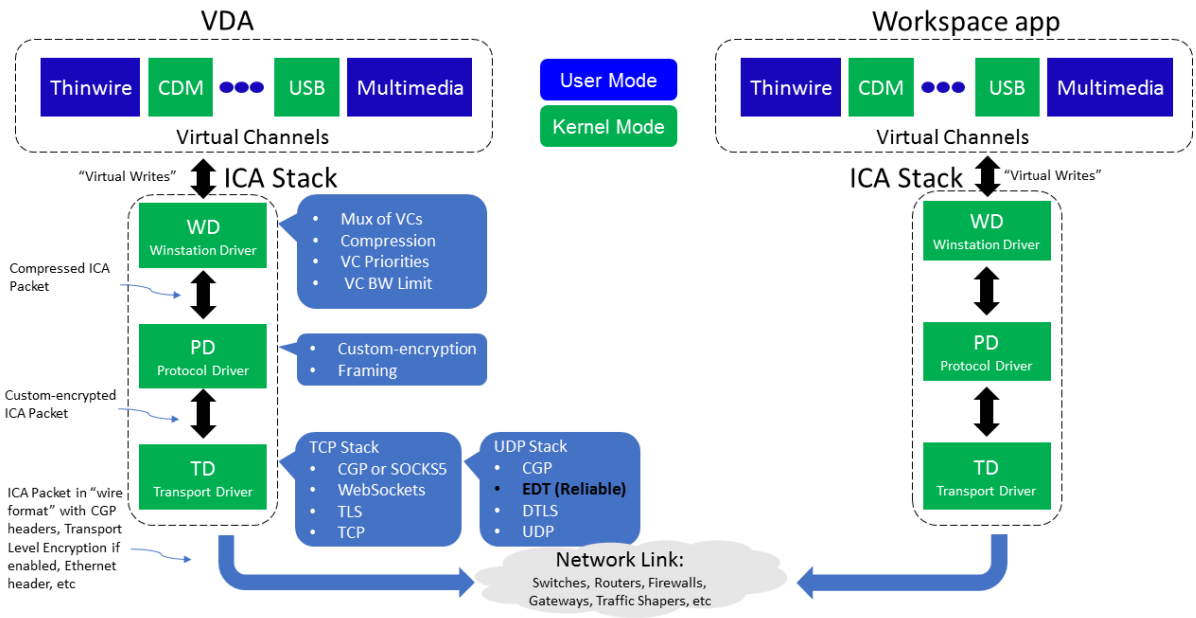
Os não administradores podem usar o Director para exibir as políticas que se aplicam a uma sessão de usuário.

Visão geral do HDX

May 30, 2023

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado 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 áreas de trabalho centralizados, em qualquer dispositivo e em qualquer rede.

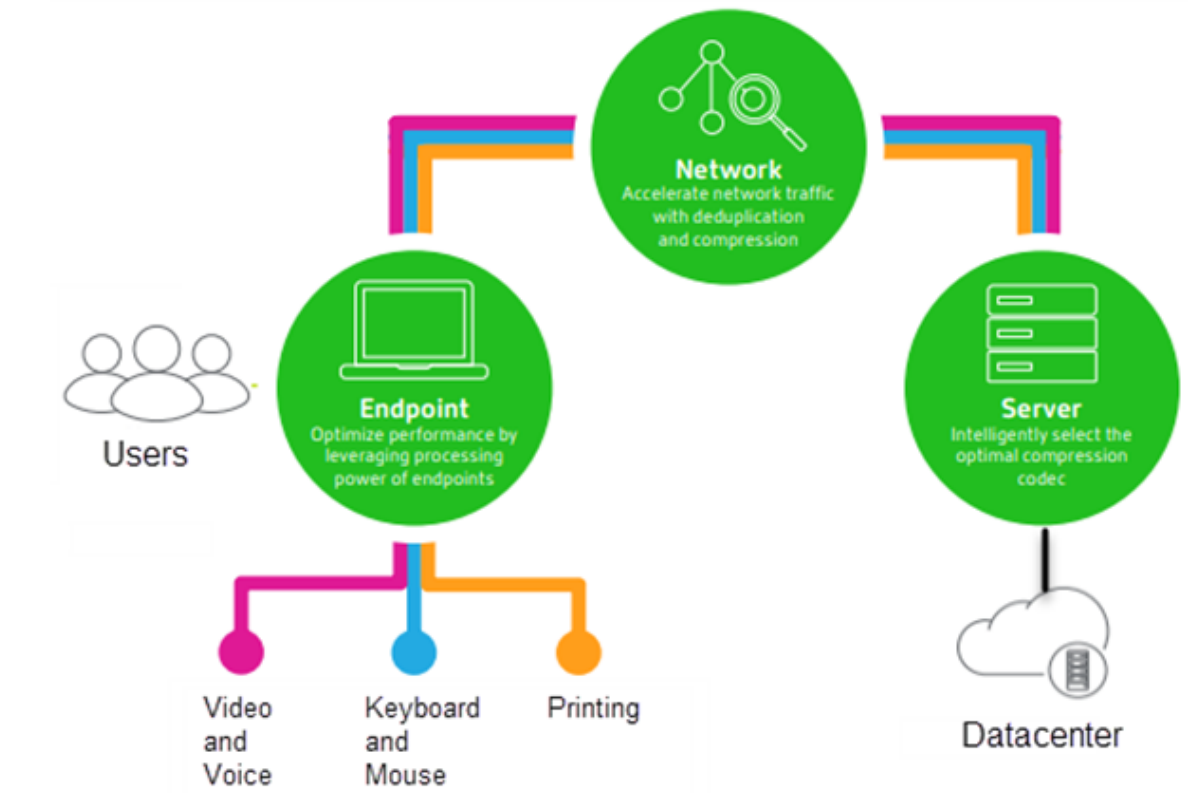


O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente
- Compactação adaptativa
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência do usuário e TI, diminuem o consumo de largura de banda e aumentam a densidade do usuário por servidor de hospedagem.

- **Redirecionamento inteligente** - o redirecionamento inteligente examina a atividade da tela, comandos de aplicativos, dispositivo de ponto de extremidade e recursos de rede e servidor para determinar instantaneamente como e onde renderizar uma atividade de aplicativo ou área de trabalho. A renderização pode ocorrer no dispositivo de ponto de extremidade ou no servidor de hospedagem.
- **Compactação adaptativa** - a compactação adaptativa permite que exibições multimídia avançadas sejam entregues em conexões de rede fina. O HDX primeiro avalia algumas variáveis, como o tipo de entrada, dispositivo e exibição (texto, vídeo, voz e multimídia). Ele escolhe o codec de compactação ideal e a melhor proporção de utilização entre CPU e GPU. Em seguida, ele se adapta de forma inteligente com base em cada usuário e base únicos. Essa adaptação inteligente é por usuário, ou mesmo por sessão.



- **Desduplicação de dados** - a eliminação de duplicação 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 de bitmap, documentos, trabalhos de impressão e conteúdo de streaming. O armazenamento em cache desses padrões permite que somente as alterações sejam transmitidas através da rede, eliminando o tráfego duplicado. O HDX também suporta multicast de stream de multimídia, onde uma única transmissão de uma fonte é vista por vários assinantes em um local, em vez de uma conexão individual para cada usuário.

Para obter mais informações, consulte Aumente a produtividade com um espaço de trabalho de usuário de alta definição.

No dispositivo

O HDX usa a capacidade de computação dos dispositivos do usuário para melhorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários tenham uma experiência sem atropelos com o conteúdo multimídia em suas áreas de trabalho ou aplicativos virtuais. O controle do espaço de trabalho permite que os usuários pausem as áreas de trabalho e aplicativos virtuais e retomem o trabalho a partir de um dispositivo diferente no ponto em que 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 HDX se adaptam às mudanças no ambiente. Os recursos equilibram o desempenho e a largura de banda. Eles aplicam as melhores tecnologias para cada cenário de usuário, independentemente se a área de trabalho ou aplicativo é ou não acessados 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 canais HDX fornecido pelo Citrix Director exibe o status dos canais HDX conectados em dispositivos do usuário.

HDX Insight

O HDX Insight é a integração do NetScaler Network Inspector e do Performance Manager com o Director. Ele captura dados sobre o tráfego ICA e fornece uma visualização do painel de detalhes históricos e em tempo real. Esses dados incluem latência de sessão ICA do lado do cliente e do servidor, uso de largura de banda dos canais ICA e o valor de tempo de ida e volta do ICA de cada sessão.

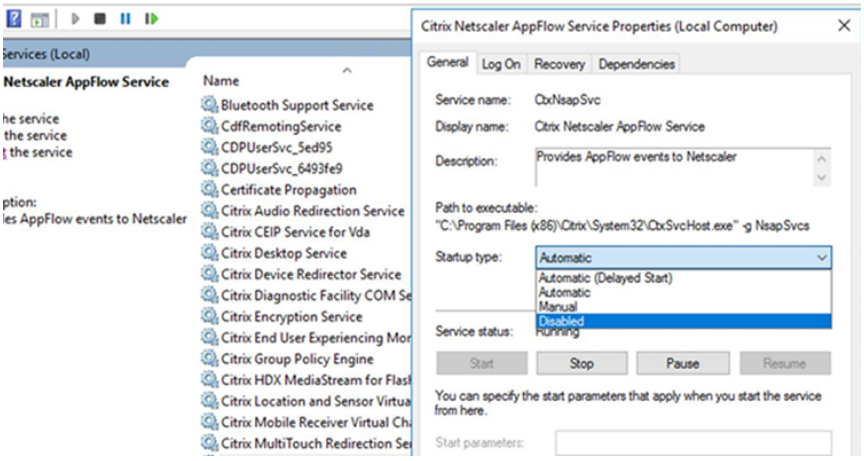
Você pode habilitar o NetScaler para usar o canal virtual HDX Insight para mover todos os pontos de dados necessários em um formato descompactado. Se você desabilitar esse recurso, o dispositivo NetScaler descriptografa e descompacta o tráfego ICA espalhado por vários canais virtuais. O uso de um único canal virtual reduz a complexidade, aumenta a escalabilidade e é mais econômico.

Requisitos mínimos:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp e XenDesktop 7.17
- NetScaler versão 12.0 compilação 57.x
- Aplicativo Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.10
- Aplicativo Citrix Workspace para Mac 1808
- Citrix Receiver para Mac 12.8

Ativar ou desativar o canal virtual HDX Insight

Para desativar esse recurso, defina as propriedades do serviço Citrix NetScaler Application Flow como Desativado. Para ativar, defina o serviço como Automático. Em ambos os casos, recomendamos que você reinicie a máquina do servidor depois de alterar essas propriedades. Por padrão, esse serviço está habilitado (Automático).



Experimente os recursos HDX da sua área de trabalho virtual

- Para ver como o redirecionamento de conteúdo do navegador, uma das quatro tecnologias de redirecionamento multimídia HDX, acelera a entrega de conteúdo multimídia HTML5 e WebRTC:
  1. Baixe a extensão do navegador Chrome e instale-a na área de trabalho virtual.
  2. Para experimentar como o redirecionamento de conteúdo do navegador acelera a entrega de conteúdo multimídia para áreas de trabalho virtuais, assista a um vídeo em sua área de trabalho a partir de um site que contenha vídeos HTML5, como o YouTube. Os usuários não sabem quando o redirecionamento de conteúdo do navegador está sendo executado. Para ver se o redirecionamento de conteúdo do navegador está sendo usado, arraste a janela do navegador rapidamente. Você verá um atraso ou deslocamento do quadro entre o visor e a interface do usuário. Você também pode clicar com o botão direito do mouse na página da Web e procurar **Sobre o redirecionamento do navegador HDX** no menu.
- Para ver como o HDX oferece áudio de alta definição:
  1. Configure seu cliente Citrix para obter a máxima qualidade de áudio; consulte a documentação do aplicativo Citrix Workspace para obter detalhes.
  2. Reproduza arquivos de música usando um player de áudio digital (como o iTunes) em sua área de trabalho.

O HDX fornece uma experiência superior com gráficos e vídeos para a maioria dos usuários por padrão,

e a configuração não é necessária. As configurações da política da Citrix que oferecem a melhor experiência para a maioria dos casos de uso são ativadas por padrão.

- O HDX seleciona automaticamente o melhor método de entrega com base no cliente, na plataforma, no aplicativo e na largura de banda da rede e, em seguida, faz o ajuste automático com base nas condições de mudança.
- O HDX otimiza o desempenho de gráficos e vídeos 2D e 3D.
- O HDX permite que os dispositivos do usuário transmitam arquivos multimídia diretamente do provedor de origem na internet ou na intranet, em vez de através do servidor host. Se os requisitos para essa busca de conteúdo no lado do cliente não forem atendidos, a entrega de mídia se volta à busca de conteúdo no lado do servidor e ao redirecionamento multimídia. Normalmente, ajustes nas políticas do recurso de redirecionamento multimídia não são necessários.
- O HDX oferece conteúdo de vídeo renderizado por servidor para áreas de trabalho virtuais quando o redirecionamento multimídia não está disponível: veja 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 sobre suporte e requisitos para recursos HDX, consulte o artigo Requisitos do sistema. Exceto quando indicado de outra forma, os recursos HDX estão disponíveis para máquinas com Windows com SO multissessão e SO de sessão única suportadas, além de áreas de trabalho de acesso ao PC remoto.
- 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 da Citrix e as configurações de políticas, consulte a documentação de políticas da Citrix para esta versão.
- Em instruções que incluem a edição do registro, tenha cuidado: editar o registro incorretamente pode causar sérios problemas que exigirão que você reinstale o 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Reconexão automática de cliente e confiabilidade da sessão

Ao acessar aplicativos ou áreas de trabalho hospedados, pode ocorrer interrupção de rede. Para experimentar uma reconexão mais descomplicada, oferecemos reconexão automática de cliente e confiabilidade da sessão Em uma configuração padrão, a confiabilidade da sessão é iniciada e, em seguida, ocorre a reconexão automática de cliente.

Reconexão automática de cliente:

A reconexão automática de cliente reinicia o mecanismo cliente para se reconectar a uma sessão desconectada. A reconexão automática de cliente fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Se a reconexão automática de cliente estiver em andamento, o sistema envia a notificação de interrupção de rede de aplicativos e áreas de trabalho para o usuário da seguinte forma:

- **Áreas de trabalho.** A janela da sessão fica acinzentada e um temporizador 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 temporizador de contagem regressiva mostrando o tempo até as tentativas de reconexão.

Durante a reconexão automática de cliente, as sessões reiniciam esperando que haja conectividade de rede. O usuário não pode interagir com sessões enquanto a reconexão automática de cliente estiver em andamento.

Na reconexão, as sessões desconectadas se reconectam usando informações de conexão salvas. O usuário pode interagir com os aplicativos e áreas de trabalho normalmente.

Configurações padrão de reconexão automática de cliente:

- Tempo limite de reconexão automática de cliente: 120 segundos
- Reconexão automática de cliente: Ativada
- Autenticação de reconexão automática de cliente: Desativada
- Log de reconexão automática de cliente: Desativado

Para obter mais informações, consulte Configurações da política de reconexão automática de cliente.

Confiabilidade da sessão:

A confiabilidade da sessão reconecta as sessões ICA sem problemas nas interrupções de rede. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Após o tempo limite da confiabilidade da sessão, as configurações de reconexão automática de 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 áreas de trabalho são enviadas ao usuário da seguinte forma:

- **Áreas de trabalho.** A janela de sessão torna-se translúcida e um temporizador de contagem regressiva mostra o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela torna-se translúcida e são lançados pop-ups de conexão interrompida na bandeja do sistema.

Quando a confiabilidade da sessão está ativa, o usuário não pode interagir com as sessões ICA. No entanto, as ações do usuário, como pressionamento de teclas, são armazenadas no buffer por alguns segundos imediatamente após a interrupção da rede e retransmitidas quando a rede fica disponível.

Na reconexão, o cliente e o servidor retomam no mesmo ponto em que estavam durante a troca de protocolos. As janelas da sessão perdem a translucidez e os pop-ups apropriados da área da bandeja 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: Ativada
- Número da porta de confiabilidade da sessão: 2598

Para obter mais informações, consulte Configurações da política de confiabilidade da sessão.

NetScaler com reconexão automática de cliente e confiabilidade da sessão:

Se as políticas Multistream e Multiporta estiverem habilitadas no servidor e uma ou todas estas condições forem verdadeiras, a reconexão automática de cliente não funciona:

- A confiabilidade da sessão está desativada 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 de forma inteligente a taxa de transferência máxima da sessão ICA ajustando os buffers de saída. O número de buffers de saída é inicialmente definido em um valor alto. Esse alto valor permite que os dados sejam transmitidos ao cliente de forma mais rápida e eficiente, especialmente em redes de alta latência. Fornecer melhor interatividade, transferência de arquivos mais rápida, reprodução de vídeo mais uniforme, maior taxa de quadros e de resolução resulta em uma experiência de usuário melhorada.

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 reduzida para diminuir o impacto do grande fluxo de dados na sessão e permitir que a interatividade se restabeleça.

> **Importante:**
>
> A taxa de transferência adaptativa HDX muda a forma como os buffers de saída são ajustados, movendo o mecanismo do cliente para o VDA, sem nenhuma configuração manual.

Esse recurso tem os seguintes requisitos:

- VDA versão 1811 ou posterior
- Aplicativo Workspace para Windows 1811 ou posterior

Melhorar a qualidade da imagem enviada aos dispositivos do usuário

As seguintes configurações de política de exibição visual controlam a qualidade das imagens enviadas de áreas de trabalho virtuais para dispositivos do usuário.

- Qualidade visual. Controla a qualidade visual das imagens exibidas no dispositivo do usuário: médio, alto, sempre sem perdas, compilação para sem perdas (padrão = médio). A qualidade real do vídeo usando a configuração padrão Médio depende da largura de banda disponível.
- Taxa de quadros alvo. Especifica o número máximo de quadros por segundo que são enviados da área de trabalho 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 mais profundidade de cor e resolução mais alta, aumente o limite. Você pode calcular a memória máxima necessária.

Melhorar o desempenho de videoconferências

Vários aplicativos populares de videoconferência são otimizados para a entrega com o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) por meio 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 a videoconferência em uma sessão. Esta tecnologia transmite o tráfego da webcam através de um canal virtual multimídia dedicado. Essa tecnologia usa menos largura de banda em comparação com o suporte de redirecionamento USB Plug-n-Play HDX isócrono e funciona bem em conexões WAN.

Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração Mic & Webcam do Desktop Viewer **Não usar meu microfone ou webcam**. Para evitar que os usuários mudem a compactação de vídeo da webcam HDX, desative o redirecionamento do dispositivo USB usando as configurações da política em Configurações de política em ICA policy settings > USB Devices policy.

A compactação de vídeo da webcam HDX requer que as seguintes configurações de política estejam habilitadas (todas estão habilitadas por padrão).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

Se uma webcam suportar codificação de hardware, a compactação 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 compactação 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 através de várias conexões para uma sessão usando roteadores suportados pela qualidade de serviço. Quatro streams TCP e dois streams UDP estão disponíveis para transportar o tráfego ICA entre o dispositivo do usuário e o servidor:

- Streams TCP - tempo real, interativo, em segundo plano e em massa
- Streams UDP - voz e telas remotas 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 multicanal são compatíveis com os VDAs (Virtual Delivery Agents) instalados em computadores Windows 10 e Windows 8. Fale com o seu administrador de rede para garantir que as portas do CGP (Common Gateway Protocol) definidas na configuração de política multiporta estejam atribuídas corretamente nos roteadores de rede.

A Qualidade de Serviço (QoS) é suportada somente quando várias portas de confiabilidade da sessão, ou as portas CGP, são configuradas.

> **Aviso:**
>
> Use a segurança de transporte quando usar esse recurso. A Citrix recomenda o uso de IPsec (Internet Protocol Security) ou TLS (Transport Layer Security). As conexões TLS só são suportadas quando as conexões atravessam um NetScaler Gateway compatível com ICA multistream Em uma rede corporativa interna, as conexões multistream com TLS não são suportadas.

Para definir a qualidade de serviço para várias conexões de streaming, adicione as seguintes configurações da política da Citrix a uma política (consulte Configurações de políticas de conexões multistream para obter detalhes):

- Política multiporta - esta configuração especifica as portas para o tráfego ICA através de várias conexões e estabelece prioridades de rede.
  - Selecione uma prioridade na lista de prioridades de 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 prioridades para cada uma. Cada porta deve ter uma prioridade exclusiva.

Configure explicitamente os firewalls nos VDAs para permitir o tráfego TCP adicional.

- Configuração do computador para multistream - esta configuração está desativada por padrão. Se você usar o Citrix NetScaler SD-WAN com suporte a multistream no seu ambiente, não será necessário definir essa configuração. Defina essa configuração da política quando usar roteadores de terceiros ou Branch Repeaters legados para alcançar a Qualidade de Serviço (QoS) desejada.
- Configuração do usuário multistream - esta configuração está desativada por padrão.

Para que as políticas que contêm essas configurações entrem em vigor, os usuários devem fazer logoff e, em seguida, fazer logon na rede.

Mostrar ou ocultar a barra de idiomas remota

A barra de idiomas exibe o idioma de entrada preferido em uma sessão de aplicativo. Se esse recurso estiver ativado (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. Ao usar uma configuração de registro no lado VDA, você pode desativar o controle cliente do recurso da barra de idiomas. Se esse recurso estiver desativado, a configuração da interface do usuário cliente não entrará em vigor 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 cliente do recurso de barra de idiomas a partir do VDA:

1. No editor de registro, navegue 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

Citrix Receivers não Windows usam o layout do teclado local (Unicode). Se um usuário alterar o layout do teclado local e o layout do teclado do servidor (código de varredura), eles podem ficar fora de sincronia e a saída ficará incorreta. Por exemplo, o usuário-1 altera a configuração do teclado local de inglês para alemão. O usuário-1 então altera o teclado do lado do servidor para alemão. Mesmo que ambos os layouts de teclado sejam alemães, eles podem não estar em sincronia, o que causa a saída de caracteres incorretos.

Ativar ou desativar o mapeamento de layout de teclado Unicode

Por padrão, o recurso é desabilitado no lado do VDA. Para ativar o recurso, alterne o recurso usando o editor de registro regedit no VDA. Adicione a seguinte chave de registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

Para desativar esse recurso, defina **EnableKlMap** como 0 ou exclua a chave **CtxKlMap**.

Ativar modo compatível com mapeamento de layout de teclado Unicode

Por padrão, o mapeamento de layout de teclado Unicode conecta automaticamente algumas APIs do Windows para recarregar o novo mapa de layout do teclado Unicode quando você altera o layout do teclado no lado do servidor. Alguns poucos aplicativos não podem ser vinculados. Para manter a compatibilidade, você pode alterar o recurso para o modo compatível para dar suporte a esses aplicativos sem gancho de vinculação. 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

June 24, 2022

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

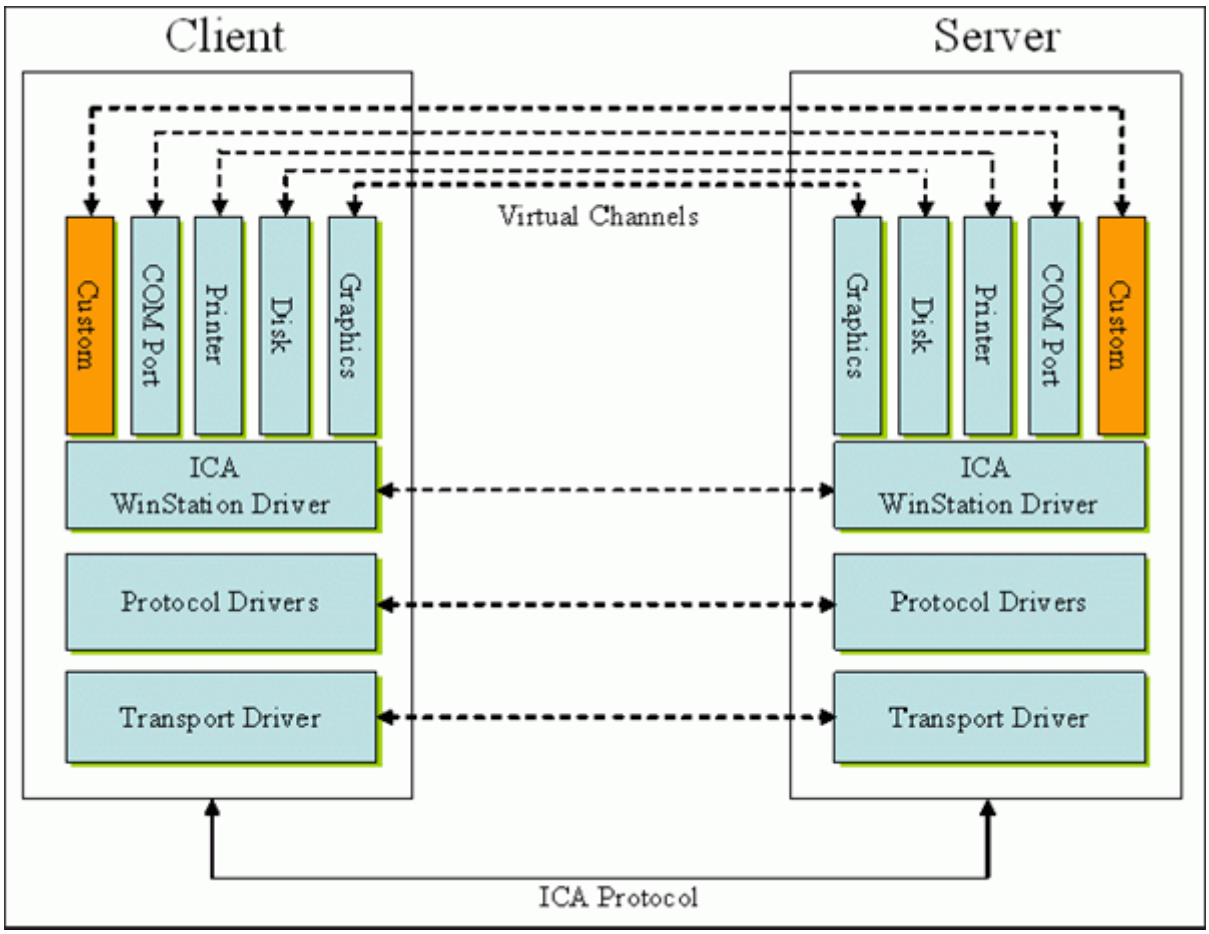
O que são os canais virtuais ICA?

Uma grande parte da funcionalidade e comunicação entre o aplicativo Citrix Workspace e os servidores do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) ocorre por canais virtu-

ais. 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

Às vezes, novos canais virtuais são lançados com os produtos Citrix DaaS e aplicativo Citrix Workspace para oferecer 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 está se comunicando com um dispositivo do lado do cliente ou com um aplicativo que está se comunicando com o ambiente do lado do cliente.

No lado do cliente, os canais virtuais correspondem aos drivers virtuais. Cada driver virtual fornece uma função específica. Alguns são necessários para operação normal, outros são opcionais. Os drivers virtuais operam no nível do protocolo da camada de apresentação. Pode haver vários protocolos ativos a qualquer momento mediante a multiplexação de canais fornecidos pela camada de protocolo do 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
- Área de transferência
- ClientComm
- ClientAudio
- LicenseHandler (Obrigatório)
- TWI (Obrigatório)
- SmartCard
- ICACTL (Obrigatório)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**
>
> Você pode desativar a funcionalidade específica do cliente removendo um ou mais desses valores da chave de registro. Por exemplo, se você quiser remover a Área de transferência cliente, remova a palavra **Clipboard**.

Esta lista contém os arquivos do driver virtual 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 Links Dinâmicos (modo de usuário), não 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 de área de trabalho
- vdcamN.dll —Áudio bidirecional
- vdcdm30n.dll —Mapeamento da unidade cliente
- vdcom30N.dll –Mapeamento de porta COM cliente
- vdcpm30N.dll —Mapeamento da 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 de chave transparente
- vdlfpn.dll —Canal de exibição Framehawk por UDP como transporte
- vdmmn.dll —Suporte multimídia
- vdmrvc.dll —Canal virtual do Mobile Receiver
- vdmtchn.dll –Suporte multitoque
- vdscardn.dll —Suporte a cartão inteligente
- vdsens.dll —Canal virtual de sensores
- vdspl30n.dll —UPD cliente
- vdsspin.dll —Kerberos
- vdtuin.dll —Interface do usuário transparente
- vdtw30n.dll —Cliente Thinwire
- vdtwin.dll —Contínuo
- 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 com 64 bits

O aplicativo Citrix Workspace para Windows é compatível com 64 bits. Tal como acontece com a maioria dos binários compilados para 32 bits, estes arquivos 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 no modo kernel juntamente com o driver de canal virtual vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

Como funcionam os canais virtuais ICA

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 canais virtuais 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 da unidade cliente
- Picaser.sys —Redirecionamento de porta COM
- Picapar.sys —Redirecionamento de porta LPT

Canal virtual gráfico no lado do servidor

Começando com o 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 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.

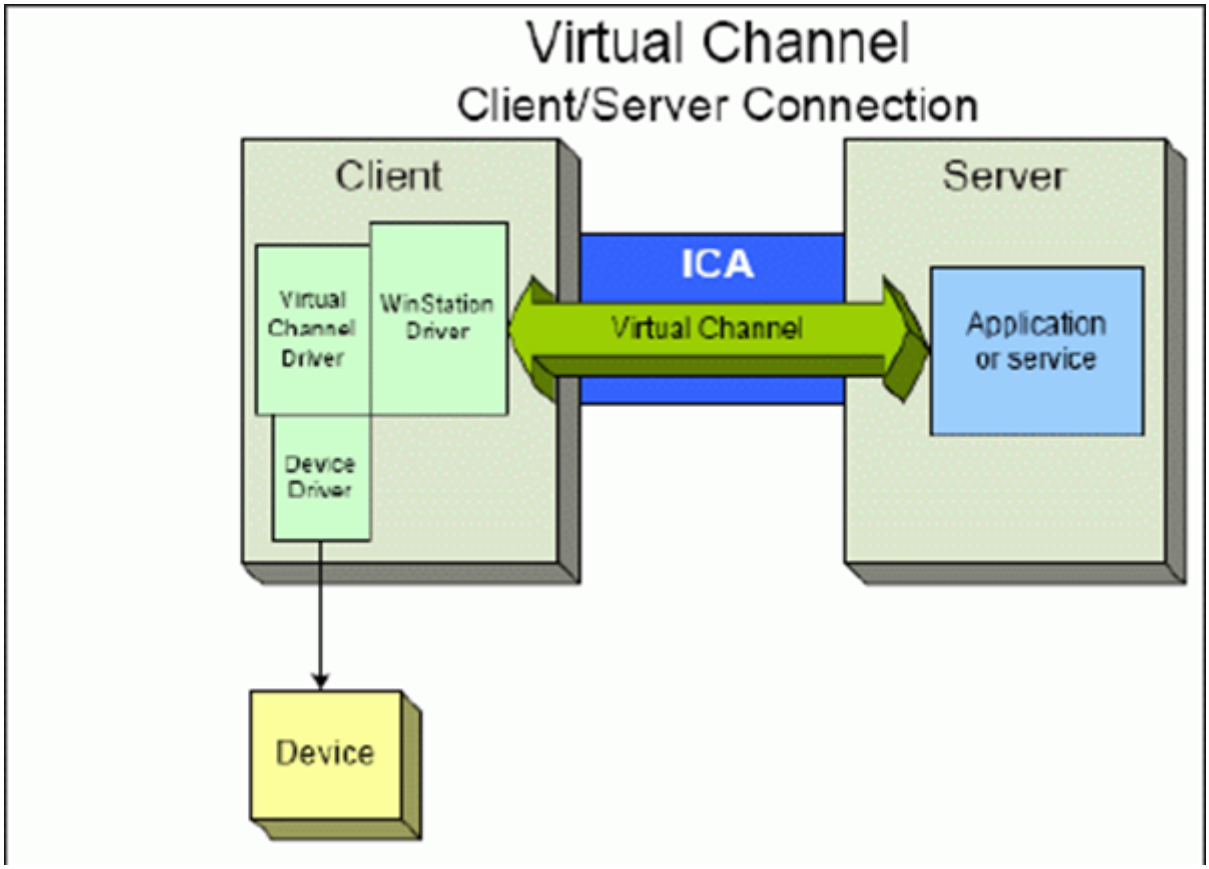
Hospedagem de canais especializados em serviços Windows

Nos servidores Citrix DaaS, vários canais são hospedados como serviços do Windows. Essa hospedagem fornece semântica um-para-muitos para múltiplos aplicativos em uma sessão e múltiplas sessões no servidor. Exemplos de tais serviços incluem:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops somente)

O canal virtual de áudio no Citrix Virtual Apps é hospedado usando o serviço Windows Audio.

No lado do servidor, todos os canais virtuais cliente são roteados através do driver WinStation, Wdica.sys. No lado do cliente, o driver WinStation correspondente, integrado no wfica32.exe, sonda os canais virtuais cliente. Esta imagem ilustra a conexão cliente-servidor do canal virtual.



Esta ilustração mostra a 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 aos quais dá suporte para o servidor.
2. O aplicativo do lado do servidor é iniciado, obtém um identificador para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.
3. O driver virtual 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 para o cliente imediatamente. Quando o cliente recebe os dados, o driver do WinStation desmultiplexa os dados do canal virtual a partir do stream do ICA e os passa imediatamente para o driver virtual cliente.
   - Se o driver virtual cliente tiver dados para enviar para o servidor, os dados serão enviados na próxima vez que o driver do WinStation fizer a sondagem. Quando o servidor recebe os dados, eles são enfileirados até que o aplicativo de canal virtual os leia. Não há como alertar o aplicativo de canal virtual do servidor que os dados foram recebidos.
4. Quando o aplicativo do canal virtual do servidor é concluído, ele fecha o canal virtual e libera todos os recursos alocados.

Criando o seu próprio canal virtual usando o Virtual Channel SDK

Criar um canal virtual usando o Virtual Channel SDK 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 que o WFAPI SDK para gravar no lado do servidor do canal virtual.
> - Devido à segurança aprimorada do Citrix DaaS, você deve especificar quais canais virtuais podem ser abertos em uma sessão do ICA. Para obter mais informações, consulte Configurações de política de lista de permissões de canal virtual.

Criando o seu próprio canal virtual usando o ICA Client Object SDK

Criar um canal virtual usando o ICA Client Object (ICO) é mais fácil do que usando o Virtual Channel SDK. Use o ICO criando um objeto nomeado no 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), é necessária uma etapa extra ao criar um canal virtual ICO.

Para obter mais informações, consulte Client Object API Specification Programmer's Guide.

Funcionalidade de passagem de canais virtuais

A maioria dos canais virtuais que a Citrix fornece operam sem modificação quando você usa o aplicativo Citrix Workspace para Windows em uma sessão ICA (também conhecida como uma sessão de passagem). Há considerações ao usar o cliente em saltos extras.

As seguintes funções operam da mesma forma em saltos simples ou múltiplos:

- Mapeamento de porta COM cliente
- Mapeamento da unidade cliente
- Mapeamento da impressora cliente
- UPD cliente
- Monitoramento da experiência do usuário
- USB genérico

- Kerberos
- Suporte multimídia
- Suporte a cartão inteligente
- Passagem de chave transparente
- Twain

Com a natureza inerente de latência e fatores como compressão e descompressão e renderização sendo executada em cada salto, o desempenho pode ser afetado com cada salto adicional sobre o cliente. As áreas afetadas são:

- Áudio bidirecional
- Transferências de arquivos
- Redirecionamento USB genérico
- Continuidade
- Thinwire

> **Importante:**
>
> Por padrão, as unidades cliente mapeadas por uma instância do cliente em execução em uma sessão de passagem são restritas às unidades cliente do cliente de conexão.

Funcionalidade de passagem de canais virtuais entre uma sessão do Citrix Virtual Desktops e uma sessão do Citrix Virtual Apps

A maioria dos canais virtuais fornecidos pela Citrix opera sem modificação quando você usa o aplicativo Citrix Workspace para Windows em uma sessão ICA em um servidor Citrix Virtual Desktops (também conhecida como uma sessão de passagem).

Especificamente, no servidor Citrix Virtual Desktops, há um gancho VDA que executa **picaPassthruHook**. Esse gancho 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 cliente
- Mapeamento da unidade cliente
- Mapeamento da impressora cliente
- USB genérico (limitado pelo desempenho)
- Suporte multimídia
- Suporte a cartão inteligente
- SSON
- Passagem de chave transparente

A segurança e os canais virtuais ICA

A proteção da utilização é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança no decorrer deste documento.

Práticas recomendadas

Abra os canais virtuais quando se **Conectar** e **Reconectar**. Feche os canais virtuais quando fizer logoff e se **Desconectar**.

Tenha em mente as seguintes diretrizes ao criar scripts que usam funções de canal virtual.

Nomenclatura de canais virtuais:

Você pode criar um máximo de 32 canais virtuais. Dezessete dos 32 canais são reservados para fins especiais.

- O nome dos canais virtuais não deve ter mais de sete caracteres de comprimento.
- 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 referidos por um nome em ASCII de sete caracteres (ou mais curto). Em algumas versões anteriores do protocolo ICA, os canais virtuais eram numerados. Os números agora são atribuídos dinamicamente com base no nome em ASCII, facilitando a implementação. Os usuários que estão desenvolvendo códigos 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 maiúsculas e minúsculas em ASCII. 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 apenas para uso pela Citrix.

Suporte para salto duplo:

Canal virtual	O salto duplo é suportado?
Áudio	Não
Redirecionamento de conteúdo do navegador	Não
CDM	Sim
CEIP	Não
Área de transferência	Sim
Continuum (MRVC)	Não

Canal virtual	O salto duplo é suportado?
Control VC	Sim
Redirecionamento de vídeo HTML5 (v1)	Sim
Teclado, Mouse	Sim
MultiTouch	Não
NSAPVC	Não
Impressão	Sim
SensVC	Não
Smartcard	Sim
Twain	Sim
USB VC	Sim
Dispositivos WAYCOM -K2M usando USB VC	Sim
Compressão de vídeo de webcam	Sim
Windows Media Redirection	Sim

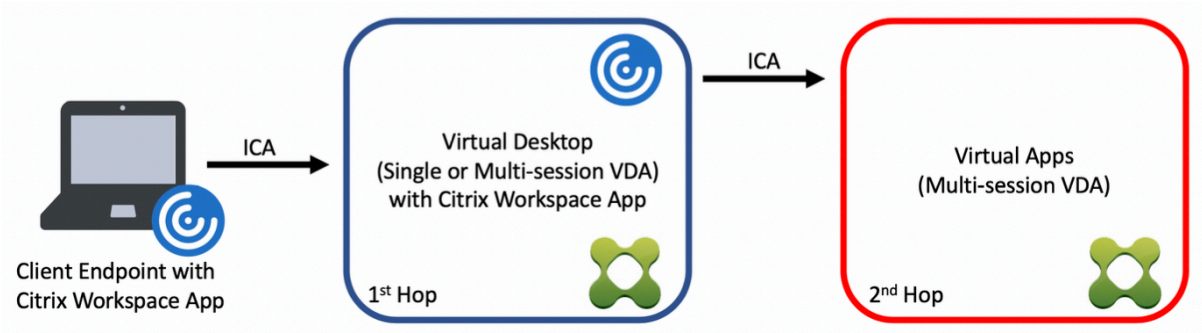
Veja também

- ICA Virtual Channel SDK
- Citrix Developer Network reúne todos os recursos técnicos e discussões envolvendo o uso de SDKs da Citrix. Nessa rede de recursos, você tem acesso a SDKs, exemplos de códigos e scripts, extensões e plug-ins, e documentação do SDK. Inclui também os fóruns do Citrix Developer Network, onde as discussões técnicas acontecem em torno de cada um dos SDKs da Citrix.

Salto duplo no Citrix DaaS

July 1, 2022

No contexto de uma sessão de cliente Citrix, o termo “salto duplo”refere-se a uma sessão do Citrix Virtual Apps que está sendo executada em uma sessão do Citrix Virtual Desktops. O diagrama a seguir ilustra um salto duplo.



Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktops em execução em um SO VDA de sessão única (conhecido como VDI) ou em um SO VDA multissessão (conhecido como área de trabalho publicada), esse é considerado o primeiro salto. Depois que o usuário se conecta à área de trabalho virtual, o usuário pode iniciar uma sessão do Citrix Virtual Apps. Esse é considerado o segundo salto.

Você pode usar um modelo de implantação de salto duplo para oferecer suporte a vários casos de uso. O caso em que os ambientes Citrix Virtual Desktops e Citrix Virtual Apps são gerenciados por diferentes entidades 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 Citrix Virtual Apps and Desktops Service) suportam salto duplo.

O primeiro salto deve usar uma versão compatível do SO VDA de sessão única ou multissessão e do aplicativo Citrix Workspace. O segundo salto deve usar uma versão suportada do SO VDA multissessão. Consulte a página Product Matrix para ver as versões compatíveis.

Para melhor desempenho e compatibilidade, a Citrix recomenda o uso de um cliente Citrix da mesma versão ou mais recente que as versões VDA em uso.

Em ambientes em que o primeiro salto envolve uma solução de área de trabalho 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 problemas relacionados à área de trabalho virtual de terceiros, incluindo compatibilidade de aplicativos Citrix Workspace, redirecionamento de dispositivos de hardware e desempenho da sessão, a Citrix pode fornecer suporte técnico com capacidade limitada. Talvez seja necessário o Citrix Virtual Desktops no primeiro salto como parte da solução de problemas.

Considerações de implantação para HDX no salto duplo

Em geral, cada sessão em um salto duplo é única e as funções cliente-servidor são isoladas para um determinado salto. Essa seção inclui áreas que exigem consideração especial por parte dos administradores da Citrix. A Citrix recomenda que os clientes realizem testes completos dos recursos HDX necessários para garantir que o desempenho e a experiência do usuário sejam adequados para uma determinada configuração de ambiente.

Gráficos

Use as configurações de gráficos padrão (codificação seletiva) no primeiro e segundo saltos. No caso de HDX 3D Pro, a Citrix recomenda altamente 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 afetar a experiência geral do usuário. Considere a latência adicionada entre o primeiro e o segundo saltos. Isso é especialmente importante com o redirecionamento de dispositivos de hardware.

Multimídia

A renderização do conteúdo de áudio e vídeo no lado do servidor (em sessão) tem melhor desempenho no primeiro salto. A reprodução de vídeo no segundo salto requer decodificação e recodificação no primeiro salto, resultando no aumento da utilização de recursos de hardware e largura de banda. 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 especial atenção ao modo em uso em cada salto e use a tabela a seguir como referência para melhores resultados. Para obter mais informações sobre modos de redirecionamento genéricos e otimizados, consulte Dispositivos USB genéricos.

Primeiro salto (VDI ou área de trabalho publicada)	Segundo salto (Virtual Apps)	Notas de suporte de compatibilidade
Otimizado	Otimizado	Recomendado (com base na compatibilidade dos dispositivos). 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, recomenda-se usar o modo otimizado em ambos os saltos quando o suporte de compatibilidade ao dispositivo estiver disponível.
Otimizado	Genérico	Sem suporte

> **Nota:**
>
> Devido à alta atividade inerente dos protocolos USB, o desempenho pode diminuir entre os saltos. A funcionalidade e os resultados variam dependendo dos requisitos específicos do dispositivo e do aplicativo. O teste de validação é altamente recomendado em todos os casos de redirecionamento do dispositivo e especialmente importante em cenários de salto duplo.

Exceções de suporte

As sessões de salto duplo suportam a maioria das funcionalidades e recursos do HDX, exceto:

- Redirecionamento de conteúdo do navegador
- Acesso a aplicativo local
- RealTime Optimization Pack para Skype for Business
- Otimização para Microsoft Teams

Transporte HDX

May 2, 2023

O Citrix HDX representa um amplo conjunto de tecnologias que oferecem uma experiência de alta definição aos usuários de aplicativos e áreas de trabalho centralizados, em qualquer dispositivo e em qualquer rede.

O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente
- Compactação adaptativa
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência do usuário e TI, diminuem o consumo de largura de banda e aumentam a densidade do usuário por servidor de hospedagem.

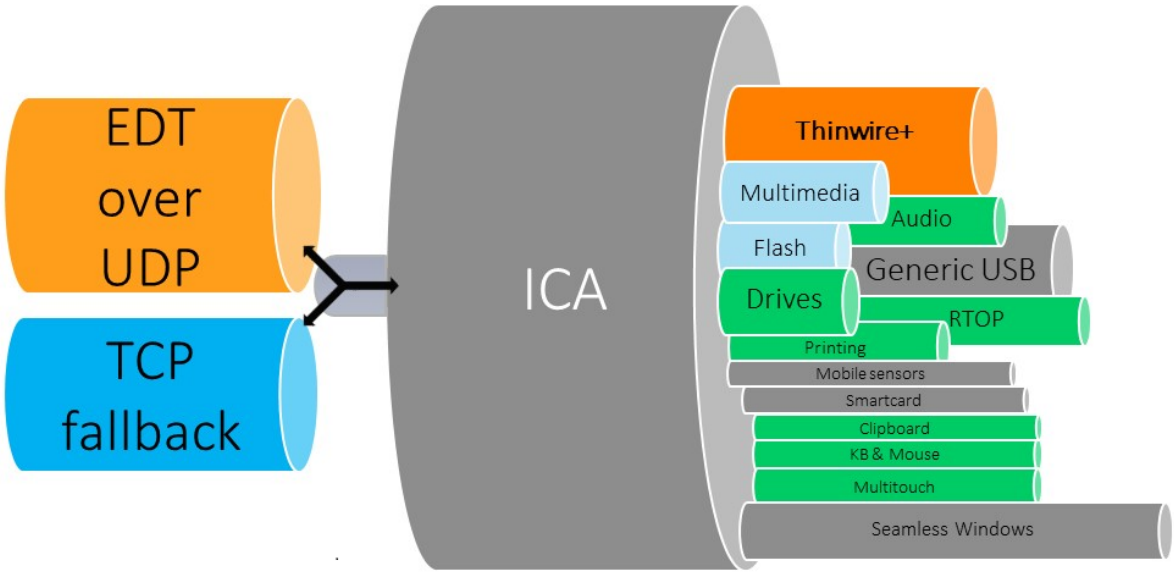
Dentro da oferta HDX, você pode se conectar por meio de um protocolo de transporte proprietário exclusivo e conectar-se com um protocolo de rendevous enquanto usa o Citrix Gateway Service.

Transporte adaptativo

August 30, 2023

O transporte adaptativo é um mecanismo no Citrix Virtual Apps and Desktops que fornece a capacidade de usar o Enlightened Data Transport (EDT) ou EDT Lossy como protocolo de transporte para conexões ICA. O transporte adaptativo muda para o TCP quando o EDT não está disponível.

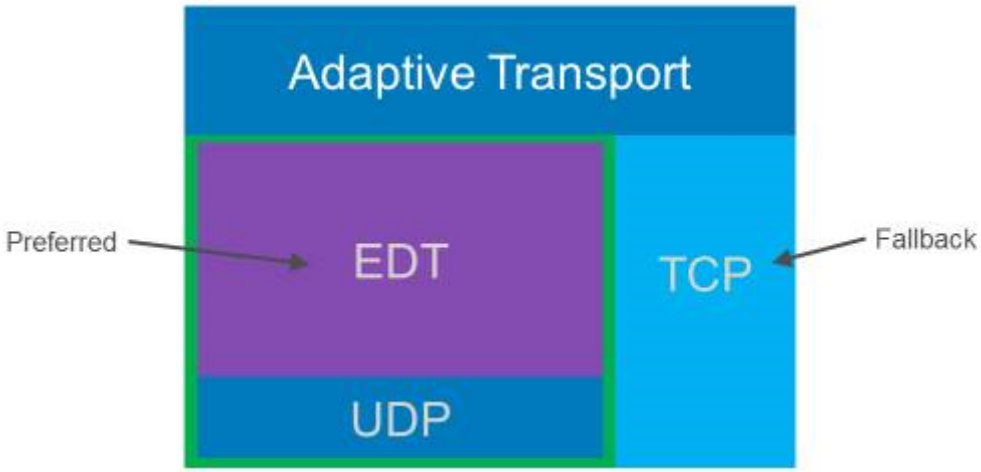
EDT é um protocolo de transporte proprietário da Citrix desenvolvido sobre o protocolo UDP (User Datagram Protocol). Ele oferece uma experiência de usuário superior em conexões mais difíceis de longo alcance, mantendo a escalabilidade do servidor. O EDT melhora a taxa de transferência de dados para todos os canais virtuais ICA em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.



Quando o transporte adaptativo é definido como **Preferred**, o EDT é usado como o protocolo de transporte primário e o TCP é usado para fallback. Por padrão, o transporte adaptativo é definido como **Preferred**. Você pode definir o transporte adaptativo para o **modo de diagnóstico** para fins de teste, o que permite apenas o EDT e desabilita o fallback para TCP.

Com o aplicativo Citrix Workspace para Windows, Mac e iOS, as conexões EDT e TCP são realizadas em paralelo durante a conexão inicial, a reconexão de confiabilidade da sessão e a reconexão automática de cliente. Isso reduz o tempo de conexão se o transporte UDP subjacente não estiver disponível e o TCP precisar ser usado em seu lugar. Se o transporte adaptativo estiver definido como **Preferred** e a conexão for estabelecida usando TCP, o transporte adaptativo continuará tentando alternar para EDT a cada cinco minutos.

Com o aplicativo Citrix Workspace para Linux e Android, as tentativas de conexões EDT são realizadas primeiro. Se a conexão não for bem-sucedida, o aplicativo Citrix Workspace tentará se conectar usando TCP depois que a solicitação EDT expirar.



Requisitos do sistema

A seguir estão os requisitos para usar o transporte adaptativo e EDT:

- Plano de controle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 1912 ou posterior
- Virtual Delivery Agent
  - Versão 1912 ou posterior (recomendado 2203 ou posterior)
  - A versão 2012 é o mínimo necessário para usar o EDT com o Citrix Gateway Service
- StoreFront (*aplica-se somente quando usado na implantação*)
  - Versão 3.12.x
  - Versão 1912.0.x
- Aplicativo Citrix Workspace
  - Windows: versão 2105 ou posterior
  - Linux: versão 2109 ou posterior
  - Mac: versão 2108 ou posterior
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível na Google Play
- Citrix Gateway (ADC)
  - 13.1.17.42 ou posterior (recomendado)
  - 13.0.52.24 ou posterior
  - 12.1.56.22 ou posterior

- Firewall (da perspectiva do VDA)
  - Entrada UDP 1494 —se a confiabilidade da sessão estiver desativada
  - Entrada UDP 2598 —se a confiabilidade da sessão estiver ativada
  - Entrada UDP 443 —se o VDA SSL estiver ativado para criptografia ICA (DTLS)
  - Saída UDP 443 —se estiver usando o Citrix Gateway Service. Para obter mais informações, consulte a documentação do Citrix Gateway Service.

Considerações

- Permita a confiabilidade da sessão para usar EDT MTU Discovery e usar o EDT com o Citrix Gateway e o Citrix Gateway Service.
- Certifique-se de que o EDT MTU esteja configurado adequadamente para evitar fragmentação. Caso contrário, o desempenho pode ser afetado ou as sessões podem não ser iniciadas em algumas situações. Para obter mais informações, consulte a seção Descoberta de MTU em EDT.
- Para obter detalhes sobre requisitos e considerações para usar o EDT com o Citrix Gateway Service, consulte HDX Adaptive Transport with EDT support for Citrix Gateway service.
- Para obter detalhes sobre a configuração do Citrix Gateway para oferecer suporte ao EDT, consulte Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight.
- Atualmente, o IPv6 não é suportado.

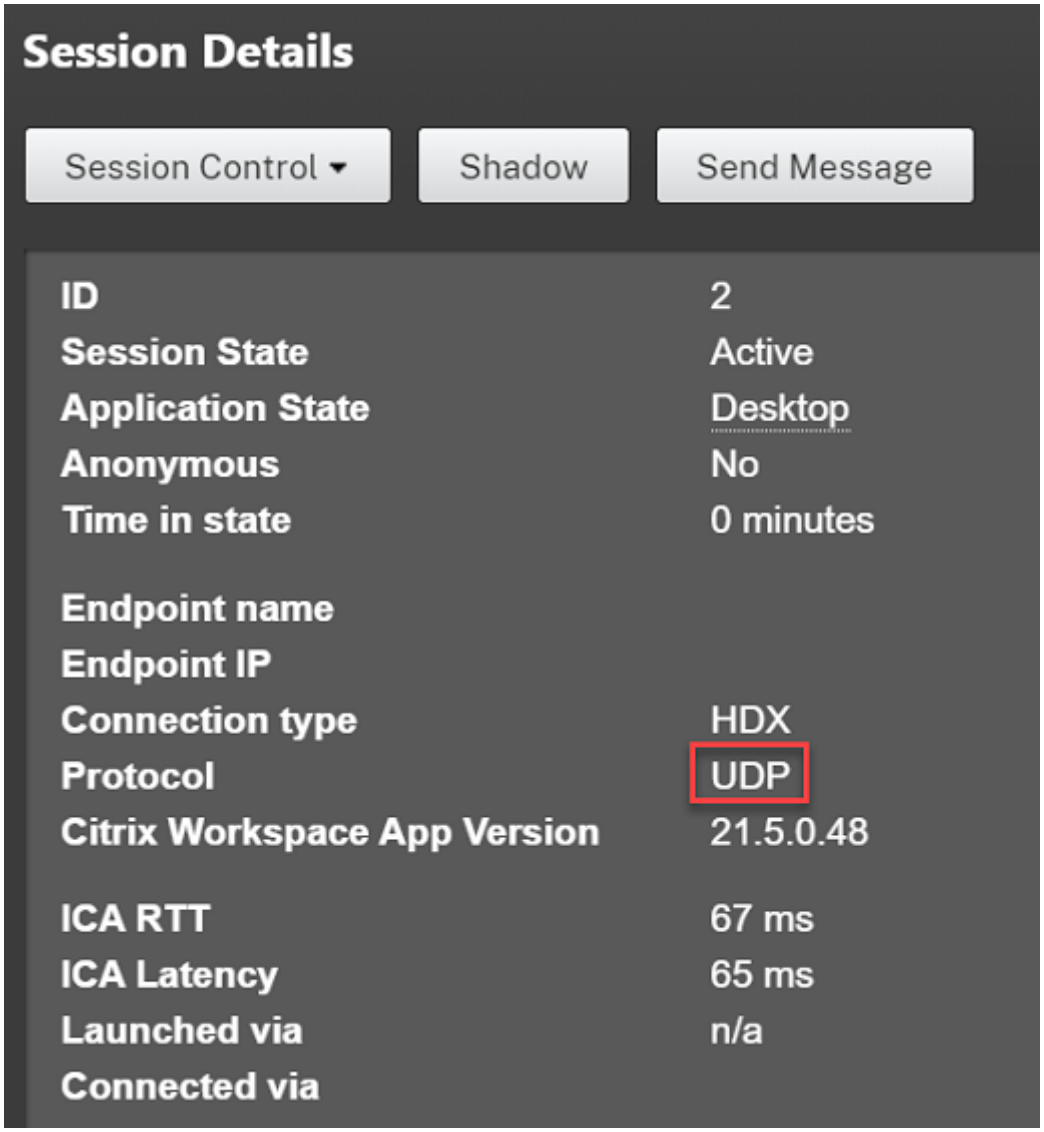
Configuração

O transporte adaptativo está habilitado por padrão. Você pode configurar as seguintes opções usando a configuração de **transporte adaptativo HDX** na política da Citrix.

- **Preferred**. Essa é a configuração padrão. O transporte adaptativo está ativado e usa o EDT como o protocolo de transporte preferido, com fallback para TCP.
- **Diagnostic mode**. O transporte adaptativo está ativado e força o uso do EDT. O fallback para TCP está desativado. Essa configuração é recomendada somente para testes e solução de problemas.
- **Off**. O transporte adaptativo está desativado e somente o TCP é usado para o transporte.

Para confirmar se 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 **Details**. Se **Connection type** for **HDX** e **Protocol** for **UDP**, EDT está sendo usado como o protocolo de transporte para a sessão. Se **Connection type** for **RDP**, ICA não está em uso e **Protocol** exibe N/A. Para obter mais informações, consulte Monitorar sessões.



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 EDT estiver em uso, o protocolo de transporte mostra um dos seguintes:

- **UDP > ICA** (confiabilidade da sessão desativada)
- **UDP > CGP > ICA** (confiabilidade da sessão ativada)
- **UDP > DTLS > CGP > ICA** (ICA é criptografada por DTLS de ponta a ponta)


```
Administrator: Windows PowerShell
PS C:\windows\system32> ctxsession -v

Session Id  2:
Transport Protocols:    UDP -> DTLS -> CGP -> ICA
      Local Address:
     Remote Address:
     Client Address:
  Security Protocol:    UNKNOWN VALUE - 131072
    Security Cipher:    128 bit AES
    Cipher Strength:    128 bits
     ICA Encryption:    Basic

EDT Reliable Statistics:
    Bandwidth 121.777 Mbps,  Send Rate 0 bps,  Recv Rate 0 bps,  RTT 65.531 ms
    Sent            0,  Sent Lost        0 (0.00%),  Rcvd            0,  Rcvd Lost        0 (0.00%)
    Sent ACKs       0,  Sent NAKs        0,          Rcvd ACKs       0,  Rcvd NAKs        0
    Flow Window  16383,  Congest Window   4050,   Delivery Rate   7591
    EDT MTU: 1400

ICA Statistics:
     SentBandwidth (bps) =       6376    RecvBandwidth (bps) =        568
     SentPreCompression  =    1800688    RecvPreExpansion    =      32864
     SentPostCompression =    1429125    RecvPostExpansion   =     137041
     Compression Ratio % =         79    Expansion Ratio %   =         23
     LastLatency         =         67    AverageLatency      =         53
     IcaBufferLength     =        980
```

Descoberta de MTU em EDT

A descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso impede a fragmentação do pacote EDT que possa resultar em degradação de desempenho ou falha para estabelecer uma sessão.

> **Importante:**
>
> - A confiabilidade da sessão deve estar ativada para que a Descoberta de MTU funcione.
> - A Descoberta de MTU com Multi-Stream ICA está disponível com o VDA versão 2209 e posterior.

Para controlar a descoberta de MTU em EDT no VDA

A descoberta de MTU é ativada por padrão. Para desativar esse recurso, exclua o valor do registro e **EDT MTU Discovery** e reinicie o VDA. Para obter mais informações, consulte a configuração de EDT MTU Discovery na lista de recursos HDX gerenciados através do registro.

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Loss tolerant mode

O modo de tolerância a perdas usa o protocolo de transporte EDT com perdas para melhorar a experiência dos usuários que se conectam através de redes com alta latência e perda de pacotes.

Inicialmente, as sessões são estabelecidas usando o EDT. Se os limites de latência e perda de pacotes forem alcançados ou ultrapassados, os canais virtuais aplicáveis passam do EDT para o EDT com perdas, deixando os outros canais virtuais no EDT. Se a latência e a perda de pacotes caírem abaixo dos limites, os canais virtuais aplicáveis voltam para o EDT.

Os limites padrão são:

- Perda de pacotes: 5%
- Latência: 300 ms (RTT)

O modo de tolerância a perdas é ativado por padrão. Você pode desativar o recurso ou ajustar os limites de perda de pacotes e latência usando as configurações Loss tolerant mode e Loss tolerant thresholds.

> **Importante:**
>
> - A confiabilidade da sessão deve estar ativada para que o modo tolerante a perdas funcione.
> - O modo tolerante a perdas está disponível somente com o aplicativo Citrix Workspace para Windows.
> - O modo de tolerância a perdas não é suportado no Citrix Gateway ou no Citrix Gateway Service. Esse modo está disponível apenas com conexões diretas.

Problemas conhecidos

Transporte adaptativo e EDT contêm os seguintes problemas:

- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha ao iniciar as sessões. Você pode ajustar o EDT MTU para evitar isso. Use a descoberta de MTU ou a solução alternativa descrita em CTX231821.
- Uma tela cinza ou preta pode aparecer ao iniciar uma sessão a partir de um cliente Windows se a descoberta de MTU estiver ativada. Para resolver esse problema, atualize para o aplicativo Workspace para Windows 2105, ou posterior, ou para o aplicativo Workspace para Windows 1912 CU4, ou posterior.
- O fallback para TCP pode falhar em clientes Linux e Android ao se conectar por meio do Citrix Gateway ou Citrix Gateway Service. Isso acontece quando há uma negociação EDT bem-sucedida entre o cliente e o Gateway, e a negociação EDT falha entre o Gateway e o VDA. Para resolver esse problema, atualize para o aplicativo Workspace para Linux 2104, ou posterior, e para o aplicativo Workspace para Android 21.5, ou posterior.

- Caminhos de rede assimétricos podem fazer com que a descoberta de MTU falhe nas conexões que não passam pelo Citrix Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para o VDA versão 2103 ou posterior. [CVADHELP-16654]
- Ao usar o Citrix Gateway ou o Citrix Gateway Service, caminhos de rede assimétricos podem fazer com que a descoberta de MTU falhe. Isso se deve a um problema no Gateway que faz com que o bit DF (Don't Fragment) no cabeçalho dos pacotes EDT não seja propagado. Ainda não há uma correção disponível para esse problema. [CGOP-18438]
- A descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não conseguem respeitar o bit DF quando o processamento de pacotes está ativado, impedindo que a descoberta de MTU detecte a fragmentação. Nessa situação, estas são as opções disponíveis:
  - Desativar o processamento de pacotes no modem do usuário.
  - Desativar a descoberta de MTU e usar uma MTU codificada conforme descrito em CTX231821.
  - Desativar o transporte adaptativo para forçar as sessões a usarem o 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.

Solução de problemas

Para solucionar problemas de transporte adaptativo e EDT, sugerimos o seguinte:

1. Analise e valide minuciosamente os requisitos, considerações e problemas conhecidos.
2. Verifique se há políticas Citrix no Studio ou no objeto de política de grupo substituindo a configuração de **HDX Adaptive Transport** desejada.
3. Verifique se há configurações no cliente substituindo a configuração de HDX Adaptive Transport desejada. Pode ser uma preferência de GPO, uma configuração definida usando o modelo administrativo do aplicativo Workspace opcional ou uma configuração manual do parâmetro **HDXoverUDP** no registro ou no arquivo de configuração do cliente.
4. Em máquinas VDA multissessão, certifique-se de que os ouvintes UDP estão ativos. Abra um prompt de comando na máquina VDA e execute `netstat -a -p udp`. Para obter mais informações, consulte Como confirmar o protocolo HDX Enlightened Data Transport.
5. Inicie uma sessão direta internamente, ignorando o Citrix Gateway, e verifique o protocolo em uso. Se a sessão usar o EDT, o VDA estará pronto para usar o EDT para conexões externas por meio do Citrix Gateway.
6. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo Citrix Gateway:

- Certifique-se de que a confiabilidade da sessão está ativada
- Certifique-se de que o Gateway tenha o DTLS ativado

7. Verifique se as regras de firewall apropriadas foram configuradas nos firewalls de rede e nos firewalls em execução nas máquinas VDA.
8. Verifique se as conexões de usuários exigem uma MTU não padrão. Conexões com uma MTU efetiva inferior a 1500 bytes causam fragmentação de pacotes EDT, que, por sua vez, pode afetar o desempenho ou, até mesmo, causar falhas no início da sessão. Esse problema é comum ao usar VPN, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Para obter informações sobre como resolver esse problema, consulte a seção Descoberta de MTU em EDT.

Interoperabilidade com Citrix SD-WAN

A otimização WAN do Citrix SD-WAN (WANOP) oferece compactação indexada com token entre sessões (desduplicação de dados), incluindo cache de vídeo baseado em URL, e fornece redução significativa da largura de banda. A redução ocorre se duas ou mais pessoas em um escritório assistir ao mesmo vídeo recuperado pelo cliente, ou transferir ou imprimir partes significativas do mesmo arquivo ou documento. Além disso, ao executar os processos de redução de dados ICA e compactação de trabalho de impressão no dispositivo da filial, a WANOP oferece descarregamento de CPU do servidor VDA e permite maior escalabilidade do servidor Citrix Virtual Apps and Desktops.

Atualmente, o SD-WAN WANOP não suporta EDT. No entanto, não há necessidade de desativar o transporte adaptativo se o SD-WAN WANOP estiver em uso. Quando um usuário inicia uma sessão que passa por uma SD-WAN com WANOP ativado, isso define a sessão automaticamente para usar TCP como protocolo de transporte. Sessões não WANOP continuam a usar o EDT sempre que possível.

Protocolo Rendezvous

June 6, 2023

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud Connectors para se conectarem diretamente e com segurança ao plano de controle do Citrix Cloud.

Há dois tipos de tráfego a serem considerados:

1. Tráfego de controle, para registro do VDA e intermediação de sessão.
2. Tráfego de sessão HDX.

Há duas versões do Rendezvous disponíveis:

- Versão 1 (V1): permite ignorar os Citrix Cloud Connectors apenas para o tráfego de sessão HDX.

- Versão 2 (V2): permite ignorar os Citrix Cloud Connectors para o tráfego de controle e o tráfego de sessão HDX.

Para obter detalhes sobre os requisitos do sistema, considerações e configuração para cada uma das versões do Rendezvous, consulte sua respectiva documentação.

Documentação do Rendezvous V1

Documentação do Rendezvous V2

Rendezvous V1

May 2, 2023

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud Connectors para se conectarem diretamente e com segurança ao plano de controle do Citrix Cloud.

Requisitos

- Acesso ao ambiente usando o serviço Citrix Workspace e Citrix Gateway.
- Plano de controle: Citrix DaaS (Citrix Cloud).
- VDA: versão 1912 ou posterior.
  - A versão 2012 é o mínimo exigido para o EDT Rendezvous.
  - A versão 2012 é o mínimo necessário para o suporte a proxy não transparente (sem suporte a arquivos PAC).
  - A versão 2103 é o mínimo necessário para a configuração de proxy com um arquivo PAC.
- Ative o protocolo Rendezvous na política Citrix. Para obter mais informações, consulte Configuração de política do protocolo Rendezvous.
- Os VDAs devem ter acesso a `https://*.nssvc.net`, incluindo todos os subdomínios. Se você não puder adicionar todos os subdomínios à lista de permissões dessa maneira, use `https://*.c.nssvc.net` e `https://*.g.nssvc.net`. Para obter mais informações, consulte a seção de Requisitos de conectividade à Internet da documentação do Citrix Cloud (em Citrix DaaS) e o artigo do Knowledge Center CTX270584.
- Os VDAs devem ser capazes de se conectar aos endereços mencionados anteriormente no TCP 443 e UDP 443 para TCP Rendezvous e EDT Rendezvous, respectivamente.
- Os Cloud Connectors precisam obter os FQDNs dos VDAS ao intermediar uma sessão. Realize essa tarefa de uma dessas duas maneiras:

- **Ative a resolução de DNS para o site.** Navegue para **Full Configuration > Settings** e ative a configuração **Enable DNS resolution**. Como alternativa, use o Citrix Virtual Apps and Desktops Remote PowerShell SDK e execute o comando `Set-BrokerSite -DnsResolutionEnabled $true`. Para obter mais informações sobre o SDK do PowerShell remoto do Citrix Virtual Apps and Desktops, consulte SDKs e APIs.
- **Zona de pesquisa inversa de DNS com registros PTR para os VDAs.** Se você escolher essa opção, recomendamos que configure os VDAs para sempre tentem registrar registros PTR. Para isso, use o Editor de política de grupo ou o Objeto de política de grupo, navegue até **Configuração do Computador > Modelos Administrativos > Rede > Cliente DNS** e defina **Registrar Registros PTR** como **Ativado e Registrar**. Se o sufixo DNS da conexão não corresponder ao sufixo DNS do domínio, você também deverá definir a configuração de **Sufixo DNS específico da conexão** para que as máquinas registrem registros PTR com êxito.

> **Nota:**
>
> Se estiver usando a opção de resolução de DNS, os Cloud Connectors deverão 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 deverão corresponder aos FQDNs das máquinas VDA. Se o registro PTR contiver um FQDN diferente, a conexão do 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 funciona.

Configuração de proxy

O VDA suporta o estabelecimento de conexões do 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 a 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 é interrompida.
- Os proxies HTTP suportam autenticação baseada em máquina usando os protocolos de autenticação Negociação e Kerberos ou NT LAN Manager (NTLM).

Quando você se conecta ao servidor proxy, o esquema de autenticação Negociar seleciona automaticamente o protocolo Kerberos. Se o Kerberos não for compatível, a Negociação voltará ao NTLM para autenticação.

> **Nota:**
>
> Para usar o Kerberos, você deve criar o nome da entidade 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 o URL do proxy é recuperado da configuração da política de **proxy do Rendezvous**. Se você não criar um SPN, a autenticação voltará para o NTLM. Em ambos os casos, a identidade da máquina VDA é usada para autenticação.

- A autenticação com um proxy SOCKS5 não é suportada no momento. Se estiver usando um proxy SOCKS5, você deverá configurar uma exceção para que o tráfego destinado aos endereços do Gateway Service (especificados nos requisitos) possa ignorar a autenticação.
- Apenas os proxies SOCKS5 dão suporte ao transporte de dados através do EDT. Para um proxy HTTP, use TCP como o protocolo de transporte para ICA.

Proxy transparente

Se estiver usando um proxy transparente em sua rede, nenhuma configuração adicional será necessária no VDA.

Proxy não transparente

Se estiver usando um proxy não transparente em sua rede, defina a configuração em Rendezvous proxy configuration. Quando a configuração estiver habilitada, especifique o endereço de proxy HTTP ou SOCKS5 ou insira o caminho para o arquivo PAC para que o VDA saiba qual proxy usar. Por exemplo:

- Endereço 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 Windows HTTP: `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 na sessão HDX.
2. Execute `ctxsession.exe -v`.
3. Os protocolos de transporte em uso indicam o tipo de conexão:
    - TCP Rendezvous: **TCP > SSL > CGP > ICA**
    - EDT Rendezvous: **UDP > DTLS > CGP > ICA**
    - Proxy através do Cloud Connector: **TCP > CGP > ICA**

Outras considerações

Ordem do pacote de codificação Windows

Para a ordem de pacote de codificação personalizada, certifique-se de incluir os pacotes de codificação compatíveis com VDA da lista a seguir:

- 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 pacote de codificação personalizada não contiver esses pacotes de codificação, a conexão do Rendezvous falhará.

Zscaler Private Access

Se estiver usando o Zscaler Private Access (ZPA), é recomendável que você defina as configurações de bypass para o Gateway Service para evitar o aumento da latência e o impacto no desempenho associado. Para isso, você deve definir segmentos do aplicativo para os endereços do Gateway Service — especificados nos requisitos —e defini-los para sempre fazer o bypass. Para obter informações sobre como configurar segmentos do aplicativo para ignorar o ZPA, consulte a documentação do Zscaler.

Rendezvous V2

November 21, 2023

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud Connectors para se conectarem diretamente e com segurança ao plano de controle do Citrix Cloud.

O Rendezvous V2 é compatível com máquinas ingressadas no domínio padrão, máquinas ingressadas no Azure AD e máquinas não ingressadas no domínio.

> **Nota:**
>
> Atualmente, implantações sem conector são possíveis somente com máquinas *ingressadas no Azure AD* e *não ingressadas no domínio*. As máquinas ingressadas no domínio AD padrão ainda exigem Cloud Connectors para o registro de VDA e a 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 VDA, como conexão ao seu domínio do AD local, provisionamento de MCS para hipervisores locais etc., permanecem os mesmos.

Requisitos

Os requisitos para usar o Rendezvous V2 são:

- Acesso ao ambiente usando Citrix Workspace e Citrix Gateway Service
- Plano de controle: Citrix DaaS
- VDA versão 2203
- Ative o protocolo Rendezvous na política Citrix. Para obter mais informações, consulte Configuração de política do protocolo Rendezvous.
- A confiabilidade da sessão deve estar ativada 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, você pode usar `https://<customer_ID>.xendesktop.net`, onde <customer_ID> é 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 Gateway Service.
  - `https://*.*.nssvc.net` em `TCP` 443 e `UDP` 443 para sessões HDX por TCP e EDT, respectivamente.

> **Nota:**
>
> Se você não pode permitir o uso de todos os subdomínios `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 do Knowledge Center CTX270584.

Configuração de proxy

O VDA oferece suporte à conexão por meio de proxies para o tráfego de controle e o tráfego de sessão HDX ao usar o Rendezvous. Os requisitos e considerações para os dois tipos de tráfego são diferentes, portanto, analise-os cuidadosamente.

Considerações sobre o proxy de tráfego de controle

- Somente proxies HTTP são aceitos.
- A descriptografia e a 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 falhará.
- A autenticação de proxy não é suportada.

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 de configuração do proxy do Rendezvous.
- A descriptografia e a 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 for ingressada no domínio AD. Ela pode usar a autenticação Negotiate/Kerberos ou NTLM.

  > **Nota:**
  >
  > Para usar o Kerberos, crie o nome da entidade 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 o URL do proxy é recuperado da configuração da política de configuração do proxy do Rendezvous. Se você não criar um SPN, a autenticação voltará para o NTLM. Em ambos os casos, a identidade da máquina VDA é usada para autenticação.

- A autenticação com um proxy SOCKS5 não é suportada no momento. 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 os proxies SOCKS5 dão suporte ao transporte de dados através do EDT. Para um proxy HTTP, use TCP como o protocolo de transporte para ICA.

Proxy transparente

Se estiver usando um proxy transparente em sua rede, nenhuma configuração adicional será 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 a configuração.

No assistente de instalação do VDA, selecione **Rendezvous Proxy Configuration** na página **Additional Components**. Essa opção disponibiliza a página **Rendezvous Proxy Configuration** posteriormente no assistente de instalação. Quando estiver nela, insira o endereço do proxy ou o caminho ao arquivo PAC para que o VDA saiba qual proxy usar. Por exemplo:

- Endereço proxy: `http://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Conforme mencionado nas considerações de 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 de configuração do proxy do Rendezvous. Quando a configuração estiver habilitada, especifique o endereço de 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 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 Windows HTTP: `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 no seu ambiente:

1. Certifique-se de que todos os requisitos sejam atendidos.
2. Se você precisar usar um proxy HTTP não transparente no seu ambiente, configure-o durante a instalação do VDA. Consulte a seção de configuração de proxy para obter detalhes.
3. Depois que o VDA for instalado, 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
4. Reinicialize a máquina VDA.
5. Crie uma política da Citrix ou edite uma existente:
   - Defina a configuração de **Rendezvous Protocol** como **Allowed**.
   - Se você precisar configurar um proxy HTTP ou SOCKS5 para o tráfego HDX, configure o parâmetro **Rendezvous proxy configuration**.
   - Certifique-se de que os filtros da política da Citrix estejam configurados corretamente. A política se aplica às máquinas que precisam do Rendezvous habilitado.
6. Certifique-se de que a política da Citrix tem a prioridade correta para que ela não substitua outra política.

Validação do Rendezvous

Se você atender a todos os requisitos e tiver concluído a configuração, siga estas etapas para validar se o Rendezvous está em uso:

1. Na área de trabalho virtual, abra um prompt de comando ou o PowerShell.
2. Execute `ctxsession.exe -v`.
3. Os protocolos de transporte exibidos indicam o tipo de conexão:
   - TCP Rendezvous: TCP > SSL > CGP > ICA
   - EDT Rendezvous: UDP > DTLS > CGP > ICA
   - Não Rendezvous: TCP > CGP > ICA
4. A versão do Rendezvous exibida indica a versão em uso.

Outras considerações

Ordem do pacote de codificação Windows

Se a ordem do pacote de codificação tiver sido modificada nas máquinas VDA, certifique-se de incluir os pacotes de codificação compatíveis com 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 do pacote de codificação personalizada não contiver esses pacotes de codificação, a conexão do Rendezvous falhará.

Zscaler Private Access

Se estiver usando o Zscaler Private Access (ZPA), é recomendável que você defina as configurações de bypass para o Gateway Service para evitar o aumento da latência e o impacto no desempenho associado. Para isso, você deve definir segmentos do aplicativo para os endereços do Gateway Service — especificados nos requisitos —e defini-los para sempre fazer o bypass. Para obter informações sobre como configurar segmentos do aplicativo para ignorar o ZPA, consulte a documentação do Zscaler.

Problemas conhecidos

O Rendezvous V2 não funciona se o Rendezvous V1 estava em uso anteriormente

Se você habilitou a configuração de resolução de DNS em seu site DaaS para usar o Rendezvous V1, as conexões do Rendezvous V2 falharão. Para usar o Rendezvous V2, você deve desativar a resolução de DNS em seu site DaaS usando uma das seguintes opções:

- Vá para **Full Configuration > Settings** e ative a configuração **Enable DNS resolution**.
- Use o Citrix DaaS Remote PowerShell SDK e execute o comando `Set-BrokerSite -DnsResolutionEnabled $false`

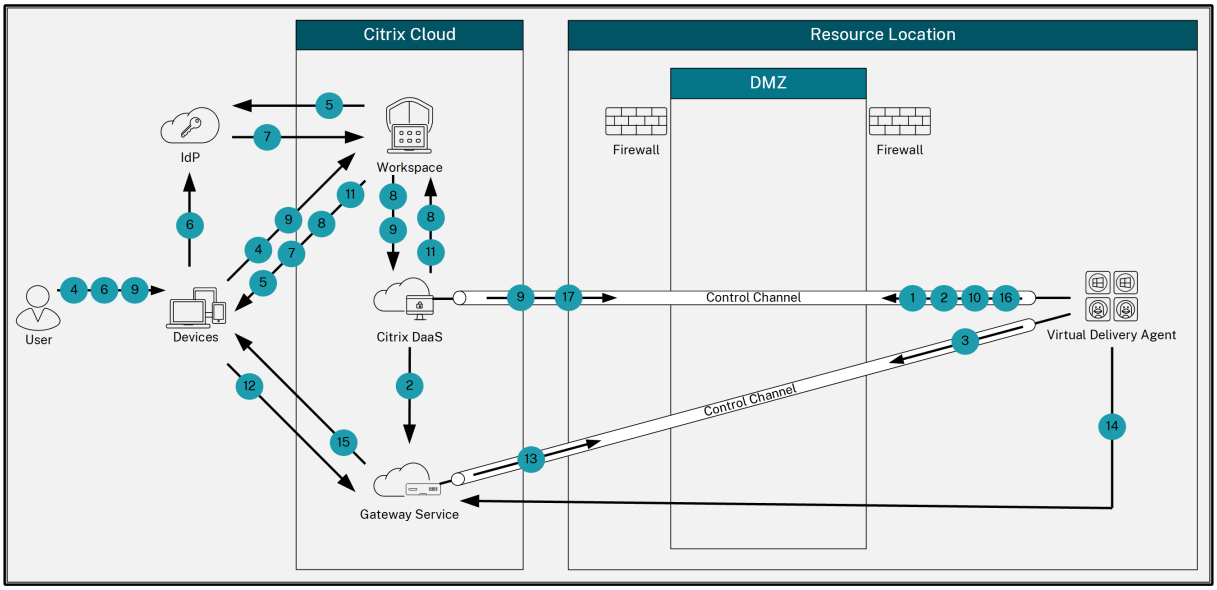
O instalador de VDA 2203 não permite inserir barra (/) no endereço proxy

Como alternativa, você pode configurar o proxy no registro depois que o VDA for instalado:

```
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 do Rendezvous

O diagrama a seguir ilustra a sequência de etapas sobre o fluxo de tráfego do Rendezvous.



1. O VDA estabelece uma conexão WebSocket com o Citrix Cloud e se registra.
2. O VDA se registra no Citrix Gateway Service e obtém um token dedicado.
3. O VDA estabelece uma conexão de controle persistente com o Gateway Service.
4. O usuário navega até o Citrix Workspace.
5. O Workspace avalia a configuração de autenticação e redireciona os usuários para o IdP apropriado para autenticação.
6. O usuário insere suas credenciais.
7. Depois de validar com êxito as credenciais do usuário, o usuário é redirecionado para o Workspace.
8. O Workspace faz a contagem dos recursos para o usuário e os exibe.
9. O usuário seleciona uma área de trabalho ou aplicativo no Workspace. O Workspace envia a solicitação ao Citrix DaaS, que faz a intermediação da conexão e instrui o VDA para se preparar para a sessão.
10. O VDA responde com o recurso Rendezvous e sua identidade.
11. O Citrix DaaS gera um tíquete de inicialização e o envia para o dispositivo do usuário por meio do Workspace.
12. O ponto de extremidade 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 conclui a conexão entre o ponto de extremidade e o VDA.
16. O VDA verifica o licenciamento para a sessão.
17. O Citrix DaaS envia as políticas aplicáveis ao VDA.

HDX Direct (Preview técnico)

May 15, 2023

Ao acessar os recursos fornecidos pela Citrix, o HDX Direct permite que os dispositivos do cliente estabeleçam uma conexão direta segura com o VDA se houver uma linha de visão direta.

> **Importante:**
>
> O HDX Direct está atualmente na versão Preview técnica. Para enviar feedback ou relatar problemas, use este formulário.

Requisitos

A seguir estão os requisitos para usar o HDX Direct:

- Plano de controle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2303 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2303 ou posterior
- Aplicativo Workspace
  - Windows: versão 2303 ou posterior
- Nível de acesso
  - Citrix Workspace
  - Citrix Gateway Service
  - NetScaler Gateway
- Firewall
  - Máquina VDA
    - TCP 443 de entrada (ICA por TCP)
    - UDP 443 de entrada (ICA por EDT)
  - Rede

Protocolo	Porta	Origem	Destino
TCP	443	Cliente	VDA
UDP	443	Cliente	VDA

Configuração

O HDX Direct está desativado por padrão. Você pode configurar esse recurso usando a configuração HDX Direct na política da Citrix.

- **Allowed**: o HDX Direct está ativado e tenta estabelecer uma conexão direta com o host da sessão quando uma sessão está conectada.
- **Prohibited**: a configuração padrão. O HDX Direct está desativado e impede que o cliente tente se conectar diretamente ao host da sessão quando conectado por meio de um Gateway.

Para confirmar que o HDX Direct estabeleceu com êxito uma conexão direta, use 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 uma conexão HDX Direct foi estabelecida com sucesso, você verá o seguinte:

- Protocolo de transporte
  - UDP > DTLS > CGP > ICA (se estiver usando EDT)
  - TCP > SSL > CGP > ICA (se estiver usando TCP)
- O endereço remoto e o endereço do cliente são iguais

Considerações

A seguir estão algumas considerações sobre o uso do HDX Direct:

- Ao usar máquinas não persistentes para seus aplicativos e áreas de trabalho virtuais, não habilite o HDX Direct na imagem mestre/modelo para evitar gerar certificados para a máquina virtual (VM) mestre.

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, a

criptografia em nível de rede (TLS/DTLS) é usada para protegê-las, aproveitando os certificados autoassinados.

Há três estágios que abrangem diferentes partes do recurso: pré-lançamento, lançamento e pós-lançamento.

Etapa de pré-lançamento

Esse é o estágio inicial, que abrange a criação e o gerenciamento de certificados. Essas tarefas são gerenciadas pelos seguintes serviços na máquina VDA, e são configuradas para serem executadas automaticamente na inicialização da máquina:

- Citrix ClxMtp Service: responsável pela geração e rotação do certificado CA.
- Citrix Certificate Manager Service: responsável por gerar e gerenciar o certificado CA raiz autoassinado, as chaves dos certificados da máquina e os certificados da máquina.

Veja a seguir uma visão geral do processo de gerenciamento de certificados:

1. Os serviços começam na inicialização da máquina.
2. O Citrix ClxMtp Service cria chaves se nenhuma tiver sido criada ainda.
3. O Citrix Certificate Manager Service verifica se o HDX Direct está ativado. Se não estiver, o serviço para sozinho.
4. Se o HDX Direct estiver ativado, o Citrix Certificate Manager Service verifica se há um certificado CA raiz autoassinado. Se não houver, é criado um certificado raiz autoassinado.
5. Quando um certificado CA raiz está disponível, o Citrix Certificate Manager Service verifica se há um certificado de máquina autoassinado. Se não houver, o serviço gera chaves e cria um novo certificado usando o FQDN da máquina.
6. Se houver um certificado de máquina existente criado pelo Citrix Certificate Manager Service e o nome do assunto não corresponder ao FQDN da máquina, um novo certificado será gerado.

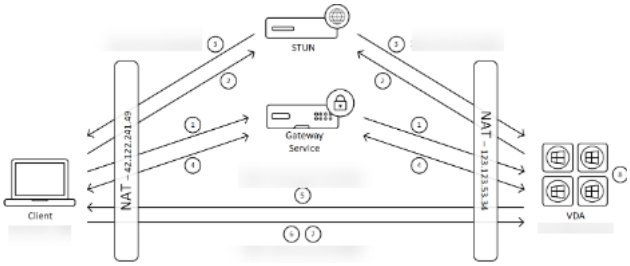
> **Nota:**
>
> O Citrix Certificate Manager Service gera certificados RSA que utilizam chaves de 2048 bits.

Etapa de lançamento

Para estabelecer com êxito uma conexão HDX Direct segura, o cliente deve confiar nos certificados usados para proteger a sessão. Para facilitar, o VDA envia suas informações de certificado ao agente quando uma sessão está sendo intermediada. Posteriormente, o agente envia essas informações ao Workspace para serem incluídas no arquivo ICA que é enviado ao cliente para iniciar a sessão.

Etapa pós-lançamento

Depois que uma sessão é intermediada com sucesso, a sessão é iniciada. A seguir você tem uma visão geral do processo de conexão HDX Direct:



1. O cliente estabelece uma conexão com o VDA por meio do Gateway Service.
2. Após uma conexão bem-sucedida, o VDA envia o FQDN da máquina VDA e uma lista de seus endereços IP para o cliente.
3. O cliente examina os endereços IP para ver se consegue acessar o VDA diretamente.
4. Se o cliente conseguir acessar o VDA diretamente com qualquer um dos endereços IP compartilhados, o cliente estabelecerá uma conexão direta segura com o VDA.
5. Quando a conexão direta é estabelecida com êxito, a sessão é transferida para a nova conexão, e a conexão com o Gateway Service é encerrada.

Problemas conhecidos

A seguir estão os problemas conhecidos com o HDX Direct:

- A conexão HDX Direct pode falhar quando o Rendezvous está desativado.
- A conexão HDX Direct pode falhar ao iniciar sessões a partir de um site do Citrix Virtual Apps and Desktops 2303 no local.
- O aplicativo Workspace pode falhar se o VDA estiver em execução no Windows 11.

Dispositivos

August 30, 2023

HDX oferece uma experiência de usuário de alta definição em qualquer dispositivo, em qualquer local. Os artigos na seção Dispositivos descrevem estes dispositivos:

- Mapeamento da unidade cliente
- Dispositivo USB genérico
- Dispositivos móveis e com tela de toque

- Dispositivos seriais
- Teclados especiais
- Dispositivos TWAIN
- Webcams
- Dispositivos WIA

Dispositivo USB otimizado x 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 otimizado de canal virtual, a menos que seja colocado 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 tem funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos recursos.

Com dispositivos USB de armazenamento em massa, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados pelas políticas da Citrix. As principais diferenças são:

Se o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estiverem ativados e um dispositivo de armazenamento em massa for inserido antes ou depois que uma sessão é iniciada, ele será redirecionado usando o mapeamento da unidade cliente.

Quando essas condições são verdadeiras, o dispositivo de armazenamento em massa é redirecionado usando o redirecionamento USB genérico:

- Tanto o redirecionamento USB genérico quanto as políticas de mapeamento da unidade cliente são ativados.
- Um dispositivo é 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 http://support.citrix.com/article/CTX123015.

Recurso	Client drive mapping	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 na sessão virtual.	Somente Citrix Virtual Desktops

Mapeamento da unidade cliente (CDM)

November 9, 2023

O Mapeamento da unidade cliente disponibiliza unidades de armazenamento no ponto de extremidade do cliente em uma sessão do Citrix HDX para permitir que arquivos e pastas sejam transferidos do cliente para o host da sessão e vice-versa. Esse recurso é ativado por padrão com os privilégios de leitura e gravação. Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, ative a configuração de política **Read-only client drive access**. Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está definida como **Allowed** e também está adicionada à política.

Por padrão, como medida de segurança, as unidades de ponto de extremidade são mapeadas sem a permissão de execução. Para permitir que os usuários executem 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 do sistema do Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 ou posterior
  - Linux: consulte a documentação do Linux VDA

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: consulte os requisitos do sistema do aplicativo Workspace para Linux

Políticas relacionadas

Consulte a seção Consulta de configurações de política para ver as configurações de CDM.

Cenários de salto duplo

O CDM é suportado em cenários de salto duplo. Por padrão, a unidade do ponto de extremidade cliente é mapeada para a sessão do segundo salto e as unidades do primeiro salto não estão disponíveis. No entanto, isso pode ser configurado de modo que as unidades do primeiro salto sejam mapeadas na sessão do segundo salto, em vez das unidades do ponto de extremidade cliente.

Para configurar a funcionalidade, edite o seguinte valor do registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanc
- Nome do valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Dados de valor:
  - True –mapeia as unidades da sessão do primeiro salto na sessão do segundo salto
  - False –mapeia as unidades do ponto de extremidade cliente na sessão do segundo salto

> **Nota:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Dispositivos USB genéricos

June 24, 2022

A tecnologia HDX fornece **suporte otimizado** para a maioria dos dispositivos USB mais difundidos. Estes dispositivos incluem:

- Monitores
- Mouses
- Teclados
- Telefones VoIP
- Fones de ouvido
- Webcams
- Scanners
- Câmeras
- Impressoras
- Unidades
- Leitores de cartões inteligentes
- Tablets de desenho
- Mesas gráficas para 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 têm suporte otimizado ou quando esse 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 Configuração do redirecionamento de dispositivo USB composto e Configuração do suporte USB.

Suporte para dispositivos clientes móveis e com tela sensível ao toque

July 13, 2023

O Citrix Virtual Apps and Desktops permite que os usuários acessem seus aplicativos e áreas de trabalho publicados a partir de dispositivos clientes móveis e com tela sensível ao toque.

Requisitos

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 7.15 ou posterior
- Citrix DaaS

Host da 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
- Aplicativo Citrix Workspace para Windows versão 1808 ou superior

Modo tablet para dispositivos de tela sensível ao toque usando o Windows Continuum

O Continuum é um recurso do Windows 10 que se adapta à maneira como o dispositivo cliente é usado. Quando o VDA detecta a presença de um teclado ou mouse em um cliente ativado por toque, ele coloca o cliente no modo desktop. Se não houver teclado nem mouse presentes, o VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão da sessão e também dentro da sessão quando o teclado ou o mouse é conectado ou desconectado.

O recurso é ativado por padrão. Para desativar esse recurso, defina as configurações da política Tablet mode toggle policy settings.

Além dos requisitos para dispositivos com tela sensível ao toque mencionados acima, o seguinte é necessário para o Windows Continuum:

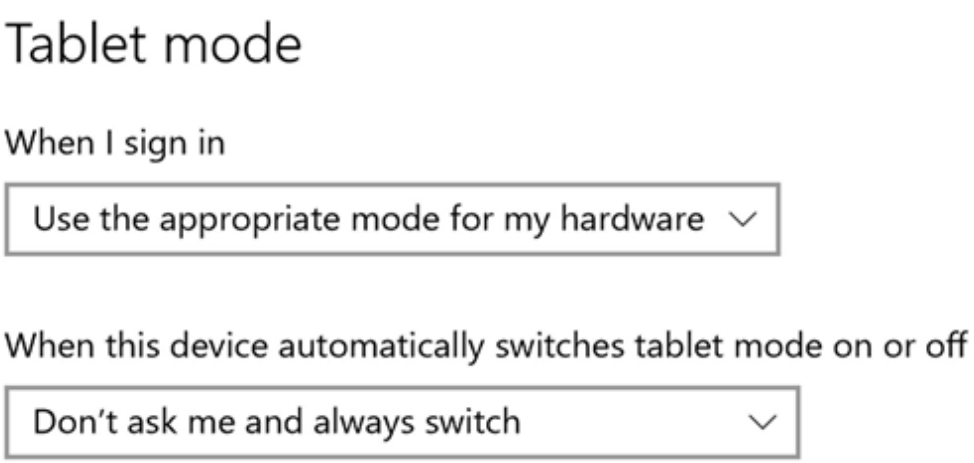
Citrix Hypervisor

- Citrix Hypervisor 8.2 ou superior
- Execute o comando XenServer CLI para permitir a comutação laptop/tablet:
  xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

> **Importante:**
>
> A atualização da imagem base de um catálogo de máquinas existente após alterar a configuração de metadados não afeta nenhuma máquina virtual provisionada anteriormente. Depois de alterar a imagem base da VM do XenServer, crie um catálogo, escolha a imagem base e provisione uma nova máquina MCS (Machine Creation Services).

Host da 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 precisará definir as seguintes opções nos menus suspensos após iniciar a primeira sessão ICA e reiniciar o VDA:**
    - **Settings > System > Tablet Mode**
      - Use the appropriate mode for my hardware
      - Don't ask me and always switch



O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores.
- A tela Iniciar e todos os aplicativos que você iniciar abrem em uma tela cheia.
- A barra de tarefas contém um botão de voltar.
- Ícones excluídos da barra de tarefas.

Você tem acesso ao Explorador de Arquivos.

O Windows 10 carrega o driver GPIO no computador virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro do computador 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 maneira que faz ao usar PC e um teclado e mouse.

Canetas Microsoft Surface Pro e Surface Book

Apoiamos a funcionalidade padrão da caneta com aplicações baseadas em Windows Ink. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e modelo de caneta. Por exemplo, a pressão da caneta pode ser de até 4096 níveis. Esse recurso é ativado por padrão.

A seguir estão os requisitos para suporte à funcionalidade da caneta:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 1903 ou posterior
- Citrix DaaS

Host da sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2016 ou posterior
- 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 neste gráfico:

Para desativar ou ativar 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 às limitações do sistema operacional no Windows Server 2k22, os usuários não poderão definir atalhos de caneta ou fazer ajustes nas configurações de caneta/tinta no Painel de Controle ao se conectarem a áreas de trabalho ou aplicativos do Server 2k22.
- Os atalhos de caneta não respondem em um cliente Windows 11 com caneta habilitada devido à limitação do sistema operacional.

Portas seriais

June 24, 2022

A maioria dos PCs novos não tem portas seriais (COM) incorporadas. As portas são fáceis de adicionar usando conversores USB. Os aplicativos adequados para portas seriais geralmente envolvem sensores, controladores, leitores de cheques antigos, pads e assim por diante. Alguns dispositivos USB de porta COM virtual usam drivers específicos do fornecedor no lugar dos drivers fornecidos pelo Windows (usbser.sys). Esses drivers permitem que você force a porta COM virtual do dispositivo USB para que ele não mude mesmo se conectado a diferentes soquetes USB. Isto pode ser feito no **Gerenciador de dispositivos > Portas (COM e LPT) > Propriedades** ou no aplicativo que controla o dispositivo.

O mapeamento de porta COM do cliente permite que os dispositivos anexados às portas COM no ponto de extremidade 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 usam então o link para acessar a porta.

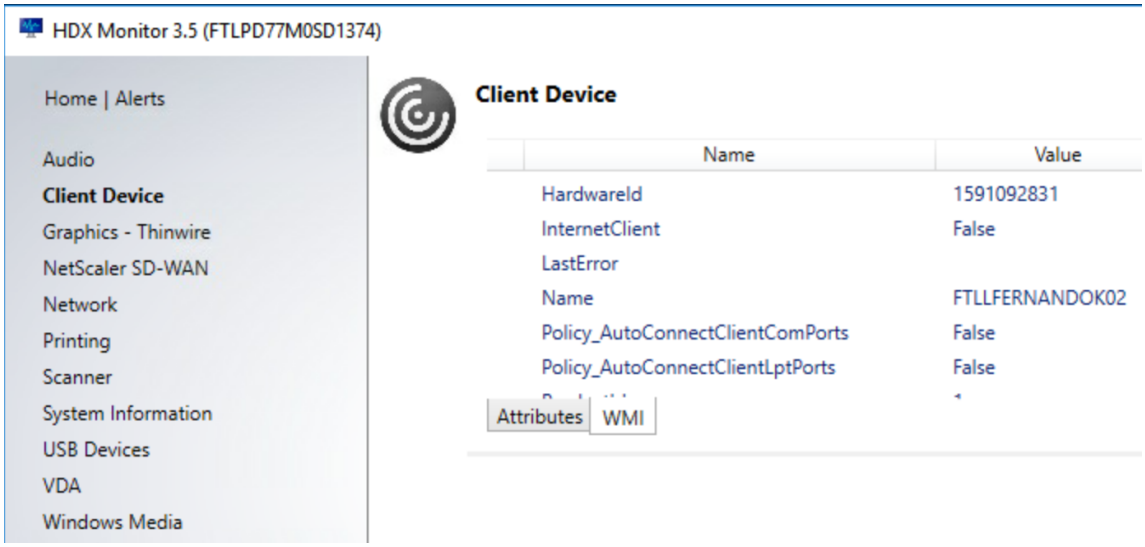
> **Importante:**
>
> Como um dispositivo pode se conectar ao ponto de extremidade usando USB diretamente, isso não significa que ele pode ser redirecionado usando o redirecionamento USB genérico. Alguns dispositivos USB funcionam como portas COM virtuais, os quais os aplicativos podem acessar da mesma maneira que a 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 conectado através de uma porta RS-485, os aplicativos podem não funcionar de todo. Obtenha um conversor de RS-485 em RS232 para usar o RS-485 como uma porta COM.
>
> **Importante:**
>
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um bloco de assinatura) consistentemente somente 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 de console Manage. Para obter mais informações sobre políticas, consulte Configurações da política de redirecionamento de porta.
- Prompt de comando de VDA.
- Ferramenta de configuração de Área de Trabalho Remota (Serviços de Terminal).

1. Ative as políticas **Client COM port redirection** e **Auto connect client COM ports Studio**. Depois de aplicadas, algumas informações estão disponíveis no HDX Monitor.



2. Se a função **Auto connect client COM ports** não conseguir mapear a porta, você poderá 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 1 a 9 estão disponíveis para mapeamento). **Z** é o número da porta COM do cliente que você quer mapear.

   Para confirmar que a operação foi bem-sucedida, digite **NET USE** em um prompt de comando VDA. A lista que aparece contém unidades mapeadas, portas LPT e portas COM mapeadas.

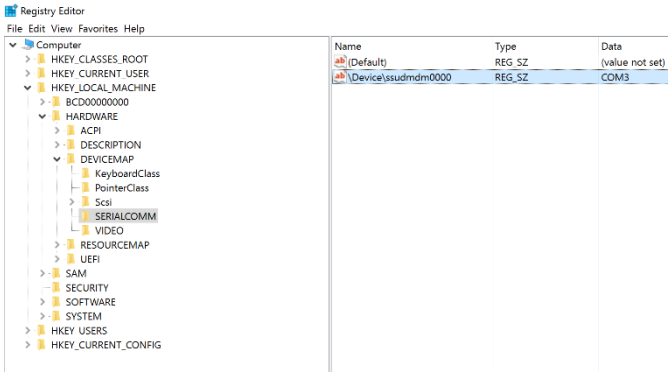
```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

3. Para usar essa porta COM em uma área de trabalho virtual ou aplicativo, instale o aplicativo de dispositivo do usuário e aponte-o para o nome da porta COM mapeado. Por exemplo, se você mapear COM1 no cliente para COM3 no servidor, instale seu aplicativo de dispositivo de porta COM no VDA e aponte-o para COM3 durante a sessão. Use esta porta COM mapeada como você faria uma porta COM no dispositivo do usuário.

> **Importante:**
>
> O mapeamento de porta COM não é compatível com TAPI. Você não pode mapear dispositivos da Windows Telephony Application Programming Interface (TAPI) às portas COM do cliente. A TAPI define uma maneira padrão para que os aplicativos controlem funções telefônicas para chamadas de dados, fax e voz. A TAPI gerencia a sinalização, incluindo discagem, atendimento e término de chamadas. Além disso, serviços suplementares, como espera, transferência e chamadas em conferência.

Solução de problemas

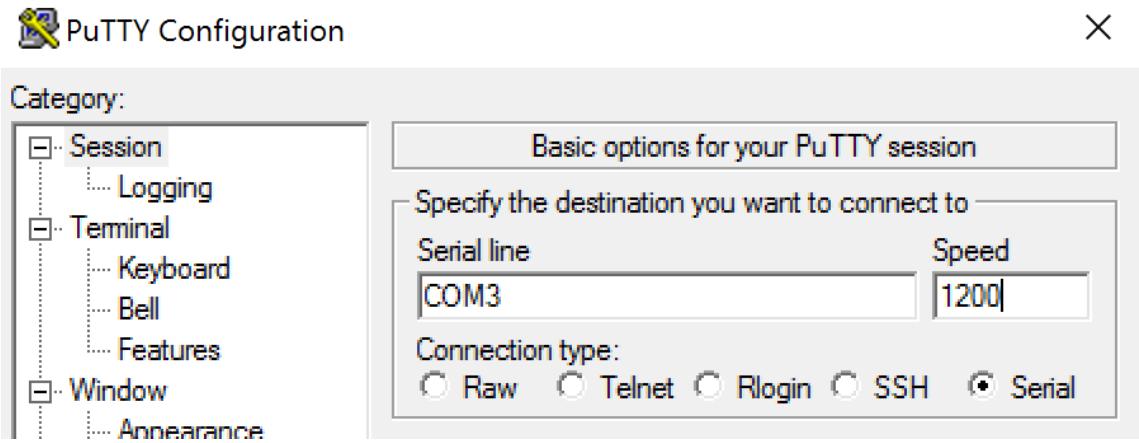
1. Você deverá ser capaz de acessar o dispositivo diretamente do ponto de extremidades, sem passar pelo Citrix. Embora a porta não seja mapeada para o VDA, você não está conectado a uma sessão Citrix. Siga todas as instruções de solução de problemas que acompanham o dispositivo e primeiro verifique se ele funciona localmente.
   Quando um dispositivo é conectado a uma porta COM serial, é criada uma chave de registro na estrutura de registro mostrada aqui:



   Você também pode encontrar essas informações no prompt de comando executando **chgport/-query**.


```
C:\Windows\system32\cmd.exe
C:\Users\fernandok>chgport /query
COM3 = \Device\ssudmdm0000

C:\Users\fernandok>mode

Status for device COM3:
-----------------------
    Baud:            1200
    Parity:          Even
    Data Bits:       7
    Stop Bits:       1
    Timeout:         OFF
    XON/XOFF:        OFF
    CTS handshaking: OFF
    DSR handshaking: OFF
    DSR sensitivity: OFF
    DTR circuit:     ON
    RTS circuit:     ON
```

Se as instruções de solução de problemas do 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 indicar a porta COM em uso e os bits Baud/Parity/Data Bits/Stop, de que você precisa em sua sessão do PuTTY. Se a conexão PuTTY for bem-sucedida, pressione **Enter** para ver o feedback no dispositivo. Os caracteres que você digitar poderão 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 na etapa anterior, mas desta vez no PuTTY do VDA. Se o PuTTY não mostrar o erro **Unable to open connection to COM1. Unable to open serial port**, outro dispositivo pode estar usando COM1.

3. Execute **chgport /query**. Se o driver serial do Windows integrado 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 todos os mapeamentos existentes (por exemplo, COM1) no VDA.

   NET USE COM1 /DELETE

   C. Mapeie o dispositivo para o VDA.

   NET USE COM1: \\CLIENT\COM3:

   D. Aponte o 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 a COM1, por exemplo, COM3). Verifique se o seu aplicativo está apontando para essa porta:
   NET USE COM3: \\CLIENT\COM3

4. Se você vir agora a porta mapeada, o PuTTY está funcionando, mas sem passar dados, pode ser uma condição de corrida. O aplicativo pode conectar e abrir a porta antes que ela seja mapeada, impedindo-a de ser mapeada. Experimente uma das seguintes soluções:

- Abra um segundo aplicativo publicado no mesmo servidor. Aguarde alguns segundos para que a porta seja mapeada e abra então o aplicativo real que tenta usar a porta.
- Ative as políticas de redirecionamento de porta COM a partir do Editor de Política de Grupo no Active Directory em vez de usar a interface Manage > Full Configuration do serviço. Essas políticas são o **Client COM port redirection** e **Auto connect client COM ports**. As políticas aplicadas desta maneira podem ser processadas antes das políticas de console Manage, garantindo que a porta COM seja mapeada. As políticas da 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 exclua qualquer mapeamento no VDA, remapeie a porta COM virtual e, em seguida, inicie 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\<Caminho do seu software>\
```

5. O Process Monitor da Sysinternals é a ferramenta de último recurso. Ao executar a ferramenta no VDA, encontre e filtre objetos como COM3, picaser.sys, CdmRedirector, mas especialmente <seu_app>.exe. Podem aparecer erros como Acesso negado ou similares.

Teclados especiais

June 24, 2022

Teclados Bloomberg

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Os Citrix Virtual Apps and Desktops são compatíveis com o teclado Starboard Bloomberg modelo 4 (e o modelo 3 anterior). Este teclado apresenta características especiais que os clientes do setor financeiro usam para acessar dados do mercado financeiro e realizar as negociações rapidamente.

Esse teclado é compatível com os chaveadores KVM e pode funcionar em dois modos:

- PC (um cabo USB sem KVM)
- Modo KVM (dois cabos USB com um roteamento através do KVM)

> **Importante:**
>
> Recomendamos que você use o teclado Bloomberg com apenas uma sessão. Não recomendamos usar o teclado com várias sessões simultâneas (um cliente para várias sessões).

O teclado Bloomberg 4 é um dispositivo composto USB que compreende quatro dispositivos USB em um shell 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 integrado, microfone e tomada para o microfone e fone de ouvido.
- 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.
- Aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver para Windows 4.8, no mínimo, para oferecer suporte ao teclado Bloomberg modelo 3 e 4.
- Aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver for Windows 4.12, no mínimo, para usar o modo KVM (dois cabos USB com um roteado através do KVM) para o modelo 4.

Para obter informações sobre como configurar teclados Bloomberg no aplicativo Citrix Workspace para Windows, consulte Configurar teclados Bloomberg.

Para habilitar o suporte ao teclado Bloomberg, consulte Teclados Bloomberg na lista de recursos gerenciados por meio do registro.

Verifique o suporte:

Para determinar se o suporte ao teclado Bloomberg está habilitado no aplicativo Citrix Workspace, verifique se o Desktop Viewer relata corretamente os dispositivos do teclado Bloomberg.

Cenário de desktop:

Abra o Desktop Viewer. Se o suporte para o teclado Bloomberg estiver habilitado, o Desktop Viewer mostra três dispositivos sob o ícone USB:

- Scanner de impressão digital Bloomberg
- Características do teclado Bloomberg
- Teclado Bloomberg LP 2013

Cenário de aplicativo sem interrupção:

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 em cada um desses dispositivos indica que eles são remotos para a sessão.

Dispositivos TWAIN

June 24, 2022

Requisitos

- O scanner deve estar em conformidade com TWAIN.
- Instale os drivers TWAIN no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, através de USB).
- Verifique se o scanner está usando o driver TWAIN local e não o Serviço de Aquisição de Imagens do Windows.
- Verifique se não há nenhuma política aplicada à conta de usuário que é usada para o teste, e que esteja limitando a largura de banda dentro da sessão de ICA. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Para obter informações sobre as configurações de política, consulte Configurações da política de dispositivos TWAIN.

Webcams

August 18, 2022

Streaming de webcam de alta definição

Podem ser usadas webcams por aplicativos de videoconferência em execução dentro da sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de

formato suportados. Quando uma sessão começa, 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. Damos suporte a resoluções de webcam até 1920x1080.

Esse recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para obter uma lista de plataformas de aplicativos Citrix Workspace que suportam o redirecionamento de webcam HDX, consulte Citrix Workspace app feature matrix.

Para obter mais informações sobre streaming de webcam de alta definição, consulte Videoconferência HDX e compactação de vídeo na webcam.

Você pode usar uma chave de registro para desativar e ativar 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 pelo registro.

Dispositivos WIA

June 24, 2022

Requisitos

- O scanner deve estar em conformidade com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, através de USB).
- Verifique se o scanner está usando o Serviço de Aquisição de Imagens do Windows local e não o driver TWAIN.
- Verifique se não há nenhuma política aplicada à conta de usuário que é usada para o teste, e que esteja limitando a largura de banda dentro da sessão de ICA. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Lista de permissões de aplicativos de Aquisição de Imagens do Windows

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento do scanner de Aquisição de Imagens do Windows. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém Aquisição de Imagens do Windows. Por padrão, nenhum aplicativo tem acesso a Aquisição de Imagens do Windows.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração de Lista de permissões de aplicativos de Aquisição de Imagens do Windows na lista de recursos gerenciados pelo registro.

Para obter informações sobre as configurações de política, consulte WIA devices policy settings.

Gráficos

June 24, 2022

Os elementos gráficos do Citrix HDX incluem um extenso conjunto de tecnologias de codificação e aceleração gráfica que otimiza a entrega de aplicativos gráficos avançados do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops). As tecnologias gráficas oferecem a mesma experiência de uso que de um desktop físico ao trabalhar remotamente com aplicativos virtuais com uso intensivo de gráficos.

Você pode usar software ou hardware para renderização gráfica. A renderização de software requer uma biblioteca de terceiros chamada software rasterizer. Por exemplo, o Windows inclui o WARP rasterizer para gráficos baseados em DirectX. Às vezes, você pode preferir usar um software renderer alternativo. A renderização de 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. Ao usar as políticas da Citrix, os administradores de TI também podem definir várias configurações relacionadas a gráficos para atender a diferentes requisitos e oferecer a experiência desejada ao usuário.

Thinwire

Thinwire é a tecnologia de exibição remota padrão da Citrix usada no Citrix DaaS.

A tecnologia de exibição remota permite que os gráficos gerados em um computador sejam transmitidos, normalmente através de uma rede, para outro computador para exibição. Os gráficos são gerados como resultado de uma entrada do usuário, por exemplo, pressionamentos de teclas ou ações do mouse.

HDX 3D Pro

Os recursos do HDX 3D Pro no Citrix DaaS permitem que você forneça áreas de trabalho e aplicativos com 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 apenas a aceleração da GPU do DirectX.

Aceleração da GPU para SO Windows de sessão única

Usando o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de áreas de trabalho ou aplicativos hospedados em computadores com SO de sessão única. O HDX 3D Pro suporta computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de virtualização GPU e GPU Passthrough oferecidas pelos hipervisores XenServer, vSphere e Hyper-V (somente passagem).

Usando GPU Passthrough, você pode criar VMs com acesso exclusivo a hardware dedicado de processamento gráfico. Você pode instalar várias GPUs no hipervisor e atribuir VMs a cada uma dessas GPUs individualmente.

Usando a virtualização da GPU, várias máquinas virtuais podem acessar diretamente o poder de processamento gráfico de uma única GPU física.

Aceleração da GPU para SO multissessão Windows

O HDX 3D Pro permite que aplicativos gráficos pesados em execução em sessões de SO multissessão Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não diminui a velocidade de processamento da 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 tem mais suporte. Em vez disso, use o Thinwire com o transporte adaptativo ativado.

Framehawk é uma tecnologia de exibição remota para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE). O Framehawk supera os desafios da interferência espectral e da propagação multipath e oferece uma experiência de usuário fluida e interativa aos usuários de áreas de trabalho e aplicativos virtuais.

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a deter e ativar o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um estorvo para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que seja 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 a VDA.

Informações correlatas

- HDX 3D Pro

- Aceleração da GPU para SO Windows de sessão única
- Aceleração da GPU para SO multissessão Windows
- Thinwire
- Marca d'água de sessão baseada em texto

HDX 3D Pro

June 24, 2022

Os recursos do HDX 3D Pro no Citrix Virtual Apps and Desktops permitem que você forneça áreas de trabalho e aplicativos com 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 apenas a aceleração da GPU do DirectX.

Para obter as configurações de política HDX 3D Pro, consulte Optimize for 3D graphics workload.

Todos os aplicativos Citrix Workspace com suporte 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 aplicativo Citrix Workspace para Windows e Citrix Workspace para Linux. Para obter mais informações sobre versões compatíveis do aplicativo Citrix Workspace, consulte Lifecycle Milestones for Citrix Workspace app.

Exemplos de aplicações profissionais 3D incluem:

- Aplicações de design, fabricação e engenharia assistidas por computador (CAD/CAM/CAE)
- Software do Sistema de Informação Geográfica (SIG)
- Sistema de comunicação de arquivamento de imagens (PACS) para imagens médicas
- Aplicativos que usam as versões mais recentes OpenGL, DirectX, NVIDIA CUDA e OpenCL e WebGL
- Aplicativos não gráficos de uso intensivo computacional 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 sobre conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de uma área de trabalho 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.

HDX 3D Pro fornece aceleração de GPU para computadores com sistema operacional Windows de sessão única e computadores com sistema operacional Windows multissessão. Para obter mais informações, consulte Aceleração da GPU para SO Windows de sessão única and Aceleração da GPU para SO multissessão Windows.

HDX 3D Pro é compatível com as tecnologias de passagem de GPU e virtualização de GPU oferecidas pelos seguintes Hypervisors, além do bare metal:

- Citrix Hypervisor
  - Passagem 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 na 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 de HDX. Para baixar a ferramenta e saber mais sobre ela, consulte https://taas.citrix.com/hdx/download/.

Aceleração da GPU para SO Windows multissessão

June 24, 2022

O HDX 3D Pro permite que aplicativos com muitos gráficos em execução em sessões de SO multissessão Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Movendo a renderização do OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não diminui a velocidade de processamento da 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).

Em instruções que incluem a edição do registro, tenha cuidado: editar o registro incorretamente pode causar sérios problemas que exigirão que você reinstale o 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. Tenha o cuidado 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. Tem as seguintes características:

- Pode ser usado em máquinas virtuais ou bare metal para aumentar a escalabilidade e o desempenho dos aplicativos.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não requer 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 ou de GPU virtual (vGPU) seguindo os requisitos do fornecedor do Hypervisor e da GPU. Implantações bare-metal em computadores físicos do Windows Server também têm suporte.

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 obter uma lista de compatibilidade de hardware do Citrix Hypervisor, consulte a Lista de compatibilidade de hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de exibição habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desative todas, exceto uma delas, usando o Gerenciador de Dispositivos.

A escalabilidade usando o compartilhamento de GPU depende de vários fatores:

- Os aplicativos que estão sendo executados
- A quantidade de RAM de vídeo que eles consomem
- O poder de processamento da placa gráfica

Alguns aplicativos lidam com escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha no driver da placa gráfica. Limite o número de usuários simultâneos para evitar esses problemas.

Para confirmar que a aceleração da GPU está ocorrendo, use uma ferramenta de terceiros, como 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 (quando disponível). Se tal hardware não estiver disponível, o VDA recorre à codificação baseada em CPU usando o codec de vídeo do software. Para obter mais informações, consulte Configurações da política de gráficos.

Renderização DirectX, Direct3D e WPF

As renderizações DirectX, Direct3D e WPF só estão disponíveis em servidores com uma GPU que dá suporte a uma versão de interface de driver de exibição (DDI) de 9ex, 10 ou 11.

- No Windows Server 2008 R2, o DirectX e o Direct3D não exigem configurações especiais para usar uma única GPU.
- No Windows Server 2012 e posteriores, as sessões de Serviços de Ambiente de Trabalho Remoto (RDS) no servidor Host de Sessão de Área de Trabalho Remota usam o Driver de Renderização Básico da Microsoft como o adaptador padrão. Para usar a GPU nas sessões do RDS no Windows Server 2012 e posterior, ative 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 do 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 os aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no Registro do servidor executando sessões do sistema operacional multisessão do Windows. Para obter informações sobre a configuração do Registro, consulte Windows Presentation Foundation (WPF) rendering na lista de recursos gerenciados por meio do registro.

Aceleração de GPU para aplicações CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desativada por padrão.

Para usar os recursos POC de aceleração CUDA, faça as configurações do registro. Para obter informações, consulte GPU acceleration for CUDA or OpenCL applications na lista de recursos gerenciados por meio do registro.

Aceleração da GPU para SO Windows de sessão única

June 24, 2022

Usando o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de áreas de trabalho ou aplicativos hospedados em computadores com SO de sessão única. O HDX 3D Pro dá suporte a computadores host físicos (inclusive estações de trabalho desktop, blade e rack) e tecnologias de virtualização GPU e GPU Passthrough oferecidas pelo Citrix Hypervisor, vSphere, Nutanix e Hyper-V (somente passagem).

HDX 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para um desempenho ideal de WAN e sem fio. HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como a técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que dão suporte a NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que dão suporte a 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 são necessários gráficos perfeitos em pixels, como imagens médicas. A verdadeira compactação sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

  Ao usar compactação sem perdas:

  - O indicador de sem perdas, um ícone de 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 de política de **Visual Quality** especifica **Build to lossless**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.
  - O comutador sem perdas permite que o usuário mude ao modo sempre sem perdas a qualquer momento dentro da sessão. Para selecionar ou desmarcar **Lossless anytime within a session**, clique com o botão direito do mouse no ícone e clique em **Switch to pixel perfect** ou use o atalho ALT+SHIFT+1.

    Para compactação sem perdas: HDX 3D Pro usa o codec sem perdas para compactação, independentemente do codec selecionado através da política.

    Para compactação com perdas: HDX 3D Pro usa o codec original, o padrão ou o selecionado através da política.

    As configurações do comutador sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Always lossless** na configuração Política de **Visual quality**.
- Você pode substituir o atalho padrão, ALT+SHIFT+1, para selecionar ou desmarcar Lossless within a session. Defina uma nova configuração de registro em HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HD

  - Nome: HKEY_LOCAL_MACHINE_HotKey, Tipo: String
  - O formato para configurar uma combinação de atalhos 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:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

- Suporte de monitor múltiplo e de alta resolução. Para máquinas de SO de sessão única, o HDX 3D Pro suporta dispositivos do 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. HDX 3D Pro suporta todas as resoluções de monitor e é limitado apenas pelos recursos da GPU no computador host.
- Resolução dinâmica. Você pode redimensionar a janela da área de trabalho virtual ou do aplicativo para qualquer resolução. **Nota**: O único método com suporte para mudar a resolução é redimensionando a janela de sessão VDA. Não há suporte para alterar a resolução de dentro da sessão VDA (por meio de **Painel de Controle \ > Aparência** e **Personalização > Exibição \ > Resolução da Tela**).
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro suporta placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passagem de GPU e compartilhamento de GPU. A vGPU NVIDIA permite que várias VMs tenham acesso direto e simultâneo a uma única GPU física, usando os mesmos drivers gráficos NVIDIA implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar 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 com atribuição de dispositivo discreto no Windows Server 2016.
- Suporte para gráficos de data center com a família de processadores Intel Xeon E3. O HDX 3D Pro suporta vários monitores (até 3), apagamento 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 e http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Suporte para AMD RapidFire nas placas de servidor AMD FirePro série S. O HDX 3D Pro suporta vários monitores (até 6), apagamento do console, resolução personalizada e alta taxa de quadros. Observação: o suporte HDX 3D Pro para AMD MxGPU (virtualização de GPU) funciona

apenas com vGPUs VMware vSphere. O Citrix Hypervisor e o Hyper-V são compatíveis com a passagem da GPU. Para obter mais informações, consulte AMD Virtualization Solution.

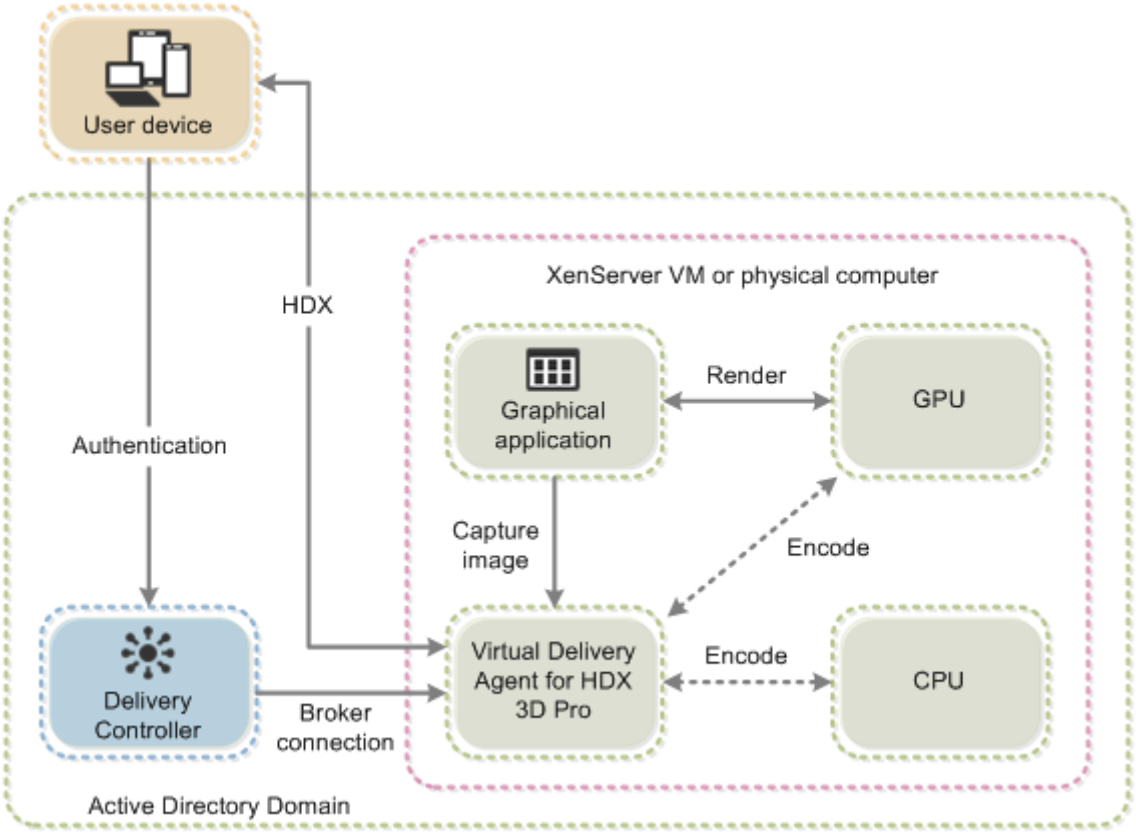
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e processadores gráficos Intel Iris Pro. Uma configuração de política (ativada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para codificação H.264 (quando disponível). Se esse hardware não estiver disponível, o VDA recorre à codificação baseada em CPU usando o codec de vídeo do software. Para obter mais informações, consulte Configurações da política de gráficos.

Como mostrado na figura a seguir:

- Quando um usuário faz logon no aplicativo Citrix Workspace e acessa o aplicativo virtual ou desktop, o Controlador 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 comprimir visualizações da área de trabalho completa ou apenas do aplicativo gráfico.

- As exibições da área de trabalho ou do aplicativo e as interações do usuário com elas são transmitidas entre o computador host e o dispositivo do usuário. Esta transmissão é feita através de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



Otimize a experiência do usuário HDX 3D Pro

Para usar o HDX 3D Pro com vários monitores, o computador host deverá estar configurado com pelo menos tantos monitores quanto 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 à área de trabalho virtual ou aplicativo 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 gráfica do aplicativo estiver em execução. Depois de 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 uma filial), recomendamos que você use a configuração de política de **Overall session bandwidth limit** para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que a largura de banda disponível não oscile extremamente 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 afetar 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 nesse cenário, determine a largura de banda necessária por usuário em períodos de pico e limite os usuários a esse valor 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 do Knowledge Center CTX128190.

Thinwire

May 30, 2023

Introdução

O Thinwire, uma 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 os gráficos gerados em um computador sejam transmitidos, normalmente através de uma rede, para outro computador para exibição.

Uma solução remota de exibição bem-sucedida fornece uma experiência de usuário altamente interativa que é semelhante à de um PC local. O Thinwire oferece essa experiência usando uma variedade de técnicas complexas e eficientes de análise de imagem e compactação. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de visualização remota.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso geral de negócios e é usado como a tecnologia de controle remoto de exibição 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 ativar o modo HDX 3D Pro usando políticas **Optimize for 3D graphics workload** ou **Visual quality > Build to lossless** para cenários em que as GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264 ou H.265) para codificar toda a tela usando aceleração de hardware se houver uma GPU. 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 sistema operacional Windows de sessão única.

Requisitos

O Thinwire é otimizado para sistemas operacionais modernos, incluindo Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e Windows 10. Para o Windows Server 2008 R2, recomenda-se o modo gráfico legado. Use os Modelos de política Citrix integradas, o SO legado de alta escalabilidade de servidor e o OS de legado otimizado para WAN para fornecer as combinações recomendadas da Citrix de configurações de política para esses casos de uso.

> **Nota:**
>
> Não oferecemos suporte ao modo gráfico legado nesta versão. Ele é incluído para compatibilidade com versões anteriores quando são usados o XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores VDA.

- A configuração de política que determina o comportamento do Thinwire, **Use video codec for compression**, está disponível nas versões VDA no Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.6 FP3 e versões posteriores. A opção **Usar codec de vídeo quando preferida** é a configuração padrão nas versões VDA Citrix Virtual Apps and Desktops 7 1808 ou versões posteriores e XenApp e XenDesktop 7.9 e versões posteriores.
- Todos os aplicativos Citrix Workspace oferecem suporte ao Thinwire. Alguns aplicativos do Citrix Workspace podem oferecer suporte a recursos do Thinwire que outros não oferecem, por exemplo, gráficos de 8 ou 16 bits para uso reduzido da largura de banda. O suporte para esses recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos de servidor (CPU, memória) em cenários de vários monitores e de 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 em 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 tela cheia H.264 ou H.265
- Thinwire com H.264 ou H.265 seletivo

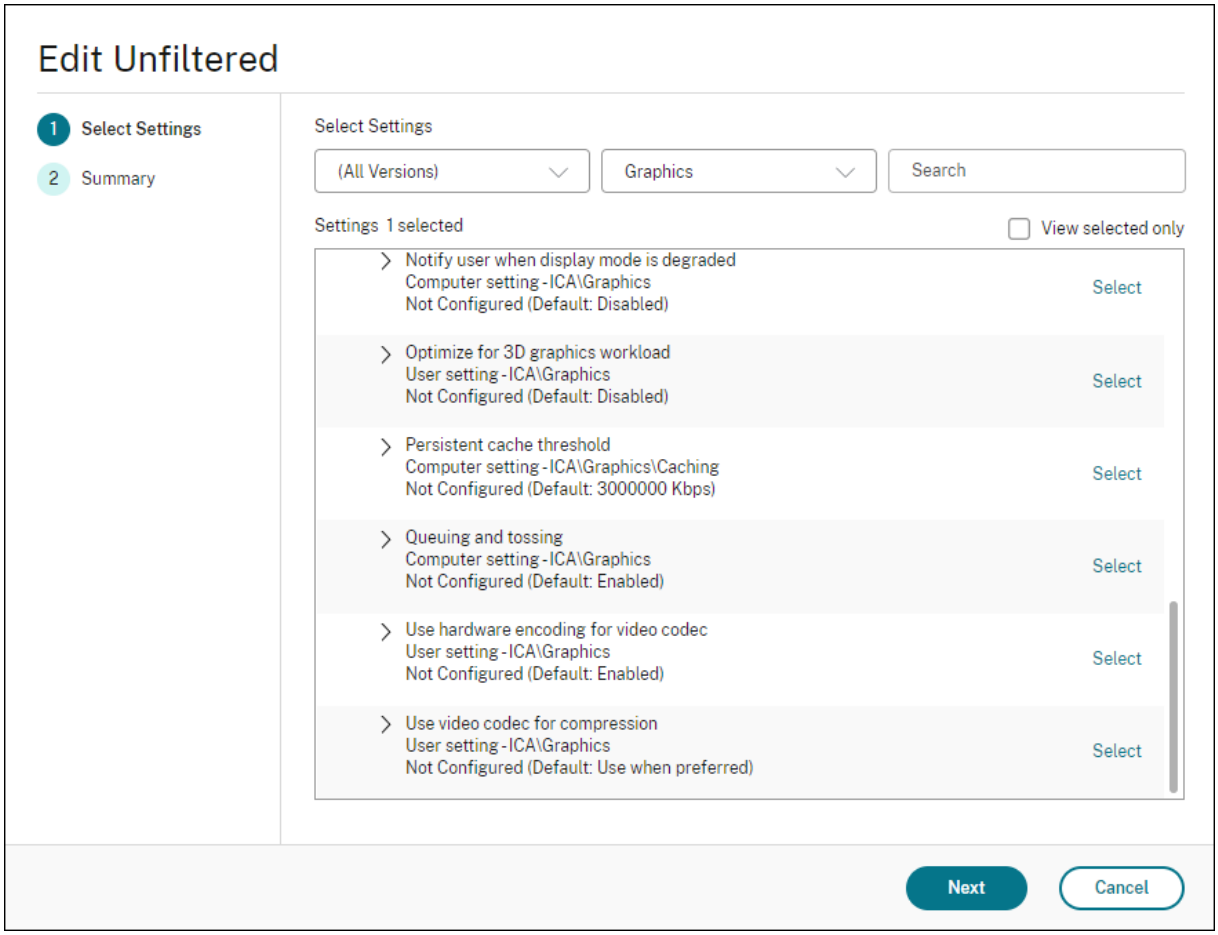
O controle remoto GDI legado usa o driver de controle remoto XPDM e não um codificador bitmap do Thinwire.

Configuração

O Thinwire é a tecnologia de exibição remota padrão.

A seguinte configuração de política de gráficos define o padrão e fornece alternativas para diferentes casos de uso:

- Use video codec for compression
  - **Use video codec when preferred**. Essa é a configuração padrão. Nenhuma configuração adicional é necessária. Manter essa 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 típicas de desktop. Isso é funcionalmente equivalente a **For actively changing regions**.
- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:
  - **For actively changing regions**. A tecnologia de exibição adaptável 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.
  - **For the entire screen**. Fornece Thinwire com tela cheia H.264 ou H.265 para otimizar a experiência do usuário e largura de banda melhoradas em casos com uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visually lossless** está desativada), a imagem final não é pixel perfeita (sem perdas) e não pode ser adequada para determinados cenários. Nesses casos, considere usar, em vez disso, H.264 Build to lossless.



Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de exibição remota. O Thinwire dá suporte a todas elas.

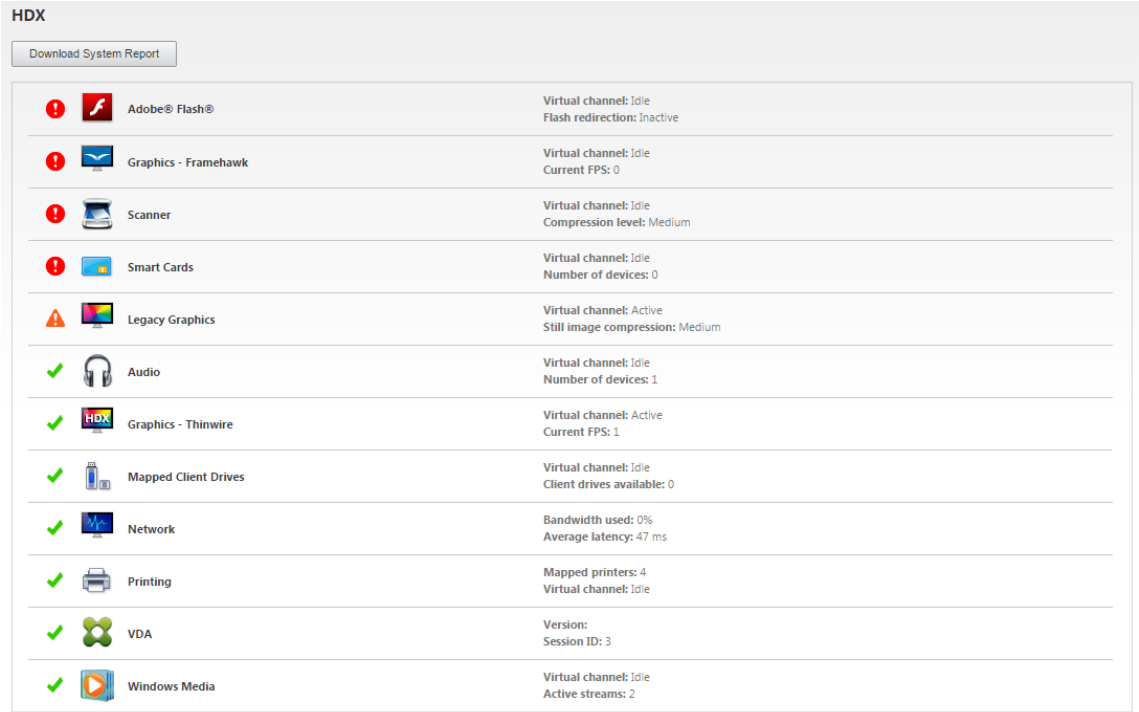
- Profundidade de cor preferida para gráficos simples
- Target frame rate
- Visual quality

Para obter as combinações recomendadas da Citrix de configurações de política para diferentes casos de uso comercial, use os Modelos de política da Citrix incorporados. Os modelos de **High Server Scalability** e **Very High Definition User Experience** usam o Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos usuários.

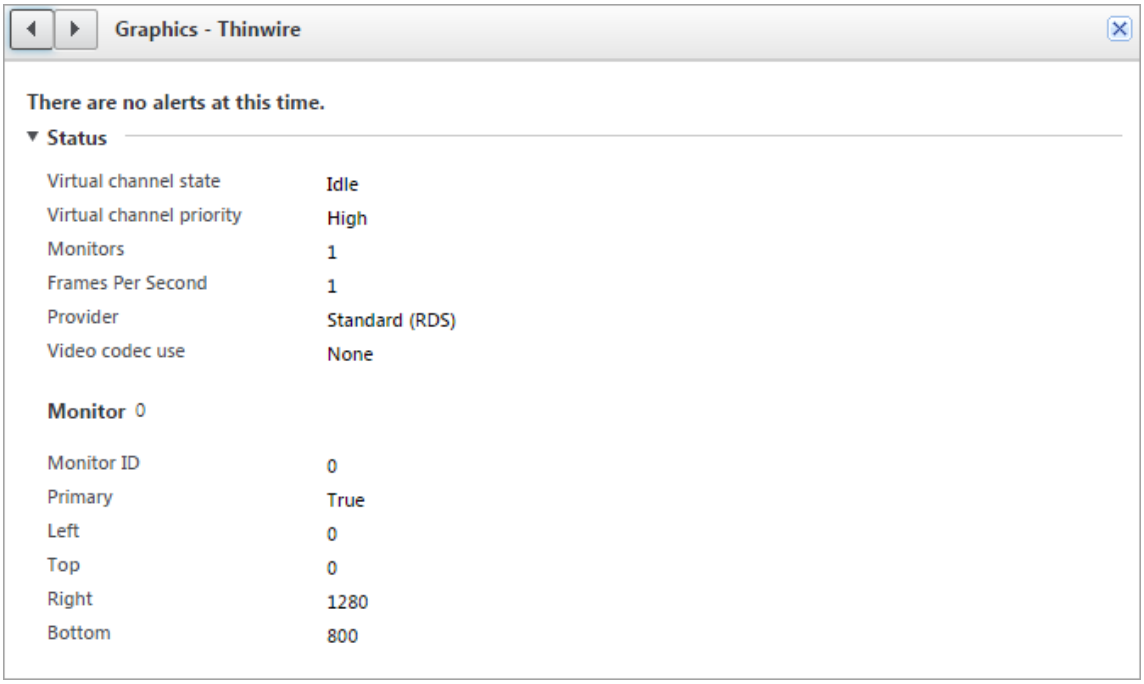
Monitoramento do Thinwire

Você pode monitorar o uso e o desempenho do Thinwire no Citrix Director. A visualização de detalhes do canal virtual HDX contém informações úteis para solução de problemas e monitoramento do Thinwire em qualquer sessão. Para exibir métricas relacionadas ao ThinWire:

1. No Director, procure um usuário, computador ou ponto de extremidade, abra uma sessão ativa e clique em **Details**. Ou você pode selecionar **Filters > Session > All Sessions**, abrir uma sessão ativa e clicar em **Details**.
2. Role para baixo até o painel **HDX**.



3. Selecione **Graphics - Thinwire**.



Codec de compressão sem perdas (MDRLE)

Em uma sessão de área de trabalho típica, a maioria das imagens é composta por gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas por meio do 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 de sessão.

No XenApp e no XenDesktop 7.17, adicionamos um codec MDRLE de taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este codec novo não afeta a escalabilidade do servidor.

Largura de banda mais baixa geralmente significa melhor interatividade de sessão (especialmente em links compartilhados ou restritos) e custos reduzidos. Por exemplo, o consumo esperado de largura de banda ao usar o codec MDRLE é aproximadamente 10 a 15% menor em comparação com o XenApp e o XenDesktop 7.15 LTSR para cargas de trabalho típicas tipo Office.

A configuração não é exigida para o codec MDRLE. Se o aplicativo Citrix Workspace oferecer suporte à decodificação MDRLE, o VDA usará a codificação VDA MDRLE e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA recorrerá automaticamente à codificação 2DRLE.

Requisitos de 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 compactação de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens fortemente compactadas têm a sua nitidez ajustada progressivamente, de forma aleatória, quando a atividade da tela for interrompida. Embora compactar e ajustar a nitidez desta 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 é desativado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada em condições de rede e flutua entre um valor mínimo e máximo pré-definido para cada configuração de **qualidade Visual**. Como não há nenhuma etapa explícita de ajuste de nitidez, o Thinwire otimiza a entrega de

imagens e mantém a eficiência do cache, proporcionando quase todos os benefícios do modo progressivo.

Alteração do comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a seguinte chave de registro: Para obter informações, consulte Progressive mode na lista de recursos gerenciados por meio do registro.

H.264 Build to lossless

Build to lossless 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 **Visual quality** como **Build to lossless**.

Build to lossless comprime a tela usando H.264 (ou H.265) durante a atividade da tela e nitidez para pixel perfeito (sem perdas) quando a atividade é interrompida. A qualidade de imagem H.264 (ou H.265) adapta-se aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de nitidez é executada gradualmente, dando uma resposta imediata se o usuário iniciar a atividade da tela logo após o início do ajuste de nitidez começar. Por exemplo, selecionando um modelo e girando-o.

H.264 **Build to lossless** oferece todas as vantagens de tela cheia H.264 ou H.265, incluindo aceleração de hardware, mas com o benefício adicional de uma tela final garantidamente sem perdas. Isso é fundamental para cargas de trabalho do tipo 3D que exigem uma imagem final com pixels perfeitos. Por exemplo, manipulação de imagens médicas. Além disso, o H.264 **Build to lossless** usa menos recursos do que a tela cheia H.264 4:4:4. Como resultado, usar **Build to lossless** geralmente resulta em uma taxa de quadros mais alta do que H.264 visualmente sem perdas 4:4:4.

> **Nota:**
>
> Além da política de **Visual quality**, defina a política **Use video codec** como **Use when preferred** (padrão) ou **For actively changing regions**. Você pode reverter para não H.264 Build to lossless definindo a política **Use video codec** como **Do not use video codec**. Isso resulta em imagens em movimento codificadas com JPEG em vez de H.264 (ou H.265).

Marca d'água de sessão baseada em texto

June 24, 2022

As marcas d'água de sessão baseadas em texto ajudam a deter e ativar o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um estorvo 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 exibida em toda a tela de sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte a 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 possibilita algum nível de dissuasão e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar esse recurso, recomendamos que você combine esse recurso com outras soluções de segurança, conforme aplicável.

A marca d'água da sessão é texto e é aplicada à sessão fornecida 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 de forma mais eficaz, inclua outras informações, como endereço de protocolo de internet do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as Configurações da 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 da sessão não têm suporte em sessões em que o acesso ao aplicativo local, o redirecionamento de mídia do Windows, o MediaStream, o redirecionamento de conteúdo do navegador e o redirecionamento de vídeo HTML5 são usados. Para usar a marca d'água da sessão, verifique se esses recursos estão desativados.
- A marca d'água da sessão não é suportada e não aparece se a sessão estiver sendo executada em modos acelerados por hardware de tela cheia (codificação H.264 ou H.265 em tela cheia).
- Se você definir essas políticas de HDX, as configurações de marca d'água não terão efeito e não será exibida nenhuma marca d'água na exibição da sessão.

Use hardware encoding for video codec como **Enabled**
Use video codec for compression como **For the entire screen**

- Se você definir essas políticas de HDX, o comportamento é indeterminado e a marca d'água não poderá ser exibida.

  Use hardware encoding for video codec como **Enabled**
  Use video codec for compression como **Use video codec when preferred**

  Para garantir que a marca d'água seja exibida, defina **Use hardware encoding for video codec** como **Disabled**, ou defina **Use video codec for compression** como **For actively changing regions** ou **Do not use video codec**.

- A marca d'água da sessão dá suporte apenas ao modo gráfico do Thinwire.
- Se você usar Session Recording, 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 VDA não inclui as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

Multimídia

July 1, 2022

A pilha de tecnologia HDX suporta a entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia de renderização do lado do servidor
- Redirecionamento de multimídia de renderização do lado do cliente

Esta estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, ao mesmo tempo em que maximiza a escalabilidade do servidor para reduzir o custo por usuário.

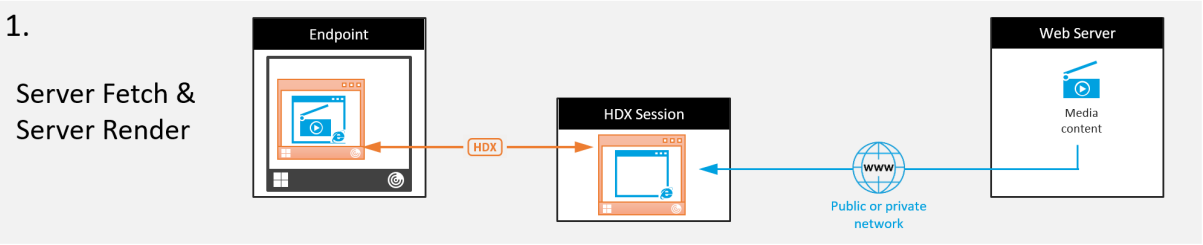
Com a entrega de multimídia renderizada pelo servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops) pelo aplicativo. O conteúdo é comprimido e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo é de computação intensiva, a entrega de multimídia renderizada pelo servidor se beneficia imensamente da aceleração de hardware integrada. Por exemplo, o suporte ao DirectX Video Acceleration (DXVA) libera a CPU executando a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

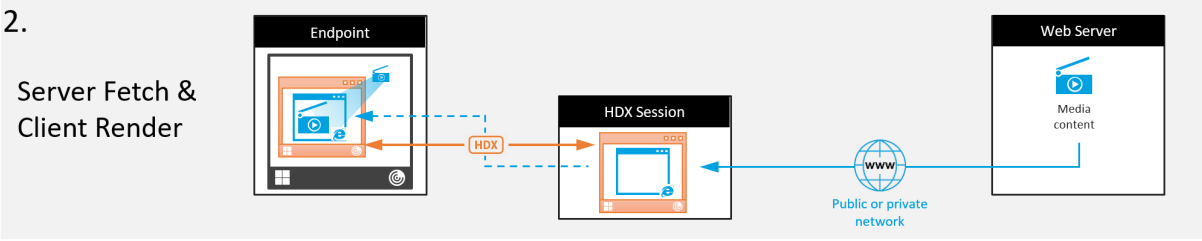
Como a maioria dos servidores não oferece nenhuma aceleração de hardware para compressão de vídeo, a escalabilidade do servidor é afetada negativamente se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter a alta escalabilidade do servidor redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

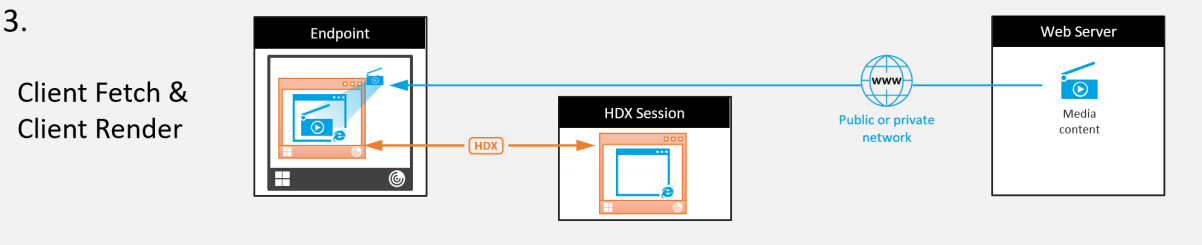
- O redirecionamento do Windows Media livra o servidor de uma grande variedade de formatos de mídia normalmente associados ao Windows Media Player.
- O vídeo HTML5 se popularizou e a Citrix introduziu uma tecnologia de redirecionamento para esse tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento de contato, Redirecionamento de 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 do lado do servidor.
Se você configurar o redirecionamento, o HDX usará Obtenção de servidor e Renderização de cliente ou Obtenção de cliente e Renderização de cliente. Se esses métodos falharem, o HDX volta à Renderização do lado do servidor conforme necessário e está sujeito à Política de Prevenção de Fallback.

Exemplos de cenários







Cenário 1. (Obtenção de servidor e Renderização de servidor):

1. O servidor obtém o arquivo de mídia de sua origem, decodifica-o e apresenta o conteúdo para 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 comprime e, em seguida, o transmite para o cliente.

Essa abordagem incorre em um alto custo de CPU, um alto custo de largura de banda (se a imagem/-som extraídos não forem comprimidos de forma eficiente) e tem baixa escalabilidade de servidor.

Os canais virtuais Thinwire e Audio lidam com essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para clientes. Usando essa abordagem, a decodificação acontece no servidor e funciona para uma maior variedade de dispositivos e formatos.

Cenário 2. (Obtenção de servidor e Renderização de cliente):

Esta abordagem depende de sua 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 comprimido é enviado ao cliente, onde é decodificado e apresentado localmente. A vantagem dessa abordagem é que ele é descarregado para os dispositivos cliente, economizando ciclos da CPU no servidor.

No entanto, isso também introduz alguns requisitos adicionais de hardware e software para o cliente. O cliente deve ser capaz de decodificar cada formato que possa vir a receber.

Cenário 3. (Obtenção de cliente e Renderização de cliente):

Esta abordagem depende de sua capacidade de interceptar a URL de conteúdo de mídia antes que ela seja obtida da origem. A URL é enviada para o cliente de onde o conteúdo de mídia é obtido, decodificado e apresentado localmente. Essa abordagem é conceitualmente simples. Sua vantagem é que ela economiza ciclos da CPU no servidor e largura de banda porque o servidor envia somente comandos de controle. No entanto, o conteúdo de mídia nem sempre é acessível aos clientes.

Estrutura e plataforma:

Os 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 da mídia em várias etapas e usa uma arquitetura baseada em pipeline.

Estrutura	Plataforma
DirectShow	Windows (98 e posterior)
Media Foundation	Windows (Vista e posterior)

Estrutura	Plataforma
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
	Windows Media redirection	Sim

Recursos de áudio

November 9, 2023

Você pode configurar e adicionar as seguintes configurações de política Citrix a uma política que otimiza os recursos de áudio HDX. Para obter detalhes de uso, além de relacionamentos e dependências com outras configurações de política, consulte Configurações de políticas de áudio, Configurações de política de largura de banda e Configurações de políticas de conexões multi-stream.

> **Importante:**
>
> Recomendamos fornecer áudio por meio de User Datagram Protocol (UDP) em vez de TCP. Somente o Windows Virtual Delivery Agent (VDA) dá suporte a áudio por UDP.
>
> A criptografia de áudio UDP usando DTLS está disponível somente 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 aplicativo VDA para o Citrix Workspace.

Qualidade de áudio

Em geral, maior qualidade de som consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para dispositivos do usuário. A compactação de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações de política Citrix para configurar os níveis de compactação que devem ser aplicados aos arquivos de som.

Como padrão, a configuração de **política de qualidade de áudio** é definida como Áudio de alta definição quando o transporte TCP é usado. A política é definida como Medium - otimizado para fala quando é usado o transporte UDP (recomendado). 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 essa qualidade de áudio para aplicativos de chat por voz ou chat por vídeo não otimizados (como softphones). A razão disso é que ele pode introduzir latência no caminho de áudio, o que não é adequado para comunicações em tempo real. Recomendamos a configuração otimizada para política de 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 dial-up, se a qualidade de áudio for reduzida para **Baixa**, é consumida a menor largura de banda possível. Nessa 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 prejudicados.

Para obter detalhes de configuração, consulte Configurações de política de áudio. Lembre-se de ativar 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 (recomendada 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
- Baixa qualidade

- 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

Client audio redirection

Para permitir que os usuários recebam áudio de um aplicativo em um servidor por meio de alto-falantes ou outros dispositivos de som no dispositivo do usuário, deixe a configuração de **Client audio redirection** em **Allowed**. Esse é o padrão.

O mapeamento de áudio do cliente coloca 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 de configuração, consulte Configurações de política de áudio. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Client microphone redirection

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Enabled** no valor padrão (Allowed).

Por segurança, os dispositivos do usuário alertam seus usuários quando os servidores em que eles não confiam tentam acessar os microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar esse alerta no aplicativo Citrix Workspace.

Para obter detalhes de configuração, consulte Configurações de política de áudio. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Audio Plug N Play

A configuração de política Áudio Plug and Play permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração é **Enabled** por padrão. O Áudio Plug and Play permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até que a sessão do usuário tenha começado.

Essa configuração se aplica apenas aos computadores do sistema operacional Windows multi-ssessão.

Para obter detalhes de configuração, consulte Configurações de política de áudio.

Limite de largura de banda de redirecionamento de áudio e percentual de limite de largura de banda de redirecionamento

A configuração de política de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para uma reprodução e gravação de áudio em uma sessão.

A configuração de 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 disponível total.

Por padrão, é especificado zero (sem máximo) para as duas configurações. Se os dois ajustes estiverem configurados, aquele com o limite mais baixo da largura de banda será usado.

Para obter detalhes sobre a configuração, consulte Configurações da política de largura de banda. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Transporte de áudio em tempo real por UDP e faixa de portas UDP de áudio

Por padrão, o transporte de áudio por User Datagram Protocol (UDP) em tempo real é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam transporte de áudio em tempo real por UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar o UDP/RTP para áudio para garantir a melhor experiência possível do usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio por UDP tem preferência em relação a EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que não seja adiciona nenhuma latência 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 os recursos do Citrix Virtual Apps and Desktops, o tráfego de áudio entre o dispositivo de ponto de extremidade e o Citrix Gateway será protegido por meio do protocolo DTLS.

A faixa de porta UDP de áudio especifica o intervalo de números de porta que o Windows VDA usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é 16500 a 16509.

Para obter detalhes sobre o transporte em tempo real de áudio sobre UDP, consulte Configurações da política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações da política de conexões multi-stream. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

O áudio sobre UDP requer o Windows VDA. Para obter políticas com suporte no Linux VDA, consulte Lista de suporte de políticas.

Políticas de configuração de áudio para dispositivos do usuário

1. Carregue os modelos de diretiva de grupo seguindo a configuração de Group Policy Object administrative template.
2. No Editor de Política de Grupo, expanda **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. Para **Client audio settings**, selecione **Not Configured**, **Enabled** ou **Disabled**.
   - **Not Configured**. Por padrão, o redirecionamento de áudio é ativado com áudio de alta qualidade ou as configurações de áudio personalizadas previamente configuradas.
   - **Enabled**. Ativa o redirecionamento de áudio com as opções selecionadas.
   - **Disabled**. Desativa o redirecionamento de áudio.
4. Se você selecionar **Ativado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Enable Real-Time Transport** e defina o intervalo de portas de entrada para abrir no firewall local do Windows.
6. Para usar o áudio UDP com o Citrix Gateway, selecione **Permitir transporte em tempo real através do gateway**. Configure o Citrix Gateway com DTLS. Para obter mais informações, consulte este artigo.

Como administrador, se você não tiver controle sobre dispositivos de ponto de extremidade para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o áudio UDP. Por exemplo, para trazer seus próprios dispositivos ou computadores domésticos.

1. No computador com StoreFront, abra C:\inetpub\wwwroot\Citrix\<nome do armazenamento>\App_Data\default.ica com um editor como o bloco de notas.
2. Faça as seguintes entradas na seção [Application].

   ; This text enables Real-Time Transport

   EnableRtpAudio=true

   ; This text allows Real-Time Transport Through gateway

   EnableUDPThroughGateway=true

   ; This text sets audio quality to Medium

   AudioBandwidthLimit=1

   ; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

Se você ativar o áudio UDP (User Datagram Protocol) editando default.ica, o áudio UDP estará ativado para todos os usuários que estão usando esse armazenamento.

Evitar eco durante conferências multimídia

Os usuários em conferências de áudio ou vídeo podem ouvir um eco. Geralmente ocorrem ecos quando há alto-falantes e microfones muito próximos uns dos outros. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX fornece uma opção de cancelamento de eco (ativada por padrão) que minimiza o eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Verifique se os dispositivos não estão muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração de registro para desativar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados pelo registro.

Softphones

Um softphone é um software que atua como uma interface de telefone. O softphone pode ser usado para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Com um softphone, você pode discar números de telefone e realizar outras funções telefônicas usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para usar softphones.

- **Control mode**. O softphone hospedado controla um telefone físico. Nesse modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.
- **HDX RealTime optimized softphone support (recommended)**. O mecanismo de mídia é executado no dispositivo do usuário e o tráfego do protocolo Voice over Internet flui ponto a ponto. Para ver exemplos, consulte:
  - HDX Optimization for Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone for VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin Zoom VDI
  - Genesys PureEngage Cloud

  - Dispositivo de ditado Nuance Dragon PowerMic

- **Local App Access**. Um recurso do Citrix Virtual Apps and Desktops e do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que permite que um aplicativo como um softphone seja executado localmente no dispositivo do usuário Windows, mas parece perfeitamente integrado à área de trabalho virtual/publicada. Este recurso passa todo o processamento de áudio para o dispositivo do usuário. Para obter mais informações, consulte Acesso ao aplicativo local e redirecionamento de URL.
- **HDX RealTime generic softphone support.** Protocolo VoIP por ICA.

Suporte softphone genérico

O suporte genérico de softphone permite que você hospede um softphone não modificado no XenApp ou no XenDesktop no data center. O tráfego de áudio passa pelo protocolo Citrix ICA (de preferência usando UDP/RTP) para o dispositivo do usuário que executa o aplicativo Citrix Workspace.

O suporte genérico de softphone é um recurso do HDX RealTime. Esta abordagem para a funcionamento do softphone é especialmente útil quando:

- Não há nenhuma solução otimizada disponível para o funcionamento do softphone e o usuário não está usando um dispositivo Windows onde pode ser usado o acesso ao aplicativo local.
- O mecanismo de mídia que é necessário para o funcionamento otimizado 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 Generic HDX RealTime fornece uma valiosa solução de fallback.

Há duas considerações sobre o funcionamento do softphone por meio do Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é fornecido ao ambiente de trabalho virtual/publicado.
- Como o áudio é fornecido de e para o fone de ouvido do usuário, microfone e alto-falantes ou telefone USB.

O Citrix Virtual Apps and Desktops inclui inúmeras tecnologias para oferecer suporte à entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida da eficiência de áudio e largura de banda em tempo real.
- 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 de WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voice over Internet Protocol. O aplicativo Citrix Workspace para Windows oferece os seguintes recursos:

- Buffer de jitter do lado do cliente - Garante áudio sem interrupções, mesmo quando a latência da rede flutua.
- Cancelamento de eco - Permite uma maior variação na distância entre microfone e alto-falantes para colaboradores que não usam um fone de ouvido.
- Áudio Plug and Play - Os dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.
- Roteamento de dispositivos de áudio - Os usuários podem direcionar o toque para alto-falantes, mas o caminho de voz para o fone de ouvido.
- Multi-stream ICA - Permite a qualidade flexível de roteamento baseado em serviço pela rede.
- O ICA é compatível com quatro fluxos TCP e dois UDP. Um dos fluxos UDP dá suporte ao áudio em tempo real via RTP.

Para obter um resumo dos recursos do aplicativo Citrix Workspace, consulte Citrix Receiver Feature Matrix.

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 com cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac oferecem suporte ao Voice over Internet Protocol. Além disso, o Dell Wyse oferece suporte a Protocolo de Voz via 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 consomem grandes quantidades de dados. A configuração de duas CPUs virtuais reduz a latência de switching de thread. Portanto, recomendamos que você configure duas vCPUs em um ambiente Citrix Virtual Desktops VDI.

Ter duas CPUs virtuais não significa necessariamente duplicar o número de CPUs físicas, porque as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de confiabilidade de sessão, também aumenta o consumo da CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo da CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor potente.

Áudio UDP:
O áudio por UDP fornece excelente tolerância ao congestionamento de rede e perda de pacotes. Recomendamos esse protocolo em vez de TCP quando disponível.

Configuração LAN/WAN:
A configuração adequada da rede é crítica para uma boa qualidade de áudio em tempo real. Tipicamente, você deve configurar LANs virtuais (VLANs) porque os pacotes de broadcast excessivos podem introduzir jitter. Os dispositivos habilitados para IPv6 podem gerar muitos pacotes de transmissão. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configurar para oferecer suporte à Qualidade de Serviço.

Configurações para usar conexões WAN:
Você pode usar o chat de voz através de conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se fornecer softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler SD-WAN entre o data center e o escritório remoto. Com isso, mantém-se uma alta qualidade de serviço. O NetScaler SD-WAN suporta ICA de fluxo múltiplo, incluindo UDP. Além disso, no caso de 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 remotas de usuários:
o Citrix Gateway oferece suporte ao DTLS para fornecer tráfego UDP/RTP de forma nativa (sem encapsulamento no TCP).
Abra firewalls bidirecionalmente para tráfego UDP pela 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 **otimizada para fala**, também conhecida como áudio de qualidade média. Entre a plataforma VDA e o IP-PBX, o softphone usa qualquer codec configurado ou negociado. Por exemplo:

- O G711 fornece boa qualidade de voz, mas tem uma exigência de largura de banda de 80 kilobits por segundo através de 100 kilobits por segundo por chamada (dependendo dos overheads da Network Layer2).
- G729 fornece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo através de 40 kilobits por segundo por chamada (dependendo dos overheads da Network Layer2).

Fornecer aplicativos de softphone para o ambiente de trabalho virtual

Existem dois métodos pelos quais você pode fornecer um softphone para a área de trabalho virtual XenDesktop:

- O aplicativo pode ser instalado na imagem da área de trabalho virtual.
- O aplicativo pode ser transmitido para a área de trabalho virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciabilidade porque a imagem da área de trabalho virtual é mantida organizada. Depois de ser transmitido para a área de trabalho virtual, o aplicativo é

executado nesse ambiente como se estivesse instalado da maneira usual. Nem todos os aplicativos são compatíveis com App-V.

Fornecimento de áudio de e para o dispositivo do usuário

Generic HDX RealTime dá suporte aos métodos de fornecimento de áudio de e para o dispositivo do usuário:

- **Canal virtual de áudio Citrix**. Geralmente, recomendamos o cana virtual de áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB genérico**. Dá suporte a dispositivos de áudio com botões ou tela (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou LAN com o servidor Citrix Virtual Apps and Desktops.

Canal virtual de áudio Citrix

O canal virtual de áudio Citrix (CTXCAM) bidirecional permite que o áudio seja fornecido de forma eficiente pela rede. O Generic HDX RealTime recebe o áudio do fone de ouvido ou microfone do usuário e o compacta. Em seguida, envia-o por ICA para o aplicativo softphone na área de trabalho virtual. Da mesma forma, a saída de áudio do softphone é compactada e enviada na outra direção para o fone de ouvido ou alto-falantes do usuário. Esta compactação é independente da compactação usada pelo próprio softphone (como G.729 ou G.711). Ela é feita por meio do codec otimizado para fala (qualidade média). Suas características são ideais para Voice over Internet Protocol. Apresenta tempo de codificação rápido e consome apenas aproximadamente 56 quilobits por segundo de largura de banda de rede (28 Kbps em cada direção), pico. Esse codec deve ser explicitamente selecionado no console Manage do serviço porque não é o codec de áudio padrão. O padrão é o codec de áudio HD (alta qualidade). Esse 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 (canal virtual CTXGUSB) da Citrix fornece um meio genérico de dispositivos USB remotos, incluindo dispositivos compostos (áudio e HID) e dispositivos USB isócronos. Essa abordagem é limitada aos usuários conectados a uma LAN. Por esse motivo o protocolo USB tende a ser sensível à latência da rede e requer largura de banda de rede considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones. Esse redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o canal de áudio virtual Citrix tem preferência 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 conectado via LAN ao data center. Nesse caso, o Redirecionamento USB Genérico suporta botões no conjunto de telefone ou fone de ouvido que controlam recursos enviando um sinal de volta para o softphone. Não há um problema com botões que funcionam localmente no dispositivo.

Limitação

Depois de instalar um dispositivo de áudio em seu cliente, ativar o redirecionamento de áudio e iniciar uma sessão do RDS, os arquivos de áudio podem não reproduzir o áudio. Como solução alternativa, adicione esta chave de registro no computador RDS e reinicie a máquina: Para obter informações, consulte Audio limitation na lista de recursos gerenciados por meio do registro.

Redirecionamento de conteúdo do navegador

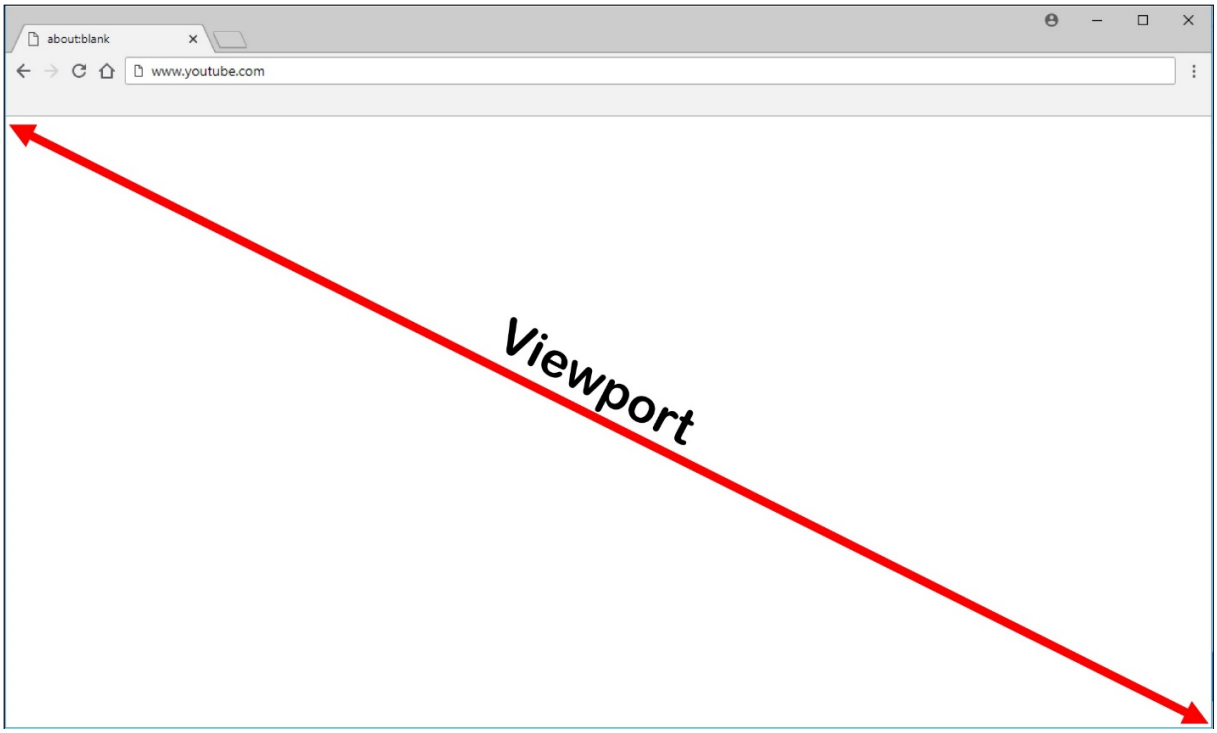
July 1, 2022

O redirecionamento de conteúdo do navegador impede a renderização de páginas da Web na lista de permissão no lado VDA. Esse recurso usa o aplicativo Citrix Workspace para instanciar um mecanismo de renderização correspondente no lado do cliente, que busca o conteúdo HTTP e HTTPS da URL.

> **Nota:**
>
> Você pode especificar que as páginas da Web sejam reorientadas ao lado VDA (e não reorientadas no lado do cliente) usando uma lista de blocos.

Esse mecanismo de layout da Web de sobreposição é executado no dispositivo de ponto de extremidade em vez de no VDA e usa o ponto de extremidade CPU, GPU, RAM e rede.

Somente o visor do navegador é redirecionado. O visor é a área retangular do seu navegador onde o conteúdo é exibido. O visor não inclui coisas como a Barra de Endereços, Barra de Ferramentas Favoritos, Barra de Status. Esses itens estão na interface do usuário, que ainda estão sendo executados no navegador no VDA.

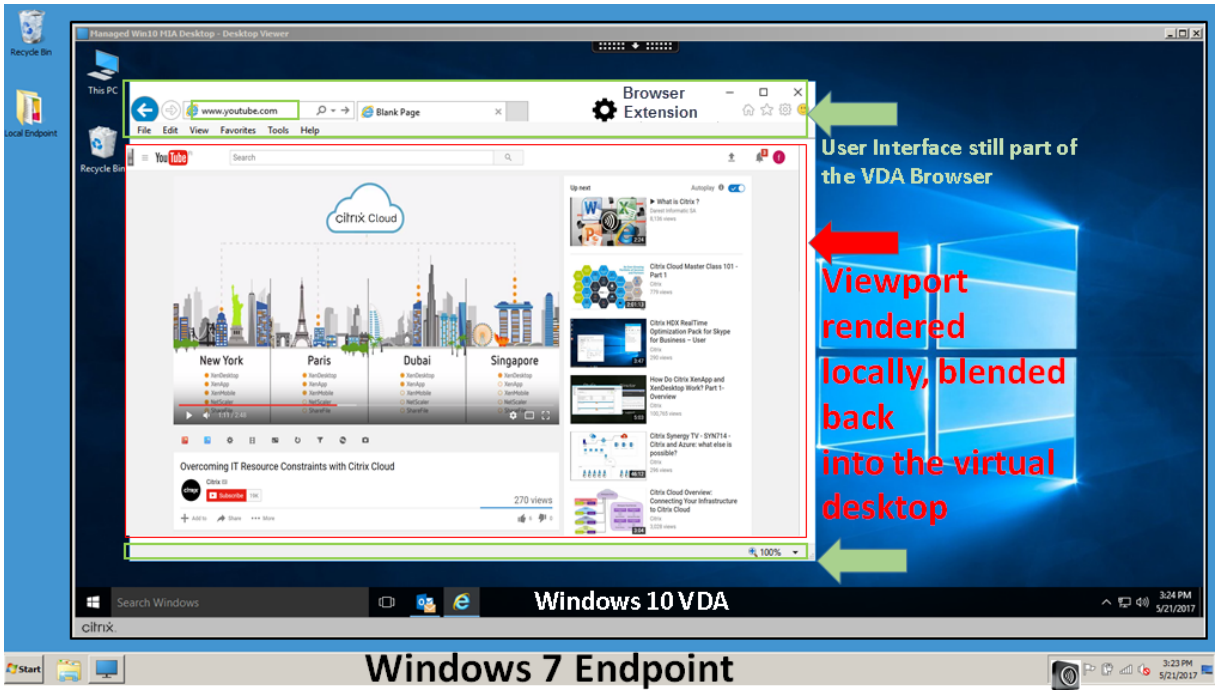


1. Configure uma política na interface Manage > Full Configuration que especifica a Lista de Controle de Acesso que contém as URLs para redirecionamento das listas de permissão ou bloqueio. Para que o navegador no VDA detecte que a URL para a qual o usuário está navegando corresponde à lista de permissões ou não corresponde a uma lista de bloqueios, uma extensão do navegador executa a comparação. A extensão do navegador (BHO) para o Internet Explorer 11 está incluída na mídia de instalação e é instalada automaticamente. No caso do Chrome, a extensão do navegador está disponível na Chrome Web Store e você pode implantá-la usando as Políticas de Grupo e os arquivos ADMX. As extensões do Chrome são instaladas por usuário. Não é necessário atualizar uma imagem dourada para adicionar ou remover uma extensão.
2. Se for encontrada uma correspondência na lista de permissão (por exemplo, `https://www.mycompany.com/`) e não houver correspondência com uma URL na lista de bloqueio (por exemplo, `https://www.mycompany.com/engineering`), um canal virtual (CTXCSB) instrui o aplicativo Citrix Workspace que é necessário um redirecionamento e retransmite o URL. O aplicativo Citrix Workspace instancia um mecanismo de renderização local e exibe o site.
3. O aplicativo Citrix Workspace combina o site com a área de conteúdo do navegador de desktop virtual sem interrupções.

A cor do logotipo especifica o status da extensão do Chrome. A cor será uma destas três:

- Verde: ativo e conectado.
- Cinza: não ativo/ocioso na guia atual.
- Vermelho: interrompido/não está funcionando.

Você pode depurar o log usando **Options** no menu de extensões.



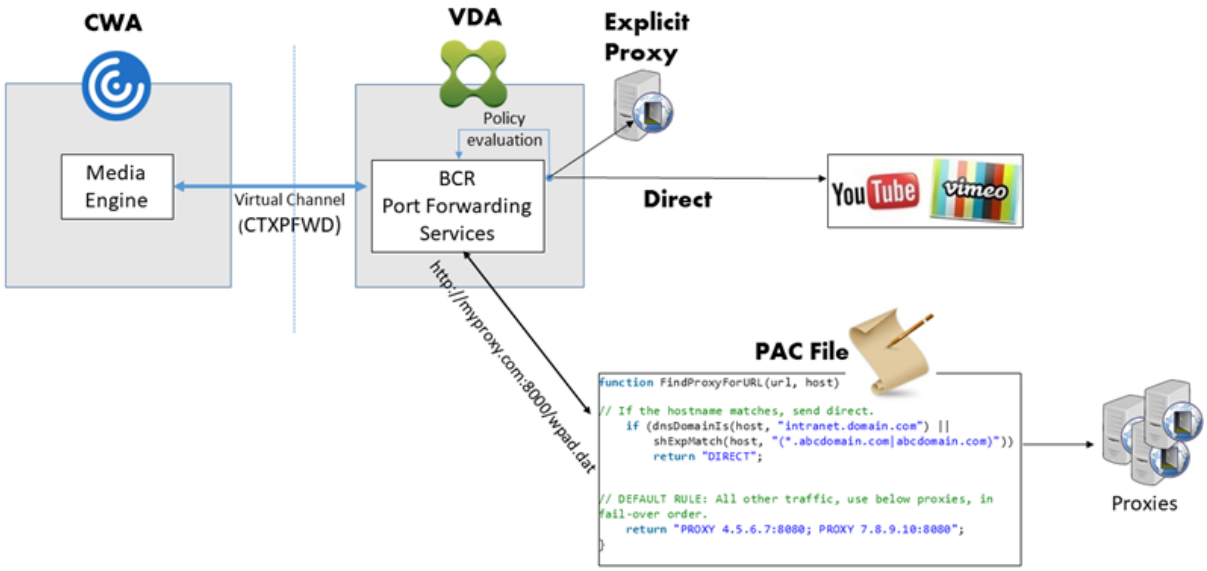
Esses são cenários de como o aplicativo Citrix Workspace busca conteúdo:

- **Obtenção no servidor e renderização no servidor**: não há redirecionamento porque você não adicionou o site à lista de permissões ou o redirecionamento foi malsucedido. Recorremos à renderização da página da Web no VDA e usamos o Thinwire para tornar os gráficos remotos. Use políticas para controlar o comportamento de fallback. Alto consumo de CPU, RAM e largura de banda no VDA.
- **Obtenção no servidor e renderização no cliente**: o aplicativo Citrix Workspace contata e busca conteúdo do servidor web por meio do VDA usando um canal virtual (CTXPFWD). Essa opção é útil quando o cliente não tem acesso à internet (por exemplo, clientes finos). 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.

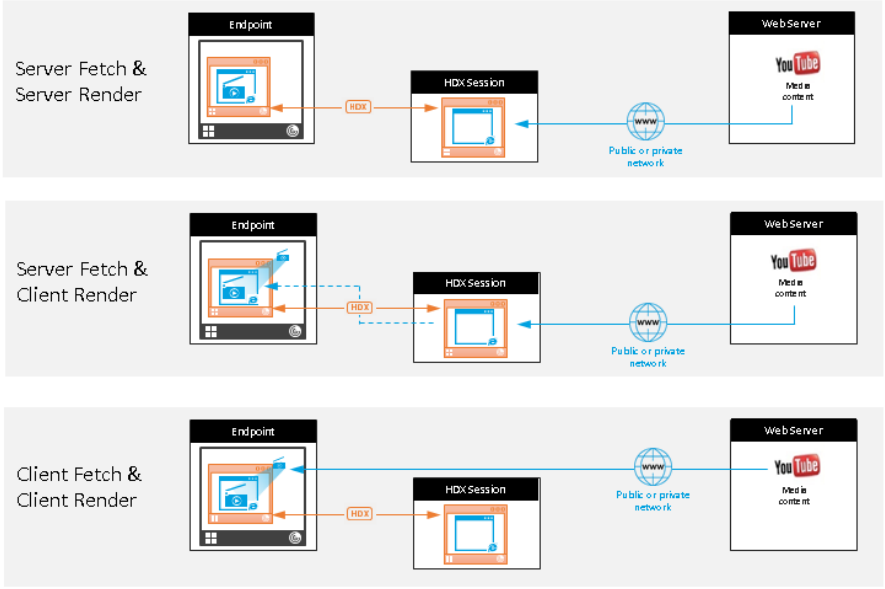
  Qual opção de política escolher:

  - Proxy explícito - Se você tiver um único proxy explícito no Datacenter.
  - Direto ou transparente - Se você não tiver proxies ou se você usar proxies transparentes.
  - Arquivos PAC - Se você depender de arquivos PAC para que os navegadores no VDA possam escolher automaticamente o servidor proxy apropriado para buscar um URL especificado.



- **Busca do cliente e renderização do cliente**: como o aplicativo Citrix Workspace entra em contato diretamente com o servidor da Web, ele requer acesso à internet. Esse cenário isenta todo o uso de rede, CPU e RAM do site XenApp e XenDesktop.

Redirection scenarios



Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

Mecanismo 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 poderá voltar ao VDA. Nesses casos, o

navegador no VDA pode recarregar e renderizar a página no servidor.

Você pode suprimir a renderização do servidor de elementos de vídeo usando a política existente de **prevenção de fallback de mídia do Windows**. Defina esta política para **Reproduzir todo o conteúdo somente no cliente** ou **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Essas configurações bloqueiam a reprodução de elementos de vídeo 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 **Lista de Controle de Acesso** contém a URL que oferece fallback. O URL não pode estar na política de lista de bloqueios.

Requisitos do sistema:

Pontos de extremidade Windows:

- Windows 10 ou 11
- Aplicativo Citrix Workspace 1809 para Windows ou posterior

> **Nota:**
>
> O redirecionamento de conteúdo do navegador é suportado apenas na versão atual (CR) do aplicativo Citrix Workspace para Windows, mas não nas versões LTSR 1912 e 2203.1 do aplicativo Citrix Workspace.

Pontos de extremidade Linux:

- Aplicativo Citrix Workspace 1808 para Linux ou posterior
- Citrix Receiver para Linux 13.9 ou posterior
- Os terminais clientes finos devem incluir WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 e XenApp e XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- Sistema operacional VDA: Windows 10 (versão mínima 1607), Windows Server 2012 R2, Windows Server 2016
- Navegador no VDA:
  - Google Chrome v66 ou superior (o Chrome requer o aplicativo Citrix Workspace 1809 para Windows no ponto de extremidade do usuário, Citrix Virtual Apps and Desktops 7 1808 VDA e a extensão de redirecionamento de conteúdo do navegador)
  - Internet Explorer 11 e configurar estas opções:
    - Limpe o **Enhanced Protected Mode** em: **Internet Options** > **Advanced > Security**
    - Assinale **Enable third-party browser extensions** em: **Internet Options > Advanced > Browsing**

Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo do Knowledge Center https://support.citrix.com/article/CTX230052

Extensão de redirecionamento de conteúdo do navegador Chrome

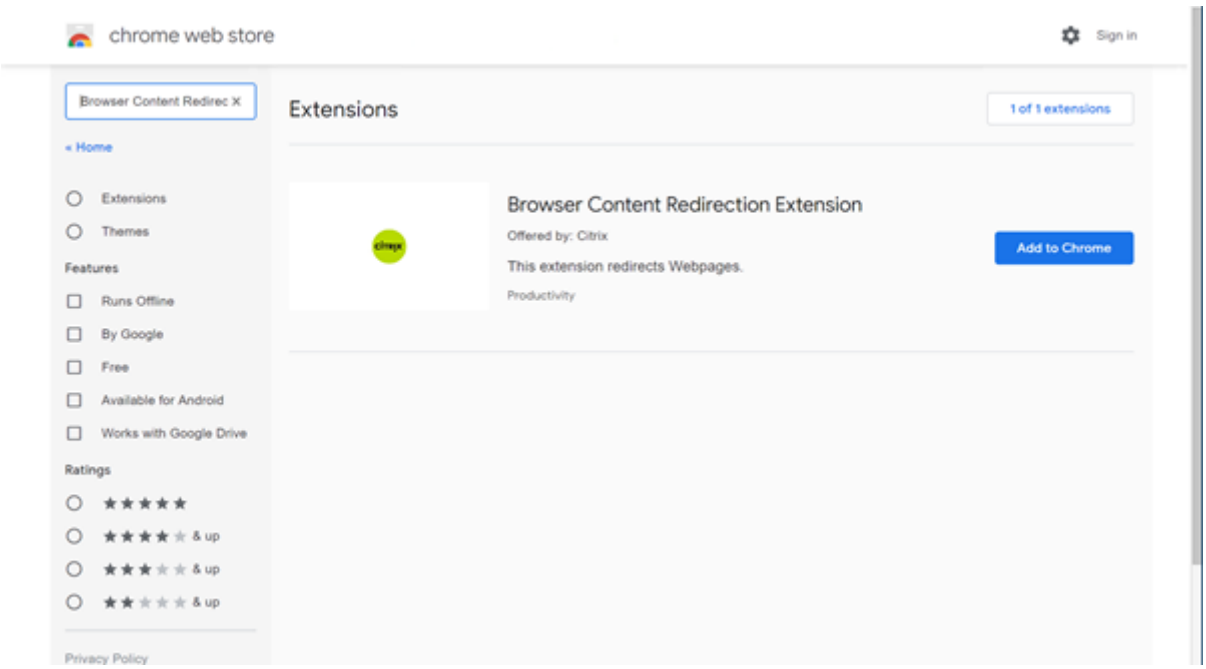
Para usar o redirecionamento de conteúdo do navegador com o Chrome, adicione a extensão de redirecionamento de conteúdo do navegador na Chrome Web Store. Clique em **Add to Chrome** no ambiente do Citrix Virtual Apps and Desktops.

A extensão **não** é necessária na máquina cliente do usuário —somente no VDA.

Requisitos do sistema

- Chrome v66 ou superior
- Extensão de redirecionamento de conteúdo do navegador
- Citrix Virtual Apps and Desktops 7 1808 ou superior
- Aplicativo Citrix Workspace 1809 para Windows ou superior

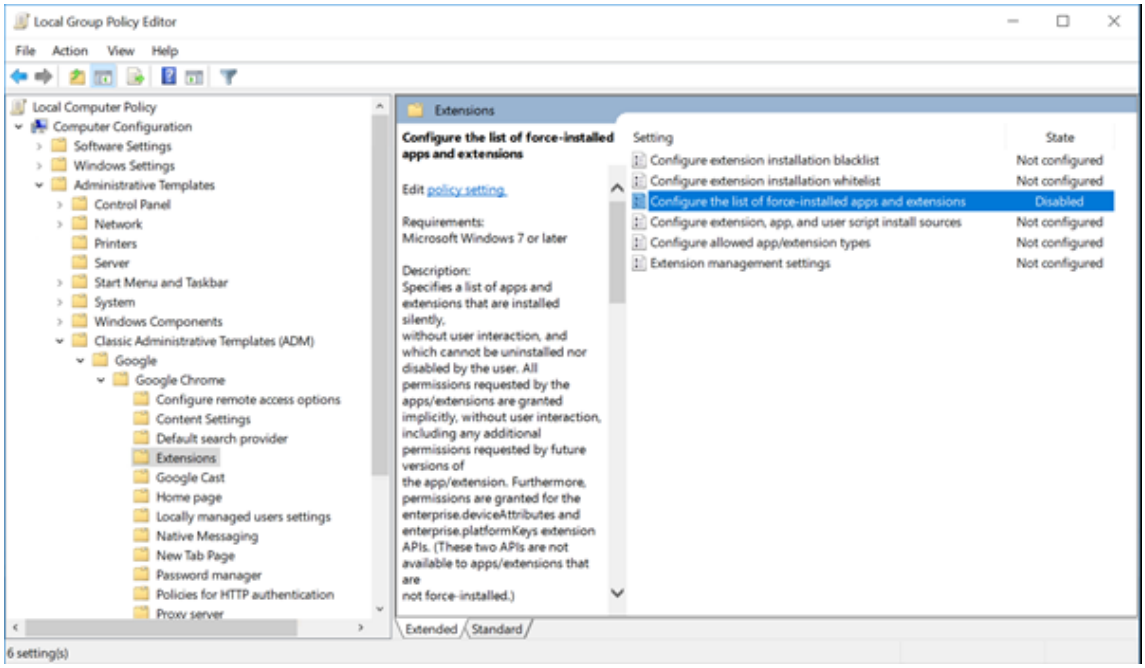
> **Nota:**
>
> O redirecionamento de conteúdo do navegador é suportado apenas na versão atual (CR) do aplicativo Citrix Workspace para Windows, mas não nas versões LTSR 1912 e 2203.1 do aplicativo Citrix Workspace.



Este método funciona para usuários individualmente. Para implantar a extensão em um grande grupo de usuários em sua organização, implante a extensão usando a Política de Grupo.

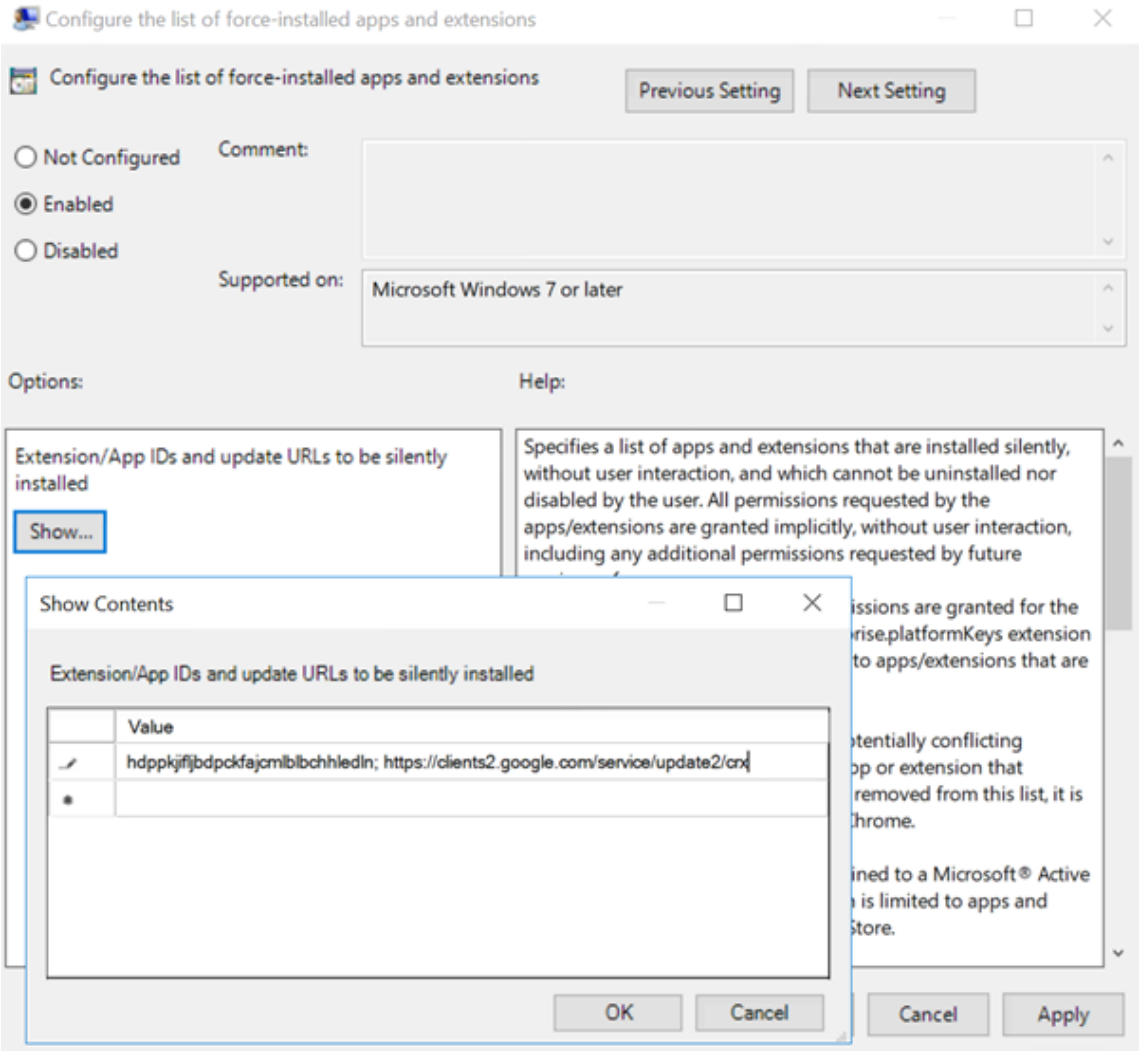
Implantar a extensão usando a Política de Grupo

1. Importe os arquivos do Google Chrome ADMX para o seu ambiente. Para obter informações sobre como baixar modelos de política e instalar e configurar os modelos no Editor de Política de Grupo, consulte Definir políticas do navegador Chrome em PCs gerenciados.
2. Abra o console de Gerenciamento de Diretiva de Grupo e vá para **User Configuration \ Administrative Templates\Classic Administrative Templates (ADM) \ Google\ Google Chrome \ Extensions**. Ative a configuração **Configure the list of force-installed apps and extensions**.



3. Clique em **Show** e digite a seguinte string, que corresponde ao ID da extensão. Atualize o URL para a extensão de redirecionamento de conteúdo do navegador.

   `hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx`



4. Aplique a configuração e depois de uma atualização do **gpupdate**, o usuário recebe automaticamente a extensão. Se você iniciar o navegador Chrome na sessão do usuário, a extensão já será aplicada e não poderá ser removida.

   Todas as atualizações da extensão são instaladas automaticamente nos computadores dos usuários por meio do URL de atualização especificado na configuração.

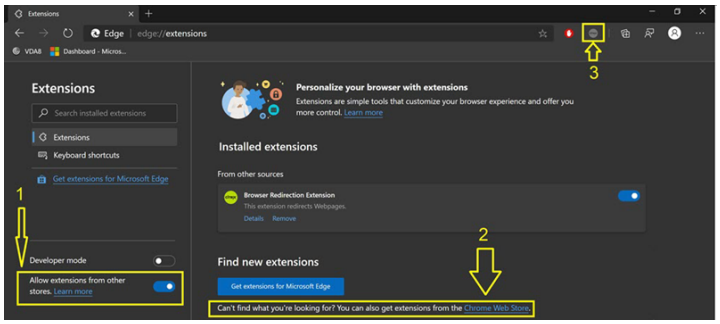
   Se a configuração **Configure the list of force-installed apps and extensions** estiver definida como **Disabled**, a extensão será removida automaticamente do Chrome para todos os usuários.

Redirecionamento de conteúdo do navegador Extensão Edge Chromium

Para instalar a extensão de redirecionamento de conteúdo do navegador no Edge, verifique se você tem instalada a versão **83.0.478.37** ou superior do navegador Edge.

1. Clique na opção **Extensions** no menu e ative **Allow extensions from other stores**.

2. Clique no link **Chrome Web Store** e a extensão aparece na barra no canto superior direito. Para obter mais informações sobre extensões do Microsoft Edge, consulte Extensões.



Redirecionamento de conteúdo do navegador e DPI

Ao usar o redirecionamento de conteúdo do navegador com o DPI (dimensionamento) definido para algum valor acima de 100% na máquina do usuário, a tela de conteúdo do navegador redirecionado é exibida incorretamente. Para evitar esse problema, não defina o DPI ao usar o redirecionamento de conteúdo do navegador. Outra maneira de evitar o problema é desativar a aceleração da GPU de redirecionamento de conteúdo do navegador para o Chrome criando a chave de registro no computador do usuário. Para obter informações, consulte Redirecionamento de conteúdo do navegador e DPI na lista de recursos gerenciados pelo registro.

Cabeçalho de solicitação do agente do usuário

O cabeçalho usuário-agente ajuda a identificar solicitações HTTP enviadas pelo redirecionamento de conteúdo do navegador. Essa configuração pode ser útil quando você configura regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas do redirecionamento de conteúdo do navegador, você poderá criar uma regra que contenha o cabeçalho usuário-agente para ignorar determinados requisitos.

Somente dispositivos Windows suportam o cabeçalho de solicitação de agente-usuário.

Por padrão, a string de cabeçalho de solicitação agente-usuário está desabilitada. Para habilitar o cabeçalho agente-usuário para conteúdo renderizado pelo cliente, use o Editor do Registro. Para obter informações, consulte User-agent request header na lista de recursos gerenciados por meio do registro.

Videoconferência HDX e compressão de vídeo na webcam

June 24, 2022

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

As webcams podem ser usadas por aplicativos executados dentro da sessão virtual usando a compactação de vídeo da webcam HDX ou o redirecionamento USB genérico HDX plug-and-play. Use o **Citrix Workspace app > Preferences > Devices** para alternar entre modos. A Citrix recomenda que você sempre use a compactação de vídeo de webcam HDX, se possível. O redirecionamento USB genérico HDX é recomendado somente quando há problemas de compatibilidade de aplicativos com compactação de vídeo HDX ou quando você precisa de funcionalidades nativas avançadas da webcam. Para um melhor desempenho, a Citrix recomenda que o Virtual Delivery Agent tenha pelo menos duas CPUs virtuais.

Para evitar que os usuários mudem a compactação de vídeo da webcam HDX, desative o redirecionamento do dispositivo USB usando as configurações da política em Configurações de política em **ICA policy settings > USB Devices policy**. Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração de microfone e webcam do Desktop Viewer **Don't use my microphone or webcam**.

Compactação de vídeo de webcam HDX

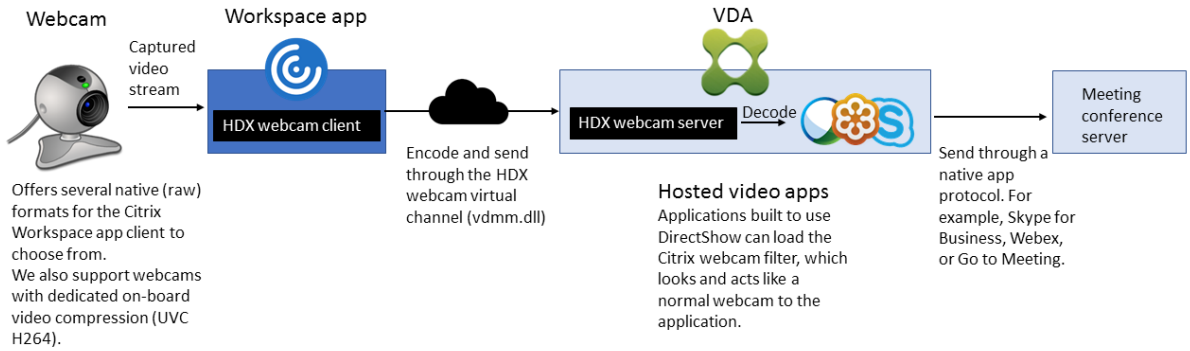
A compactação de vídeo da webcam HDX também é chamada de modo **Optimized** de webcam. Esse tipo de compressão de vídeo da webcam envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compactação de webcam HDX não codifica, transcodifica e decodifica vídeo da webcam. Esse recurso é ativado por padrão.

Para desativar o streaming direto de vídeo do servidor para o aplicativo de videoconferência, defina a chave do registro como 0 no VDA. Para obter informações, consulte Compressão de vídeo da webcam na lista de recursos gerenciados por meio do registro.

Se você desabilitar a funcionalidade padrão para recursos de streaming de vídeo, a compactação de vídeo de webcam HDX usará a tecnologia de estrutura multimídia que faz parte do sistema operacional cliente para interceptar vídeo de dispositivos de captura, transcodificar e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do sistema operacional.

O cliente lida com a comunicação com a webcam. Em seguida, o cliente envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua in-

tegração lhe proporciona o mesmo efeito em sua área de trabalho. O aplicativo Workspace compacta o vídeo para economizar largura de banda e fornecer melhor resiliência em cenários de WAN.



A compactação de vídeo da webcam HDX requer que as seguintes configurações de política estejam habilitadas (todas estão habilitadas por padrão).

- Multimedia conferencing
- Windows Media Redirection

Se uma webcam suportar codificação de hardware, a compactação 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 compactação de software, edite a chave do registro no cliente. Para obter informações, consulte Compactação de software da webcam na lista de recursos gerenciados por meio do registro.

Requisitos de compactação de vídeo de webcam HDX

A compactação de vídeo de webcam HDX suporta as seguintes versões do aplicativo Citrix Workspace:

Plataforma	Processador
Aplicativo Citrix Workspace para Windows	O aplicativo Citrix Workspace para Windows oferece suporte à compactação de vídeo de webcam para aplicativos de 32 bits e 64 bits no XenApp e XenDesktop 7.17 e versões posteriores. Em versões anteriores, o aplicativo Citrix Workspace para Windows suporta apenas aplicativos de 32 bits.

Plataforma	Processador
Aplicativo Citrix Workspace para Mac	O aplicativo Citrix Workspace para Mac 2006 ou posterior suporta compactação de vídeo de webcam para aplicativos de 64 bits no XenApp e XenDesktop 7.17 e posteriores. Em versões anteriores, o aplicativo Citrix Workspace para Mac suporta apenas aplicativos de 32 bits.
Aplicativo Citrix Workspace para Linux	O aplicativo Citrix Workspace para Linux suporta apenas aplicativos de 32 bits na área de trabalho virtual.
Aplicativo Citrix Workspace para Chrome	Como alguns Chromebooks ARM não suportam codificação H.264, apenas aplicativos de 32 bits podem usar a compactação de vídeo de webcam HDX otimizada.

Os aplicativos de vídeo baseados em base de mídia suportam compactação de vídeo de webcam HDX no Windows 8.x ou superior e Windows Server 2012 R2 e superior. Para obter mais informações, consulte o artigo do Knowledge Center CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.
- Webcam compatível com DirectShow (use as configurações padrão da webcam). As webcams capazes de codificação de hardware reduzem o uso da CPU do lado do cliente.
- Para compactação de vídeo de webcam HDX, instale drivers de webcam no cliente, obtidos do fabricante da câmera, se possível. A instalação dos drivers de dispositivo não é necessária no servidor.

Cada webcam oferece taxas de quadros diferentes e tem diferentes níveis de brilho e contraste. Ajustar o contraste da webcam pode reduzir significativamente o tráfego a montante. 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 pelo 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 começa, 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. Damos suporte a resoluções de webcam até 1920x1080.

Esse recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver for Windows, versão mínima 4.10.

Você pode usar uma chave de registro para desativar e habilitar o recurso. Para obter informações, consulte Streaming de webcam de alta definição na lista de recursos gerenciados por meio do registro.

Se a negociação de tipo de mídia falhar, o HDX cai de volta à resolução padrão de 352x288 CIF. Você pode usar chaves de registro no cliente para configurar a resolução padrão. Verifique se a câmera suporta a resolução especificada: Para obter informações, consulte Resolução de webcam de alta definição na lista de recursos gerenciados por meio do registro.

A compactação de vídeo de webcam HDX usa significativamente menos largura de banda em comparação com o redirecionamento USB genérico plug-and-play e funciona bem em conexões WAN. Para ajustar a largura de banda, configure a chave de registro no cliente. Para obter informações, consulte Largura de banda de webcam de alta definição na lista de recursos gerenciados por meio do registro.

Digite um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usam 350000 bps por padrão.

O HDX plug-and-play redirecionamento USB genérico

O redirecionamento USB genérico HDX plug-and-play (isócrono) também é chamado de modo de webcam **genérico**. O benefício do redirecionamento USB genérico HDX plug-and-play é que você não precisa instalar drivers em seu cliente fino/ponto de extremidade. A pilha USB é virtualizada de tal forma que qualquer coisa que você conecta ao cliente local seja enviada à VM remota. A área de trabalho remota age como se você o conectasse de modo nativo. A área de trabalho do Windows lida com toda a interação com o hardware e executa a lógica plug-and-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 para baixo com o protocolo USB pela rede.

Redirecionamento multimídia HTML5

May 30, 2023

O redirecionamento multimídia HTML5 estende os recursos de redirecionamento multimídia do HDX MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento na distribuição on-line de conteúdo multimídia, especialmente para dispositivos móveis, o setor de navegadores desenvolveu formas mais eficientes de apresentar áudio e vídeo.

O Flash é o padrão, mas requer um plug-in, não funciona em todos os dispositivos e causa maior uso de bateria em dispositivos móveis. Empresas como YouTube e Netflix.com e versões de navegadores mais recentes do Mozilla, Google e Microsoft estão passando para HTML5, tornando-o o novo padrão.

A multimídia baseada em HTML5 tem muitas vantagens em relação aos plug-ins proprietários, incluindo:

- Padrões independentes da empresa (W3C)
- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança criados pelos plug-ins

Downloads progressivos de HTTP

O download progressivo de HTTP é um método de pseudo-streaming baseado em HTTP que é compatível com 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 como é recebido e é reproduzido a partir dessa unidade. Se você assistir novamente o vídeo, o navegador poderá carregar o vídeo a partir do cache.

Para obter 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) em tags de vídeo HTML5, use as ferramentas de desenvolvedor no seu navegador:

Comparação entre HTML5 e Flash

Recurso	HTML5	Flash
Requer um player proprietário	Não	Sim

Recurso	HTML5	Flash
Funciona em dispositivos móveis	Sim	Alguns
Velocidade de execução em diferentes plataformas	Alta	Lenta
Suportado pelo iOS	Sim	Não
Uso de recursos	Menos	Mais
Carga mais rápida	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 adaptativa como DASH/HLS.

Oferecemos suporte ao seguinte e usamos políticas para o respectivo controle. Para obter mais informações, consulte Configurações de política multimídia.

- Renderização no lado do servidor
- Obtenção no servidor e renderização no cliente
- Obtenção e renderização do lado do cliente

Versões mínimas do aplicativo Citrix Workspace e 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	SO Windows - versão/compilação/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Versão mínima do navegador VDA	SO Windows - versão/compilação/SP
Firefox 47 Adicione manualmente os certificados ao repositório de certificados do Firefox ou configure o Firefox para procurar certificados de um repositório de certificados confiáveis 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** - Gancho de JavaScript que intercepta comandos de vídeo no site. O HdxVideo.js se comunica com WebSocketService por meio de Secure WebSockets (SSL/TLS).
- **Certificados SSL 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** - É executado no sistema local e executa a terminação SSL e o mapeamento da sessão do usuário. TLS Secure WebSocket escutando em 127.0.0.1, porta 9001.
- **WebSocketAgent.exe** - É executado na sessão do usuário e renderiza o vídeo conforme instruído a partir de comandos WebSocketService.

Como faço para habilitar o redirecionamento de vídeo HTML5?

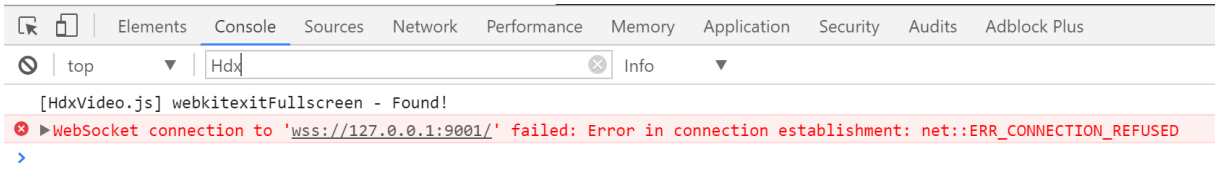
Nesta versão, esse recurso está disponível apenas para páginas da Web controladas. Ele requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas da Web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de taxas de bits adaptativas (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não têm suporte.

Para obter mais informações, consulte *Configurações de política multimídia*.

Dicas de solução de problemas

Podem ocorrer erros quando a página da Web tenta executar HdxVideo.js. Se o JavaScript não carregar, o mecanismo de redirecionamento HTML5 não funcionará. Verifique se não há erros relacionados ao HdxVideo.js inspecionando o console nas janelas de ferramentas de desenvolvedores do seu navegador. Por exemplo:



Otimização para Microsoft Teams

November 21, 2023

A Citrix oferece otimização para Microsoft Teams baseados em desktop usando o 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).

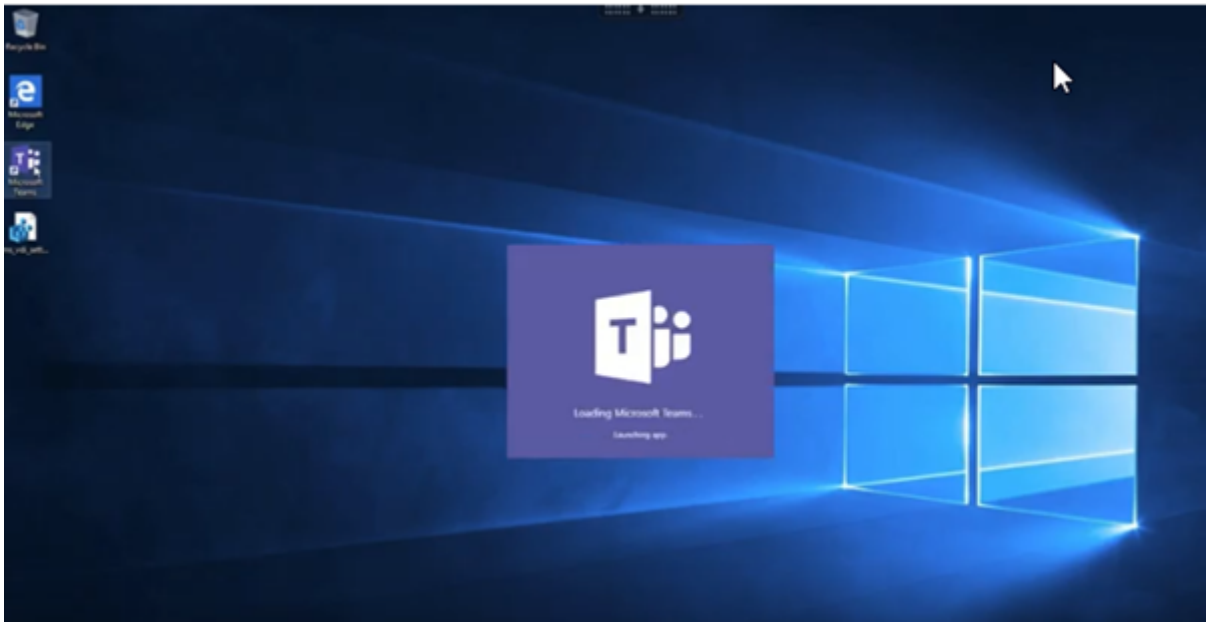
Nossa otimização para o Microsoft Teams inclui serviços HDX do lado do VDA e API para fazer interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O ponto de extremidade decodifica e renderiza a multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem de forma nativa no aplicativo hospedado pelo 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 comando e controle de canal virtual. Isso significa que não há troca de mídia entre o aplicativo Citrix Workspace e o VDA.

Apenas a busca de cliente/renderização do cliente está disponível.

Esta demonstração de vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam o uso da versão mais recente disponível do Microsoft Teams e que a mantenham atualizada.
As versões do aplicativo de desktop Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas.
Versões não suportadas do aplicativo de desktop Microsoft Teams mostram 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 em todo o computador do Microsoft Teams. Além disso, evite usar o instalador .exe que instala o Microsoft Teams no `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`. Quando você define esse parâmetro, o Instalador de Todo o Computador do Microsoft Teams 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 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` somente em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não é atualizado automaticamente sempre que há uma nova versão. Recomendamos esse modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou áreas de trabalho fora de catálogos aleatórios/agrupados do Windows Server ou Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação da VDI).

Suponha que você tem ambientes VDI persistentes dedicados do Windows 10. Você deseja que o aplicativo Microsoft Teams atualize automaticamente e prefere que o Microsoft Teams instale por usuário em `Appdata/Local`. Nesse caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> Recomendamos instalar o VDA antes de instalar o Microsoft Teams na imagem de ouro. 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 foi, desinstale e reinstale o Microsoft Teams.

Para Remote PC Access

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior depois de instalar o 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 ou posterior inclui lógica aumentada executada no momento da inicialização do Microsoft Teams e no momento do login para a detecção do VDA. Essas versões também incluem a identificação do tipo da sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem não detectar e desativar determinados recursos ou elementos da interface do usuário. Por exemplo, salas simultâneas, janelas pop-out de reuniões e chat, ou reações da reunião.

> **Importante:**
>
> Quando você faz roaming de uma sessão local para uma sessão HDX com o Microsoft Teams ainda aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar com o HDX corretamente.
> 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. Quando estiver trabalhando no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do PC remoto (HDX ou local). Isso porque o Microsoft Teams só pode avaliar o modo VDI no momento da inicialização do aplicativo, não quando ele já está sendo executado em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-up, salas simultâneas ou reações à

> reunião.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações do VDA e do Microsoft Teams em camadas diferentes, 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 perfis

Recomendamos usar o instalador em toda o computador para ambientes Windows Server e VDI em pool no Windows 10.

Quando o sinalizador **ALLUSER =1** é passado para o MSI a partir da linha de comando (o instalador em todo o computador), 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**, em vez disso.

Instalador em toda a máquina

Veja a seguir um exemplo de pastas, atalhos de área de trabalho e registros criados com a instalação do instalador do Microsoft Teams em todo o computador em uma VM de 64 bits do Windows Server 2016:

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:**
>
> A localização do registro varia de acordo com os sistemas operacionais subjacentes e o número de bits.

Recomendações, em Recommendations

- Recomendamos desativar o início automático excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do dia de trabalho) sobrecarreguem a CPU da VM.
- Se o Virtual Desktop não tiver uma GPU/vGPU, recomendamos a configuração **Desabilitar a aceleração de hardware GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada `%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 o **CPU Spikes Protection** para gerenciar o consumo do processador para o Microsoft Teams.

Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação é diferente. 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 da 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

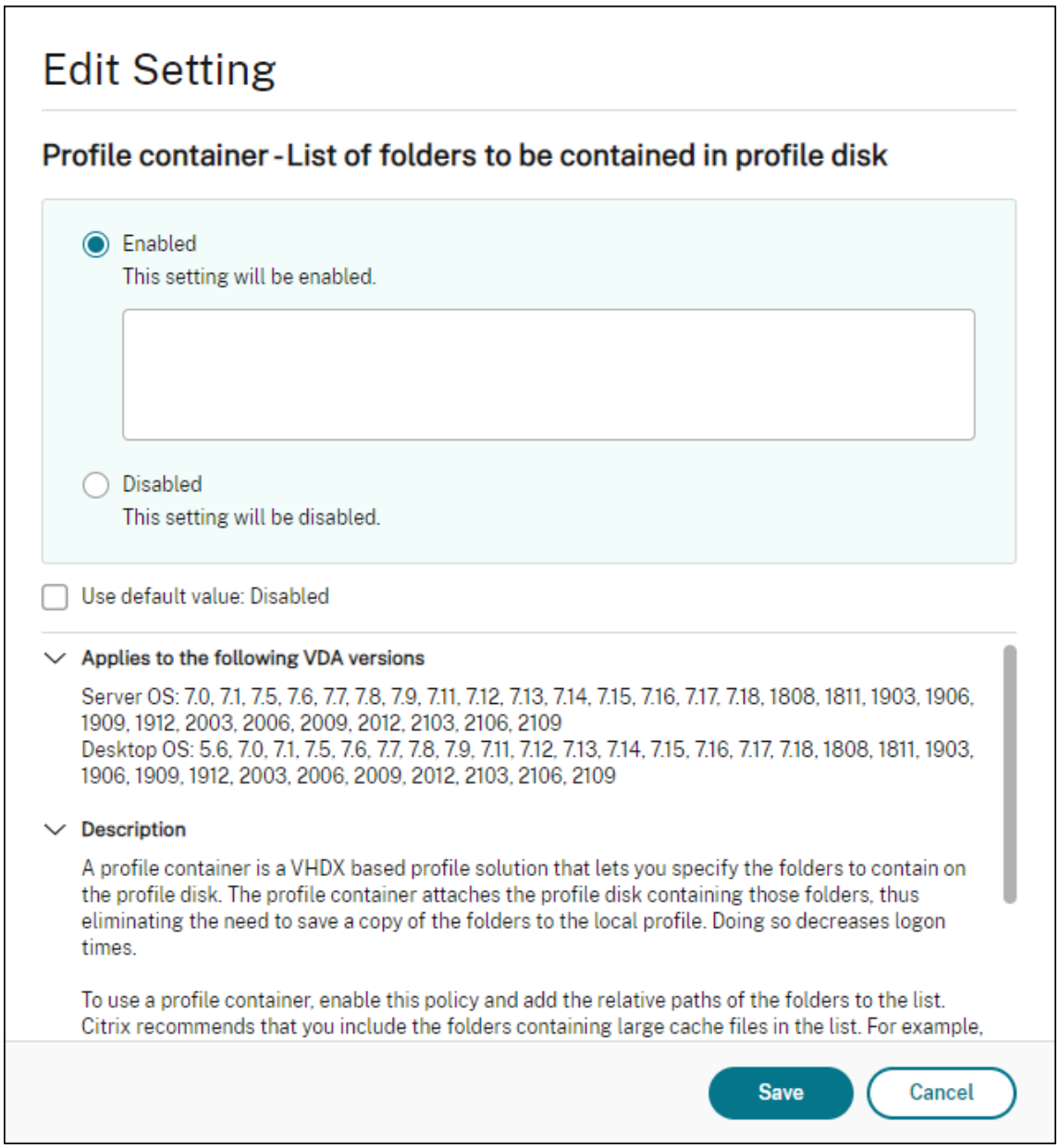
As recomendações de melhor prática baseiam-se nos cenários de caso de uso.
O uso do Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente de dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as 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 nessas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Lista de exclusão de conteúdo armazenado 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 da Microsoft . Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais a configuração não persistente.

Caso de uso: cenário de sessão única Nesse cenário, o usuário final usa o Microsoft Teams em um local de cada vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Por exemplo, em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop e o Microsoft Teams é implantado na área de trabalho virtual como um aplicativo.
Recomendamos ativar o contêiner Citrix Profile e redirecionar diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador de toda a máquina do Microsoft Teams (**ALLUSER=1**) na imagem de ouro.
2. Ative o Citrix Profile Management e configure o armazenamento de perfis de usuário com as permissões apropriadas.
3. Ative a seguinte configuração de política do Profile Management: **File system > Synchronization > Profile container –Lista de pastas que devem estar no disco de perfil**.



Liste todos os diretórios por usuário nessa configuração. Você também pode configurar essas configurações 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 Ativar a otimização do Microsoft Teams:

Sistemas operacionais compatíveis:

- Windows Server 2022, 2019, 2016, 2012R2, edições Standard e Datacenter, e com a opção Server Core

Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais compatíveis:

- Windows 11.
- Windows 10 64 bits, versões 1607 e posteriores. Os aplicativos hospedados na máquina virtual são compatíveis com o aplicativo Citrix Workspace para Windows 2109.1 ou versões posteriores.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edições Standard e Datacenter).

Requisitos:

- BCR_x64.msi - o MSI que contém 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 a exclua.

Versão recomendada —aplicativo Citrix Workspace para Windows mais recente CR e versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 bits e 64 bits, incluindo edições Embedded) (suporte para Windows 7 interrompido na versão 2006) (suporte para Windows 8.1 interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas do processador (CPU) suportadas: x86 e x64 (o ARM não é suportado).
- Requisito de ponto de extremidade: CPU dual core de aproximadamente 2,2 a 2,4 GHz que pode dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs de núcleo duplo ou quádruplo com velocidades de base mais baixas (~ 1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Clientes finos HP verificados: t630/t640, t730/t740, mt44/mt45.
- Clientes finos Dell verificados: 5070, 5470 Mobile TC e AIO.
- Clientes finos 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de pontos de extremidade verificados, consulte Clientes finos.
- O aplicativo Citrix Workspace requer um mínimo de 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 não estiver presente no sistema.

Os administradores podem ativar/desativar o Microsoft Teams iniciando no modo otimizado alterando a política de otimização do Teams. Os usuários que começam no modo otimizado no aplicativo Citrix Workspace não têm a opção de desativar 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 mínima de 1,8 GHz que possa dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com uma velocidade base de 1,8 GHz e uma alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de pontos de extremidade verificados, consulte Clientes finos.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desativar 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. Depois que a atualização for concluída, reinicie a sessão. (É necessária permissão raiz).

Versão mínima - Aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais compatíveis:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 ou 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 no **menu Apple > Preferências do sistema > Segurança e privacidade > guia Privacidade > Screen recording** e selecionam **Citrix Viewer**.

A otimização do Microsoft Teams funciona por padrão se o usuário tiver o aplicativo Citrix Workspace 2012 ou posterior e o macOS 10.15.

Se você deseja desativar 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 em execução na versão mais recente do Chrome OS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core de 2,4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desativada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de um único servidor

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) são suportados em um único host físico. Isso é comumente chamado de Citrix Virtual Apps and Desktops Single Server Scalability (SSS). No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade do usuário. A ideia é descobrir quantos usuários ou máquinas virtuais podem ser executados em um único equipamento de hardware executando um hipervisor principal.

> **Nota:**
>
> Esta seção inclui uma orientação para fazer uma estimativa de SSS. Observe que a orientação é de alto nível e pode não ser necessariamente específica para sua situação ou ambiente exclusivo. A única maneira de realmente entender o Citrix Virtual Apps and Desktops SSS é usar uma

> ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda seguir essa orientação e essas regras simples para fazer uma estimativa rápida apenas da 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 equipamentos de hardware ou tomar qualquer decisão financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máximo Turbo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- 6 TB de armazenamento SSD RAID 0 local (11 discos)

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando o Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminologia

- Carga de trabalho do Knowledge Worker: inclui Acrobat Reader, Freemind/Java, Photo viewer, Edge e aplicativos MS Office, como Excel, Outlook, PowerPoint e Word.
- Baseline: os testes de escalabilidade do servidor são executados com a carga de trabalho do Knowledge Worker (sem o Microsoft Teams).
- Carga de trabalho do Microsoft Teams: carga de trabalho típica do Knowledge Worker + Microsoft Teams.

Como é realizado o teste de estresse no Microsoft Teams

- O Microsoft Teams é otimizado com o HDX. Portanto, todo o processamento multimídia é descarregado para o ponto de extremidade ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou eliminados antes do início da carga de trabalho.
- Abra o Microsoft Teams (inicialização a frio).
- Meça o tempo gasto pelo Microsoft Teams para carregar e capturar o foco da janela principal do Microsoft Teams.
- Alterne para a janela de bate-papo usando atalhos de teclado.

- Alterne para a janela do calendário usando atalhos de teclado.
- Envie a mensagem de bate-papo para um usuário específico usando atalhos de teclado.
- Alterne para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- 40% de impacto na escalabilidade com o Microsoft Teams Workload (81 usuários), quando comparado ao Baseline (137 usuários).
- Aumentar a capacidade do servidor em ~40% (na CPU) restaura o número de usuários como com a carga de trabalho Baseline.
- 20% de memória extra necessária com o Microsoft Teams Workload, quando comparado ao Baseline.
- Aumento do tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% em gravações de IOPS, aumento de ~100% em leituras de IOPS. O Microsoft Teams pode ter um impacto significativo no ambiente com armazenamento mais lento.

Matriz de recursos e compatibilidade de versões

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace 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. Indicador de tela Borda vermelha	Versão atual menos 90 dias	1906	2002	2012	2006	Não

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para Chrome OS
ii. Limitar captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	2012	2006	Não
iii. Multi-monitor	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
Suporte a Proxy Server	Versão atual menos 90 dias	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Compartilhamento de aplicativos	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
Dar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	Não	Não

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para Chrome OS
Solicitar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	2203	2303
Várias janelas	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Transcrições de reuniões	Versão atual menos 90 dias	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Desfoque do fundo	Versão atual menos 90 dias	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer somente no modo de tela cheia. SHIFT+F2 não suportado.
2. Negociar/Kerberos, NTLM, Basic e Digest. Pac os arquivos também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, a legenda ao vivo só funcionará se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 para Linux ou 2112 para Windows. Isso ocorre porque as legendas ao vivo se comportam de maneira diferente se o Microsoft Teams está no modo de IU de Janela única ou no modo Várias janelas.
5. O modo Várias janelas foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

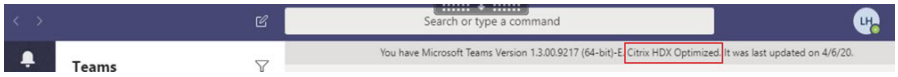
> **Nota:**
>
> Todos os recursos listados no **aplicativo Citrix Workspace para Windows 1912 CU6 (ou posterior)** são aplicáveis ao aplicativo Citrix Workspace para Windows 2203.1 LTSR CU1.

Ativar a otimização do Microsoft Teams

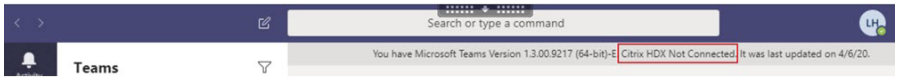
Para habilitar a otimização para o Microsoft Teams, use a política Gerenciar console descrita na política de redirecionamento do Microsoft Teams. Essa política está **ATIVADA** por padrão. Além da ativação dessa política, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima necessária. Se você habilitou a política e a versão do aplicativo Citrix Workspace for suportada, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definida como **1** automaticamente no VDA. O Microsoft Teams lê a chave a ser carregada no modo VDI.

> **Nota:**
>
> Se você estiver usando VDAs da versão 1906.2 ou posterior com versões mais antigas do controlador (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda poderá ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

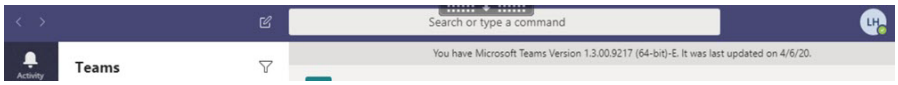
Se você clicar em **About > Version**, a legenda **Citrix HDX Optimized** exibirá:



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 em partes posteriores da pilha. O erro é mais provável nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, isso indica que o Microsoft Teams não conseguiu carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito no ícone da área de notificação e reinicie. Certifique-se de que a política Gerenciar console não esteja definida como **Prohibited** e que a versão do aplicativo Citrix Workspace seja suportada.



> **Importante: a sessão se reconecta**
>
> - Talvez seja necessário reiniciar o Microsoft Teams para obter uma sessão otimizada para HDX quando sua conectividade mudar. Por exemplo, se você estiver fazendo o roaming de um ponto de extremidade não compatível (aplicativo Workspace para iOS, Android ou versões antigas do Windows/Linux/Mac) para um ponto de extremidade compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou o oposto.
> - A reinicialização do Microsoft Teams também é necessária se você tiver instalado o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado

> para implantações de VDI persistentes. Nesses casos, o Microsoft Teams pode atualizar automaticamente enquanto a sessão HDX está no estado desconectado. Portanto, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado em um estado otimizado.
> - Ao fazer o roaming de uma sessão local para uma sessão HDX, você precisa reiniciar o Microsoft Teams para otimizar com o HDX. Essa ação é necessária em um cenário de acesso remoto ao PC.

Requisitos de rede

O Microsoft Teams conta com servidores de Processador de Mídia no Microsoft 365 para reuniões ou chamadas multipartes. O Microsoft Teams usa retransmissões de transporte do Microsoft 365 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.

Portanto, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Para obter diretrizes detalhadas sobre o planejamento de rede, consulte Princípios de conectividade de rede do Microsoft 365.

Recomendamos avaliar seu ambiente para identificar os 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 sobre suporte, consulte Suporte.

Resumo das principais recomendações de rede para o tráfego RTP (Real Time Protocol)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir da filial.
- Planeje e forneça largura de banda suficiente na filial.
- Verifique se há conectividade e qualidade de rede em cada filial.
- Se você precisar usar qualquer um dos itens a seguir na filial, confirme que o tráfego RTP/UDP (manipulado pelo HdxRtcEngine.exe no aplicativo Citrix Workspace) seja usado.
  - Ignorar servidores proxy
  - Interceptação SSL de rede
  - Dispositivos de inspeção profunda de pacotes
  - VPN hairpin (use tunelamento dividido, se possível)

> **Importante: configuração de túnel dividido de VPN**
>
> O tráfego do HdxRtcEngine.exe deve ser desviado do túnel VPN e ter a permissão de usar a

> conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira pela qual isso é realizado variará dependendo do produto VPN e da plataforma de máquina usada, mas a maioria das soluções VPN permitirá a configuração simples da política para aplicar essa lógica. Para obter mais informações com orientações de túnel dividido específicas à plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o SRTP (Secure Real-Time Transport Protocol) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para esse recurso, são usadas chaves simétricas (negociadas com DTLS) para criptografar mídia e controlar mensagens usando a codificação de criptografia AES.

As seguintes métricas são recomendadas para garantir uma experiência positiva do usuário:

Métrica	Ponto de extremidade para Microsoft 365
Latência (um sentido)	< 50 ms
Latência (RTT)	< 100 ms
Perda de pacote	< 1% durante um intervalo de 15s
Jitter entre chegada de pacotes	<30ms durante um intervalo de 15s

Para obter mais informações, consulte Preparar a rede da sua organização para o Microsoft Teams.

Em termos de requisitos de largura de banda, a otimização para o Microsoft Teams pode usar uma grande variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam estes codecs durante o processo do estabelecimento de chamada usando a oferta/resposta do Session Description Protocol (SDP).
As recomendações mínimas da Citrix são:

Tipo	Largura de banda	Codec
Áudio (em cada sentido)	~ 90 kbps	G.722
Áudio (em cada sentido)	~ 60 kbps	Opus*
Vídeo (em cada sentido)	~ 700 kbps	H264 360p a 30 fps 16:9
Compartilhamento de tela	~ 300 kbps	H264 1080p a 15 fps

Opus e H264 são os codecs preferidos para chamadas ponto a ponto e em conferência.

> **Importante:**
>
> Quanto ao desempenho, a codificação é mais cara do 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 Encoder performance estimator 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 encaminhar conexões para localhost por meio de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Bypass proxy servers for local address** em **Internet Options > Connections > LAN Settings > Proxy Servers** e ignorar `127.0.0.1:9002`.

  Se você usar um arquivo PAC, o script de configuração do proxy VDA do arquivo PAC deverá 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 por meio de um proxy, esses aplicativos suportam servidores proxy:

  - Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também têm suporte)
  - Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também têm suporte)
  - 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 configurações de proxy. Esses dispositivos enviam tráfego diretamente para servidores do Microsoft 365 TURN.

> **Importante:**
>
> - Verifique se o dispositivo cliente pode se conectar ao servidor DNS para executar resoluções de DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor Microsoft Teams Relay:


```
    - 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 de DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e o estabelecimento de mídia de chamadas em conferência falharão.

- A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não no 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 SRTP (Secure Real-Time Transport Protocol) de rede direta via User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia recorre ao TCP/TLS 443.

O mecanismo de mídia HDX dá suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal usando retransmissões em torno de NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Este suporte significa que o ponto de extremidade deve poder executar resoluções DNS.

Considere um cenário em que não há caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está ingressando em uma chamada ou reunião com vários participantes. 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 da 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 na Configuração de chamada e URLs do Office 365 e intervalos de endereços IP 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 (fallback)

Esses intervalos incluem retransmissões de transporte e processadores de mídia, com front-end por um Azure Load Balancer.

As retransmissões de transporte do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são pontos de extremidade ICE. Além disso, as retransmissões de transporte do Microsoft Teams não terminam a mídia, o TLS, nem realizam nenhuma transcodificação. Elas podem fazer a ponte TCP (se HdxRtcEngine.exe usar TCP) para o UDP quando encaminham o tráfego para outros pares ou processadores de mídia.

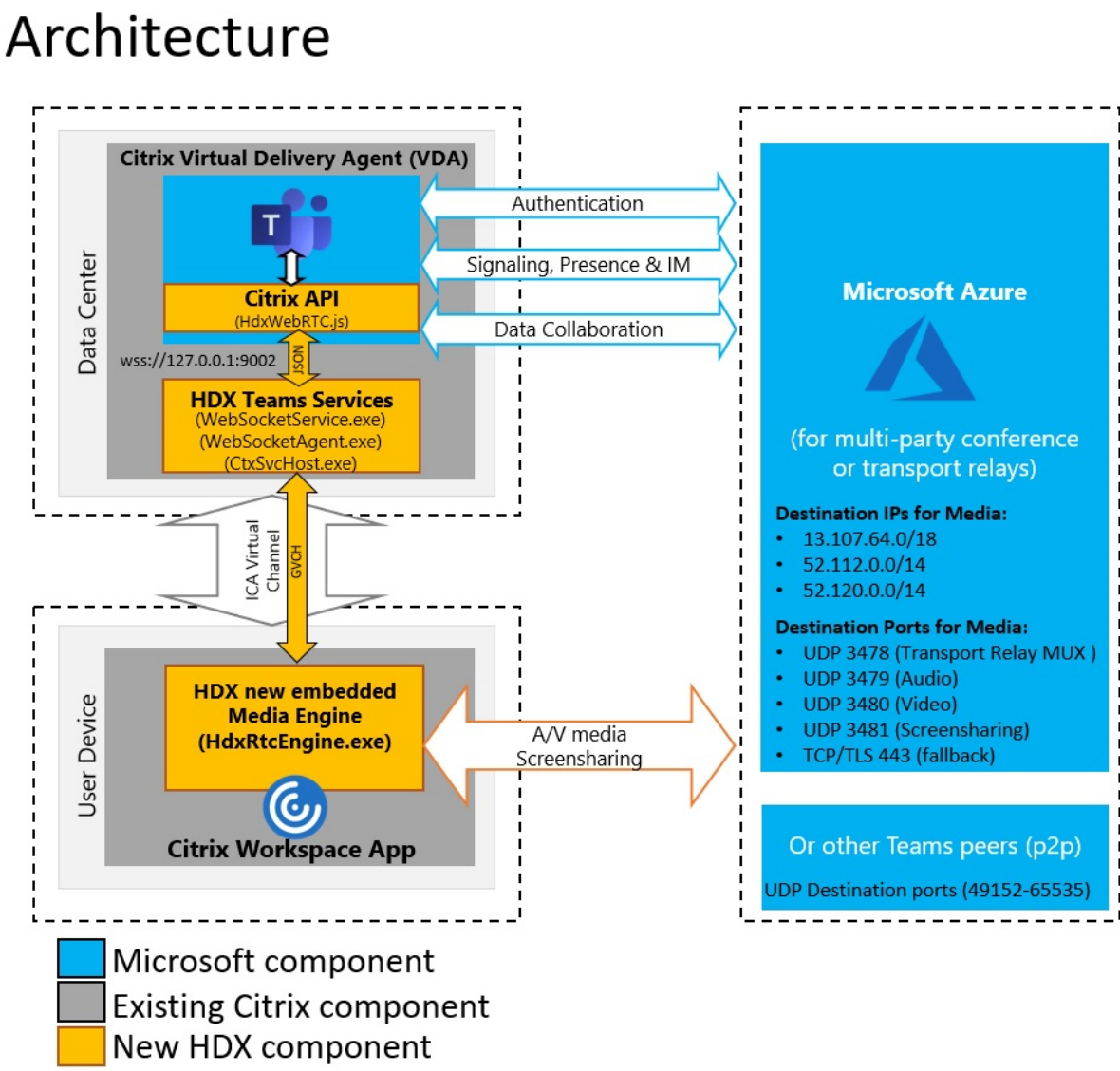
O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com a retransmissão de transporte do Microsoft Teams mais próxima na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e porta 3478—3481 UDP (portas UDP diferentes por carga de trabalho, embora possa haver multiplexação) ou 443 TCP/TLS para fallbacks. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado por TCP, aconselhamos você a projetar suas redes para acomodar o tráfego UDP na filial.

Se o Microsoft Teams for carregado no modo otimizado e o HdxRtcEngine.exe estiver sendo executado no ponto de extremidade, as falhas do ICE podem causar uma falha na configuração da chamada ou áudio/vídeo somente unidirecional. Quando um atendimento não pode ser concluído ou os fluxos de mídia não forem full duplex, verifique primeiramente o **rastreamento Wireshark** no ponto de extremidade. Para obter mais informações sobre o processo de coleta do candidato ICE, consulte "Coletando logs"na seção Suporte.

> **Nota:**
>
> Se os pontos de extremidade não tiverem acesso à Internet, os usuários talvez ainda possam fazer uma chamada ponto a ponto somente se os dois estiverem na mesma LAN. As reuniões não ocorrem. Neste caso, há um intervalo de 30 segundos antes que a configuração de chamada comece.

Configuração de chamada

Use este diagrama de arquitetura como uma referência visual para a sequência de fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.



Arquitetura

1. Inicie o Microsoft Teams.
2. O Microsoft Teams é autenticado no O365. As políticas de locatário são enviadas para o cliente Microsoft Teams e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.
3. O Microsoft Teams detecta que ele está sendo executado em um VDA e faz chamadas de API para a API JavaScript Citrix.
4. O Citrix JavaScript no Microsoft Teams abre uma conexão segura do WebSocket ao WebSocket-Service.exe em execução no VDA, que gera WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico ligando para o Citrix HDX Microsoft Teams Redirection Service (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 a otimização do Microsoft Teams.

7. O mecanismo de mídia Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem iniciar o processamento de solicitações de multimídia.

   ——Chamadas do usuário——

8. O **par A** clica no botão de **chamada**. 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 compatíveis (codecs, resoluções e assim por diante, que é conhecida como oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e daí para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização e quando são concluídas as verificações de conectividade ICE (travessia de NAT e firewall por meio de solicitações de ligação STUN). Então, a mídia Secure Real-Time Transport Protocol (SRTP) flui diretamente entre HdxRtcEngine e o outro par (ou Microsoft 365, se for uma reunião).

Sistema de Telefonia da Microsoft

O Sistema de Telefonia 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 Microsoft Teams oferece suporte ao sistema de telefonia com planos de chamadas do Microsoft 365 ou roteamento direto. Com o roteamento direto, você conecta seu próprio controlador de borda de sessão suportado ao sistema de telefonia Microsoft diretamente sem nenhum software local adicional.
Há suporte para filas de chamadas, transferência, encaminhamento, espera, silenciar e retomar uma chamada.

DTMF

O recurso de tons duplos de multifrequência (DTMF) são compatíveis com estas versões do aplicativo Citrix Workspace (ou posterior):

- 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 no Microsoft Calling Plans, Operator Connect e Direct Routing, ele permite a você:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace em execução no ponto de extremidade, em vez do cliente Microsoft Teams em execução no VDA.

A lei de Ray Baum exige que o local despachável do chamador de 911 seja transmitido para o Ponto de Atendimento Público Seguro (PSAP) apropriado. O Microsoft Teams Optimization with HDX está em conformidade com a lei de Ray Baum quando usado com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posteriores
- Aplicativo Citrix Workspace para Linux versão 2112 e posteriores
- Aplicativo Citrix Workspace para Mac versão 2112 e posteriores
- Aplicativo Citrix Workspace para Chrome OS versão 2112 e posteriores

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 localização de rede ou emergência:

- Configurações de rede
- Serviço de Informações de Local (LIS)

Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de local despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

- ID do chassi/ID da porta usando o Link Layer Discovery Protocol (LLDP) para conexões Ethernet/Switch. O Ethernet/Switch (LLDP) é suportado em:
  - Versões 8.1 e 10 do Windows
  - macOS, que requer software de ativação LLDP Para baixar o software de ativação LLDP, acesse `www.microsoft.com` e pesquise o software de ativação LLDP.
  - Linux, que exige que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do cliente fino.
- WLAN BBSID e {IPv4-IPv6; Sub-rede; Endereço MAC} do ponto de extremidade em que o aplicativo Citrix Workspace está instalado.

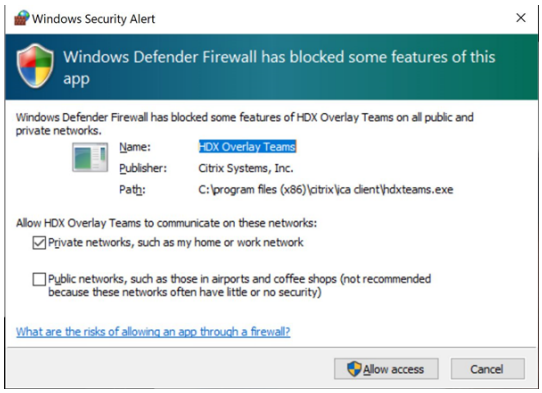
  - Locais baseados em sub-rede e WiFi são compatíveis com o aplicativo Workspace para Windows, Linux e Mac.

- Latitude e Longitude, se a permissão do usuário for concedida no nível do sistema operacional em que o aplicativo Citrix Workspace está instalado.

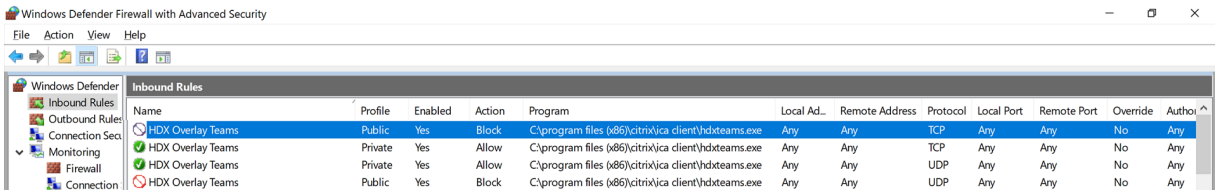
  - Compatível com todas as plataformas de aplicativos do Workspace. No entanto, no caso do Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do SO do cliente fino (sudo apt-get install libgps23 gpsd lldpd).

Considerações sobre o firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso com as configurações de **firewall do Windows**. O aviso pede aos usuários para permitir 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 **Firewall do Windows Defender > Segurança Avançada**. Você pode aplicar regras mais restritivas, se desejar.

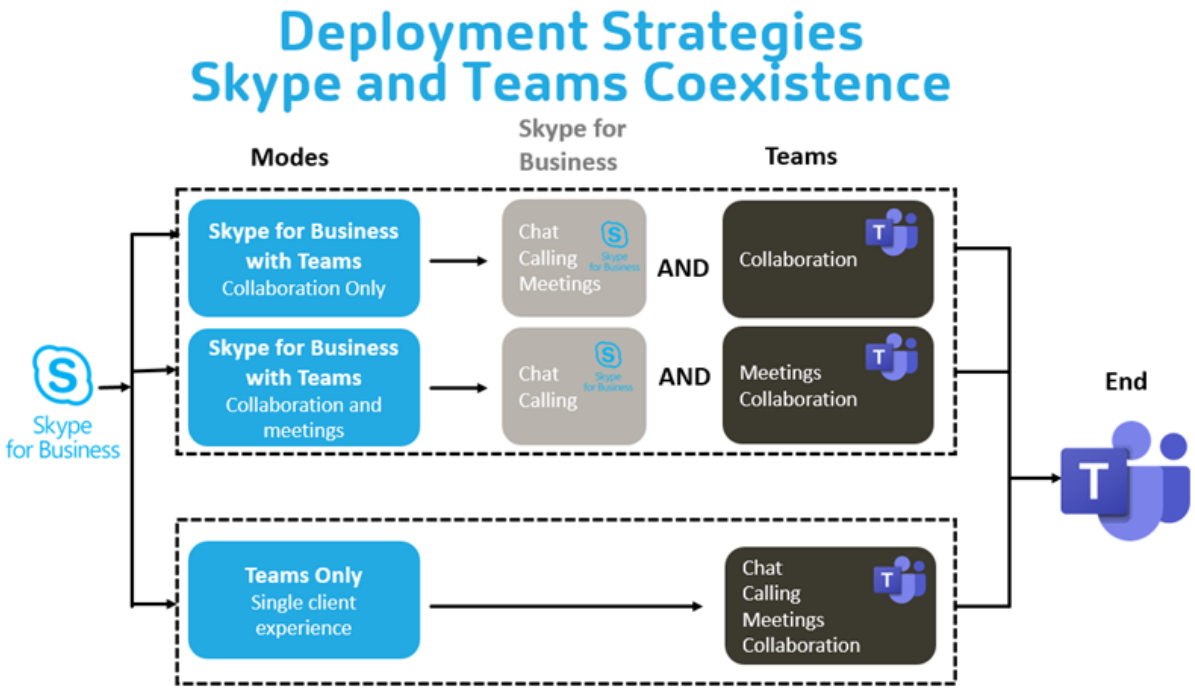


Coexistência do Microsoft Teams e Skype for Business

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 Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para os mecanismos multimídia do Microsoft Teams, em seguida, honram o conjunto de configurações Alguns exemplos são modos de ilha e colaboração do Skype for Business com o Microsoft Teams. Além disso, colaboração e reuniões do Skype for Business com Microsoft Teams.

O acesso periférico só pode ser concedido a um único aplicativo no momento. 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 Microsoft Teams

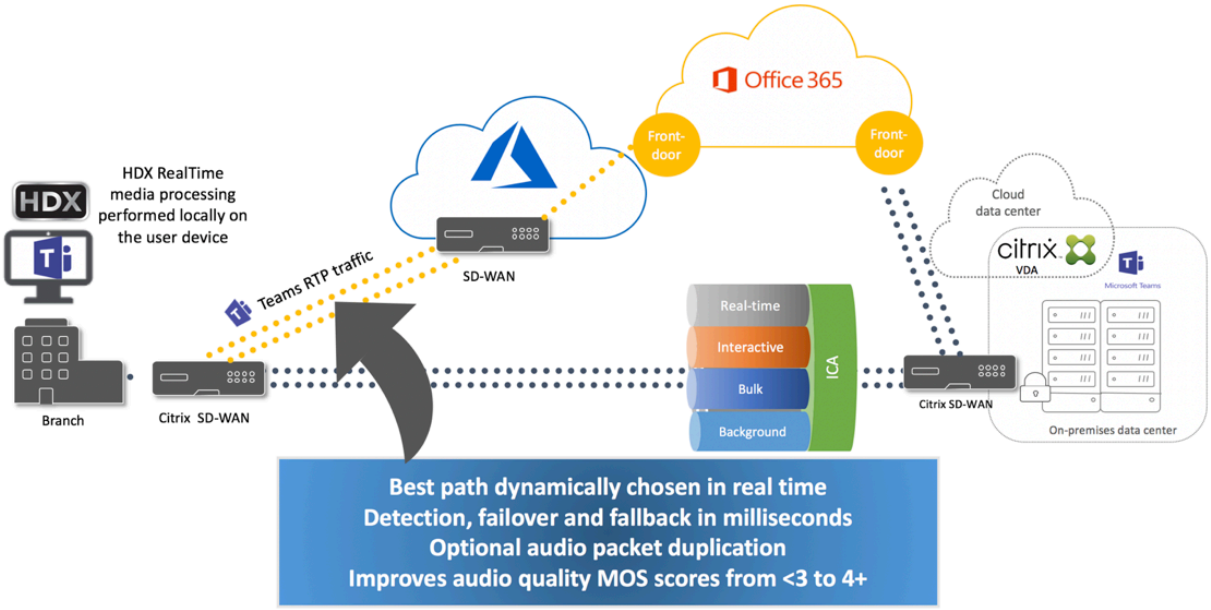
A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio-vídeo do Microsoft Teams dos usuários do aplicativo Citrix Workspace em locais de filiais para um data center antes de ir à 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 baseados 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 de banda larga de negócios em muitas áreas sofrem de perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio-vídeo do Microsoft Teams quando a integridade da rede é variável ou está degradada.

- Se você usar o Microsoft Azure, um Appliance Virtual (VPX) Citrix SD-WAN implantado no Azure VNET fornece otimizações avançadas de conectividade. Essas otimizações incluem failover de link integrado e corridas 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 fornece entrega confiável e segura para todo o tráfego direcionado à Internet.

Se a qualidade da conexão com a Internet da filial não for uma preocupação, pode ser suficiente para minimizar a latência. Desvie o tráfego do Microsoft Teams diretamente do dispositivo de filial Citrix SD-WAN para a porta da frente do Microsoft 365 mais próxima para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo com várias janelas

Você pode usar várias janelas de reuniões ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings no site do Microsoft 365.

> **Nota:**
>
> Esse 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 suporta 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 manter o foco na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas em conferência ou P2P.

> **Nota:**
>
> Esse recurso está integrado à interface do usuário/botões do Microsoft Teams. O suporte a MultiWindow é um pré-requisito que requer uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte Reuniões e bate-papo com várias janelas.

Os controles de interface do usuário do Microsoft Teams de 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 durante a substituição da imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição da imagem de fundo definida pelo administrador e pelo usuário não é compatível com a interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser definidas usando parâmetros de configuração no cliente, se a imagem também estiver armazenada no cliente.

Configurar uma imagem de fundo personalizada

As chaves de registro a seguir só são necessárias se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso ou se um administrador quiser substituir os comportamentos padrão. Por exemplo, desativar o desfoque da tela de fundo porque o ponto de extremidade não é poderoso o suficiente.

No Windows Para definir uma imagem de fundo personalizada, os administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou ponto de extremidade:

Localização: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição da imagem de fundo)

O valor definido como 1 desfoca o fundo. Esse valor pode ser definido pelo usuário final ou pelo administrador.

O valor definido como 2 também requer que a chave **VideoBackgroundImage** esteja presente também. Somente o administrador pode definir esse valor. A seguinte chave é necessária somente se você quiser substituir a imagem de fundo, não para desfocar:

- 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 do registro também pode ser usada para habilitar o desfoque em segundo plano ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de interface do usuário do Microsoft Teams. Em outras palavras, se o seu ambiente ou VDA não suportar várias janelas, você ainda poderá aplicar a solução alternativa do 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 da chave do Registro só entram em vigor quando a sessão HDX se conecta.

No Mac Localização 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 Localização 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,

```
1 {
2
3
4 "VideoBackgroundEffect":2,
5
6 "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
```



```
7
8   }
9
10 <!--NeedCopy-->
```

Em HTML5 Para HTML5, só o desfoque de fundo é suportado. A substituição de imagens personalizadas não é suportada.

Para desfocar o fundo, faça o seguinte:

1. Navegue até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
1  'features' : {
2
3      'msTeamsOptimization' :
4      {
5
6          'backgroundEffects' : true
7       }
8
9   }
10
11 <!--NeedCopy-->
```

3. Salve as alterações.

Considerações sobre o consumo de CPU cliente

Embora o recurso de desfoque seja econômico em termos de uso de CPU, você pode esperar um aumento no consumo. Por exemplo, em um cliente fino com um chip Intel® Pentium® Silver de 4 núcleos e 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%.

Exibição de galeria e alto-falantes ativos no Microsoft Teams

O Microsoft Teams oferece suporte a layouts de **Gallery**, **Large gallery** e **Together mode**.

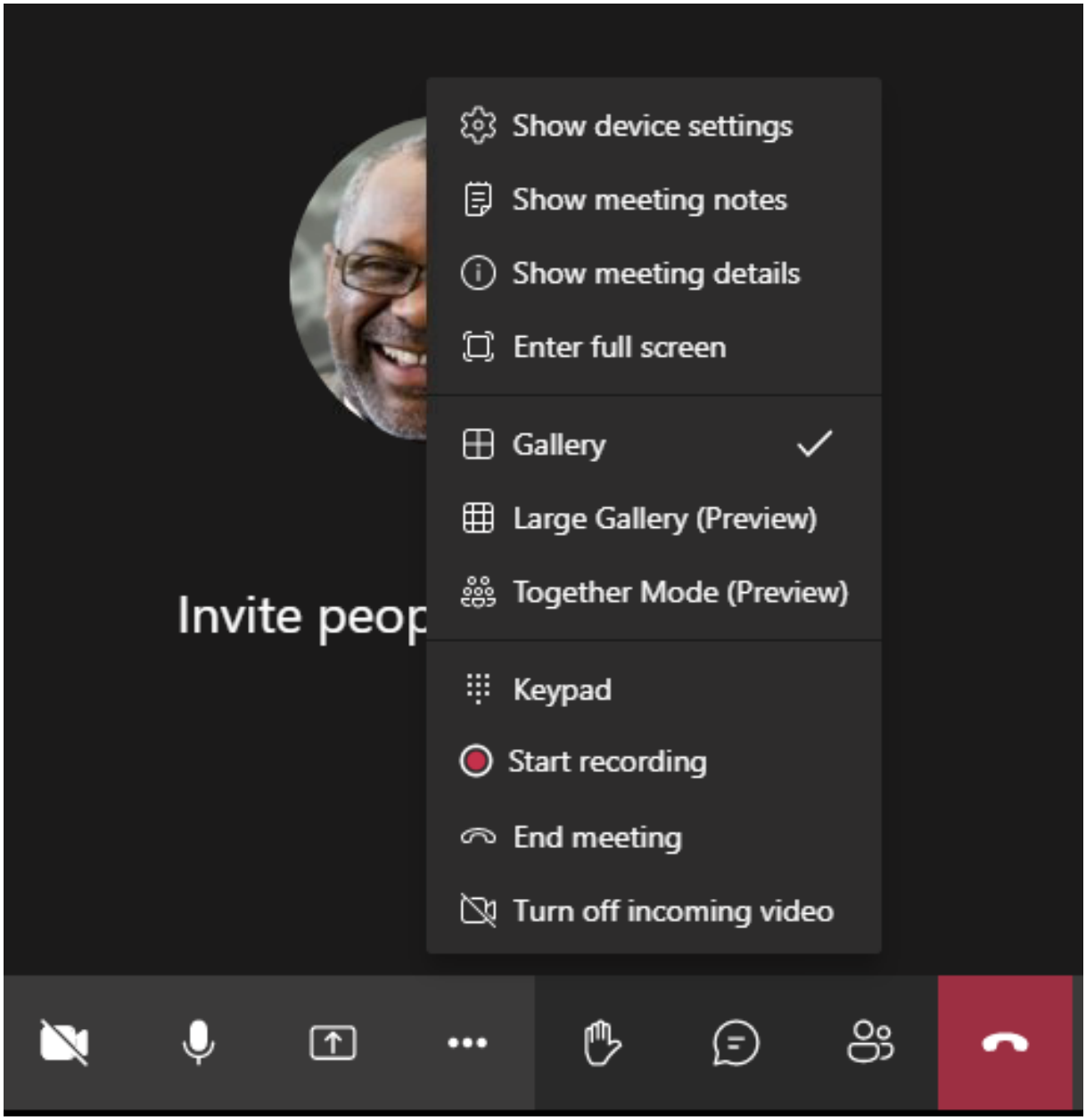
O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecidos como **Gallery**). Nesse caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham vídeo, apenas os últimos quatro alto-falantes mais ativos aparecem na tela.

O Microsoft Teams também fornece a grande visualização da galeria com uma grade de até 7x7. Como resultado, o servidor de conferência 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, em estilo de matriz, também pode incluir o vídeo de pré-visualização automática dos usuários.

Por fim, o Microsoft Teams suporta o **Together mode**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para colocar digitalmente os participantes em um histórico compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada em conferência selecionando layouts de **Gallery**, **Large gallery** ou **Together mode** no menu de reticências.



Suporte para restrições de proporção de vídeo (CWA para Windows 2102, CWA para Linux 2106, CWA para MAC 2106 ou posterior):

- A opção **Preencher a moldura** está disponível em Gallery/Large Gallery View. Essa 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 Gallery e Large Gallery:

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Layout/Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro últimos palestrantes mais ativos aparecem na tela e os outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.
Técnica mista	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central combina e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Esta ação introduz um pouco de latência adicional.
Alto-falante ativo	O novo alto-falante ativo substitui o alto-falante menos ativo na grade.	Exibe todos os participantes, independentemente de estarem ativos ou inativos.
Codificação no ponto de extremidade	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no ponto de extremidade	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no ponto de extremidade pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo de áudio e vídeo. Isso reduz o consumo de CPU no ponto de extremidade.

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo poderá ser maior.	720p para o layout composto ou misto. Não há necessidade de um stream 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.
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. Esse fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com más condições de rede afeta a qualidade de todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência fornece qualidades diferentes com base nas condições de rede de participantes individuais.
Autovisualização	Mostra você em uma pequena miniatura em tempo real.	Mostra você em uma miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout do vídeo principal com algum atraso adicional.

Compartilhamento de tela no Microsoft Teams

O Microsoft Teams conta com o compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho que está sendo compartilhada com codecs de vídeo como o 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 aplicativo Citrix Workspace 2109 ou superior, para Windows, Linux e Mac, e do aplicativo Citrix Workspace 2303, para ChromeOS, os usuários podem compartilhar suas telas e câmeras 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 é pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O par deve então retomar manualmente o compartilhamento da câmera.

> **Nota sobre o PowerPoint Live**
>
> Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros colegas ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para ver outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar uma apresentação de slides do PowerPoint Live, clique no botão da "Bandeja de compartilhamento"e selecione um dos slides sugeridos do PowerPoint, ou clique em "Procurar"e localize um arquivo do PowerPoint no 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. Aplicativos locais sobrepostos ao Desktop Viewer não são capturados.

> **Nota**
>
> Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

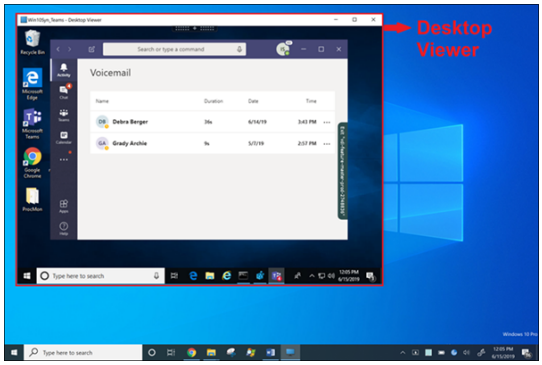
Multimonitor

Se o Desktop Viewer (CDViewer.exe) estiver no 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 selecione o monitor que deve ser compartilhado.

Limitação conhecida:

- Se o Desktop Viewer estiver desativado 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 desativado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela com vários monitores.
- Nas versões do aplicativo Workspace anteriores à 2106, somente o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor primário para que o outro par na chamada possa vê-lo.

- O compartilhamento de tela com vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout do 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 só é possível se o aplicativo local tiver sido sobreposto no Desktop Viewer. Esse comportamento foi removido na versão 2009.6 ou posterior, e 1912 CU5 ou posterior.
- Durante o compartilhamento de tela, se você mudar do modo de janela para tela cheia, o compartilhamento de tela é interrompido. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.



Compartilhamento de tela a partir de um aplicativo integrado:

Se você estiver publicando o Microsoft Teams como um aplicativo integrado independente, o compartilhamento de tela capturará a área de trabalho local do seu ponto de extremidade físico. É necessário o aplicativo Citrix Workspace versão mínima 1909.

Compartilhamento de aplicativos

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

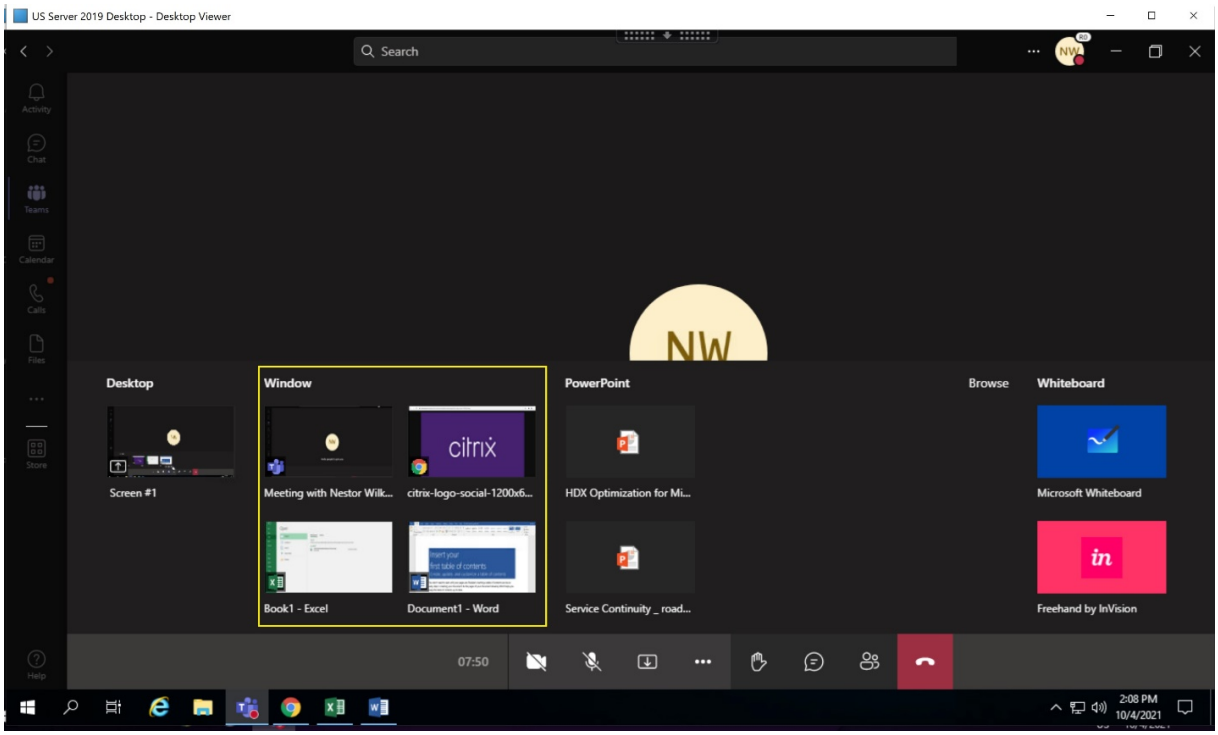
Começando com o aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Para compartilhar um aplicativo específico:

1. Navegue até o aplicativo Microsoft Teams em 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 que você selecionou e os colegas na chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desativar 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 o CTX253754 para obter 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 do lado do VDA da janela. O conteúdo é 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 colegas ou servidor de conferência.



Limitações conhecidas com o compartilhamento de tela de um aplicativo específico:

- O ponteiro do mouse não fica visível quando você está compartilhando a tela de um aplicativo.
- Se você minimizar um aplicativo ao compartilhá-lo, somente 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 você maximizar o aplicativo.
- Os aplicativos LAA (acesso a aplicativos locais) mostram uma lista de aplicativos que podem ser

compartilhados com aplicativos de desktop no Microsoft Teams otimizado no VDA. No entanto, quando você seleciona 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 a partir de um grupo de entrega que tenha a proteção de aplicativo ativada.

Quando você clica em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Área de trabalho**. Você só pode selecionar a opção **Janela** para compartilhar um aplicativo aberto.

> **Nota:**
>
> Quando você inicia aplicativos ou áreas de trabalho de um grupo de entrega com a proteção de aplicativos ativada, não é possível ver o vídeo recebido ou o compartilhamento de tela.

Conceder e solicitar controle no Microsoft Teams Este recurso é suportado nas 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 posteriores
- Aplicativo Citrix Workspace para Mac versão 2203.1 e posteriores
- Aplicativo Citrix Workspace para Linux versão 2203 e posteriores
- Aplicativo Citrix Workspace para ChromeOS versão 2303 e posteriores

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de obter o controle, você pode fazer seleções, edições ou outras atividades usando o teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela está 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 a sua solicitação.

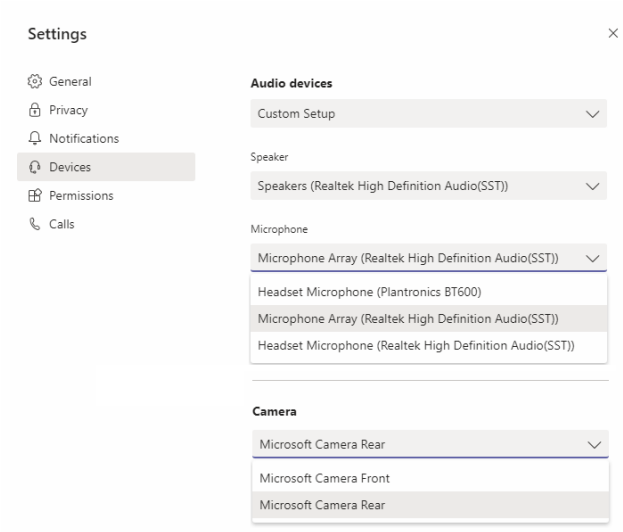
Enquanto você tem controle, você pode fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar o teclado e o mouse. Quando terminar, clique em **Solicitar controle**.

> **Limitações:**
>
> - Conceder e solicitar controle não estarão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como compartilhamento de aplicativo). A área de trabalho ou o monitor completo devem ser compartilhados.

> - O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização do Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fone de ouvidos, microfones, câmeras, alto-falantes e assim por diante). Em seguida, os periféricos são listados devidamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele usa o 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 a partir do mesmo ponto de extremidade.

Recomendações:

- Headsets certificados pelo 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 disso é uma webcam com um microfone embutido e um monitor com alto-falantes. Ao usar alto-falantes externos, coloque-os o mais longe possível do microfone. Além disso, coloque-os longe de qualquer superfície que possa refratar o som para o microfone.
- Câmeras certificadas pelo Microsoft Teams, embora os periféricos certificados pelo Skype for Business sejam compatíveis com o Microsoft Teams.

- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento de CPU com webcams que executam 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 com 24 bits ou com frequências acima de 96 kHz.
>
> O HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou mais antigo) suporta apenas esses formatos de dispositivo de áudio específicos (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**.
>
> **Webrpc** apresenta logs em **HdxTeams.exe** que 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 suportado.

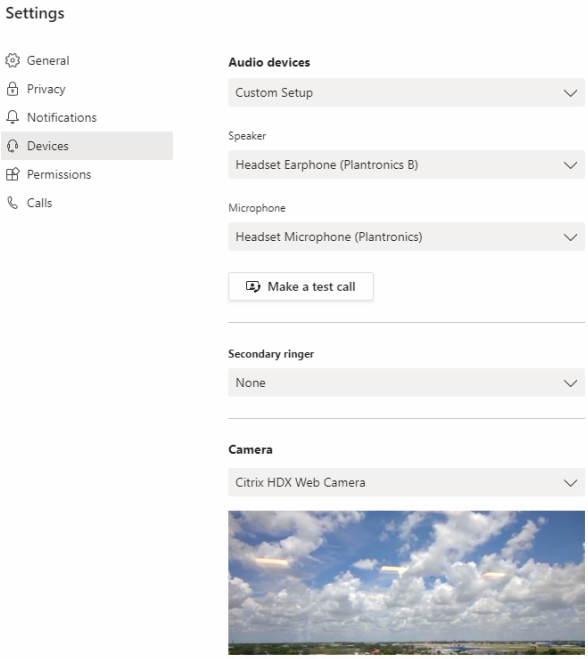
Modo de fallback

Se o Microsoft Teams não carregar no modo VDI otimizado (“Citrix HDX não conectado”em Teams/About/Version), o VDA retornará às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento da webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando um sistema operacional de versão/plataforma do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não serão aplicadas. No modo de reserva, os periféricos são traçados ao VDA. Os periféricos aparecem no 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 pelo registro.

Esse recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior.

Para determinar se você está no modo otimizado ou não otimizado ao observar 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 herdadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX** como mostrado no gráfico a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) quando comparados com o modo otimizado.



Quando são usadas as tecnologias HDX herdadas, o Microsoft Teams não descarrega o processamento de compartilhamento de áudio, vídeo e tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do ponto de extremidade. Em vez disso, as tecnologias HDX usam renderização no lado do servidor. Espere alto consumo de CPU no VDA quando você liga o vídeo. O desempenho de áudio em tempo real pode não ser otimizado.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e terminar chamada não têm suporte. Aumentar e diminuir volume têm suporte.
- As configurações de QoS no Admin Center for Microsoft Teams não se aplicam a usuários de VDI.
- O recurso complementar de proteção de aplicativo para o aplicativo Citrix Workspace impede o compartilhamento de tela de saída e bloqueia o compartilhamento de tela e o vídeo de entrada.

- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.

Limitação no VDA:

- Quando você define a configuração de DPI alto do aplicativo Citrix Workspace como **Sim**, a janela de vídeo redirecionado aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum 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 no computador cliente, não no VDA.

Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams em Windows e Mac. Para Linux, consulte seu fornecedor de cliente fino.
Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes terminais são aprimoradas com a adaptação à resolução adequada para a melhor experiência de chamada para todos os chamadores.

Com essa experiência aprimorada, cada usuário pode enviar vários fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p e assim por diante), dependendo de vários fatores, incluindo capacidade do ponto de extremidade, condições da rede e outros. Depois, o ponto de extremidade receptor solicita a resolução de qualidade máxima que pode suportar, proporcionando a todos os usuários a melhor experiência de vídeo.

> **Nota:**
>
> Esse recurso está disponível somente após o lançamento da atualização do Microsoft Teams. Para obter informações sobre o ETA, acesse https://www.microsoft.com/ e pesquise o roadmap do Microsoft 365. Quando a atualização for lançada pela Microsoft, você poderá verificar o CTX253754 para obter a atualização da documentação e o anúncio.

Limitação da Microsoft

- Uma visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams —entre em contato com a Microsoft para saber para quando esperar a grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.

- A resolução máxima de fluxo de vídeo de entrada e saída é de 720p. Dependência do Microsoft Teams —entre em contato com a Microsoft para saber para quando esperar 1080p.
- O toque de retorno de chamada PSTN não é suportado
- O desvio de mídia para roteamento direto não tem suporte.
- As funções de produtor e apresentador de eventos de transmissão e ao vivo não têm suporte. A função de participante tem suporte, mas não é otimizada (renderiza no VDA).
- A função de aumentar zoom e diminuir zoom no Microsoft Teams não é suportada.
- Não há suporte para roteamento baseado na localização e bypass de mídia.
- A mesclagem de chamadas não é suportada (opção não exibida na interface do usuário).

Limitação da Citrix e Microsoft

- Ao fazer o compartilhamento de tela, a opção **include system audio** não está disponível.
- O Simulcast não é compatível com o ChromeOS.

Fim da vida útil (EOL) da janela única do Microsoft Teams

Em 31 de janeiro de 2024, a Microsoft retirará o suporte do Microsoft Teams para interface de usuário de janela única ao usar a otimização de VDI do Microsoft Teams e oferecerá suporte somente à experiência de várias janelas. A Microsoft notificou sobre essa descontinuação em 8/9/2023 no Centro de Administração do M365 (ID da publicação: MC674419).
Detalhes públicos sobre o recurso de várias janelas podem ser encontrados no artigo da Tech Community: 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 compartilhamento de vídeo e tela. Se você não atualizar sua infraestrutura e pontos de extremidade para oferecer suporte a várias janelas, só poderá estabelecer chamadas de áudio. Você não poderá usar a funcionalidade otimizada de vídeo e compartilhamento de tela.

A tabela a seguir ilustra as versões mínimas, LTSR e recomendadas do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams no Citrix VDI:

Componente	Versão mínima	Versão compatível com LTSR	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+

Componente	Versão mínima	Versão compatível com LTSR	Versão recomendada
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 (Plan B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP (Plan B) do WebRTC atual em versões futuras. Você deve usar o Unified Plan no WebRTC para ter suporte às funcionalidades otimizadas do Microsoft Teams.

Produtos afetados

Em uma das futuras versões do aplicativo Citrix Workspace, chamadas entre pontos de extremidade com a próxima versão do aplicativo Citrix Workspace e pontos de extremidade com o aplicativo Citrix Workspace 2108 ou versões anteriores não serão suportadas. Essa incompatibilidade de chamadas inclui clientes do aplicativo Citrix Workspace (CWA) 1912 LTSR. Os seguintes clientes do CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

Substituição do Plan B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior à 2109, deverá atualizar para uma versão compatível (de preferência a versão CR mais recente). Caso contrário, chamadas com uma versão futura ou com pontos de extremidade mais recentes apresentarão falha na conexão.

As chamadas entre versões futuras e seus parceiros de comunicação federados também podem não ser concluídas se o parceiro federado não tiver atualizado o seu Citrix Workspace.

O aplicativo Citrix Workspace encerrou a data de suporte à versão 2108 em março de 2023, devendo ser atualizado para uma versão mais recente. Para obter mais informações, consulte Workspace App para obter detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plan B, consulte a documentação do WebRTC.

Informações adicionais

- Monitoramento, resolução de problemas e suporte ao Microsoft Teams
- Implantar o Microsoft Teams da área de trabalho na VM
- Instalar o Microsoft Teams usando o MSI (seção Instalação da VDI)
- Clientes finos
- Ferramenta de avaliação de rede do Skype for Business
- Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.

Windows Media redirection

July 1, 2022

O redirecionamento do Windows Media controla e otimiza a maneira como os servidores fornecem streaming de áudio e vídeo aos usuários. Com a reprodução dos arquivos de tempo de execução de mídia no dispositivo cliente em vez do servidor, o redirecionamento do Windows Media reduz os requisitos de largura de banda para reproduzir arquivos multimídia. O redirecionamento do Windows Media melhora o desempenho do Windows Media Player e players compatíveis em execução em áreas de trabalho virtuais do Windows.

Se os requisitos para a busca de conteúdo do lado do cliente do Windows Media não forem atendidos, o fornecimento de mídia usará automaticamente a obtenção no lado do servidor. Este método é transparente para os usuários. Você pode usar o Citrix Scout para executar um rastreamento de Citrix Diagnosis Facility (CDF) a partir de HostMMTransport.dll para determinar o método usado. Para obter mais informações, consulte Citrix Scout.

O redirecionamento do Windows Media intercepta o pipeline de mídia no servidor host, captura os dados de mídia em seu formato comprimido nativo e redireciona o conteúdo para o dispositivo cliente. Em seguida, o dispositivo cliente recria o pipeline de mídia para descompactar e renderizar os dados

de mídia recebidos do servidor host. O redirecionamento do Windows Media funciona bem em dispositivos clientes que têm um sistema operacional Windows. Esses dispositivos têm a estrutura multimídia necessária para reconstruir o pipeline de mídia como ele existia no servidor host. Os clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento do Windows Media** controla esse recurso e é **Permitido** por padrão. Normalmente, 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 do Windows Media parece pior do que a mídia renderizada usando compactação básica ICA e áudio normal. Você pode desativar esse recurso adicionando a configuração de **Redirecionamento de Mídia do Windows** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações da política, consulte Configurações de política multimídia.

Limitação:

Quando você estiver utilizando o Windows Media Player e as Extensões Remotas de Áudio e Vídeo (RAVE) ativadas dentro de uma sessão, poderá aparecer uma tela preta. Esta tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Em Execução no início**.

Redirecionamento geral de conteúdo

July 1, 2022

O redirecionamento de conteúdo permite controlar se os usuários acessam informações usando aplicativos publicados em servidores ou usando aplicativos executados localmente no dispositivo dos usuários.

Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a maneira como os arquivos do lado do cliente são acessíveis na sessão do lado do host.

- Quando você ativa somente o mapeamento da unidade do cliente no servidor, os volumes completos do lado do cliente são mapeados automaticamente para as sessões como links UNC (Convenção de nomenclatura universal).
- Quando você ativa o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo desktop do Windows, a parte do volume local especificado pelo usuário é redirecionada.

Redirecionamento de host para cliente

Considere usar o redirecionamento do host para o cliente para casos específicos de uso incomum. Normalmente, outras formas de redirecionamento de conteúdo podem ser melhores. Damos suporte a esse tipo de redirecionamento somente em VDAs de SO multissessão e não em VDAs de SO de sessão única.

Acesso a aplicativo local e redirecionamento de URL

O Acesso a Aplicativo Local integra aplicativos do Windows instalados localmente em um ambiente de desktop hospedado. Ele faz isso sem mudar de um computador para outro.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não têm suporte otimizado ou quando este é inadequado.

Redirecionamento de pasta do cliente

June 24, 2022

O redirecionamento de pasta do cliente altera a maneira como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Se você ativar somente o mapeamento da unidade do cliente no servidor, os volumes completos do lado do cliente são mapeados automaticamente para as sessões como links da Convenção de Nomenclatura Universal (UNC). Quando você ativa o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo desktop do Windows, a parte do volume local especificado pelo usuário é redirecionada.

Somente 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 links UNC através do registro, as pastas do cliente aparecerão como unidades mapeadas dentro da sessão.

O redirecionamento da pasta do cliente é suportado apenas em máquinas do sistema operacional Windows de sessão única.

O redirecionamento da pasta do cliente para uma unidade USB externa não é salvo ao desanexar e reconectar o dispositivo.

Ativar a direção da pasta do cliente no servidor. Em seguida, no dispositivo cliente, especifique quais pastas devem ser redirecionadas. O aplicativo usado 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 edição Embedded)
- Windows 7, edições de 32 bits e 64 bits (incluindo edição Embedded)

Para habilitar o redirecionamento de pasta de 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. Verifique se a versão mais recente do aplicativo Citrix Workspace está instalada.
2. No diretório de instalação do aplicativo Citrix Workspace, inicie o CtxCFRUI.exe.
3. Escolha o botão de opção **Custom** e adicione, edite ou remova pastas.
4. Desconecte e reconecte suas sessões para que a configuração tenha efeito.

Redirecionamento de host para cliente

July 1, 2022

O redirecionamento de host para cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix, sejam abertas usando o aplicativo correspondente no dispositivo de ponto de extremidade do usuário. Alguns casos de uso comuns para redirecionamento de host para cliente incluem:

- Redirecionamento de sites nos casos em que o servidor Citrix não tem acesso da Internet ou da rede à fonte.
- Redirecionamento de sites quando executar um navegador da Web dentro da sessão Citrix não é desejado por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos nos casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento de host para 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 redirecionar URLs em navegadores da Web, consulte Redirecionamento de URL bidirecional ou Redirecionamento de conteúdo do navegador.

Requisitos do sistema

- VDA para 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 Host to client redirection para ativar essa funcionalidade. **Host to client redirection** é desativada por padrão. Depois de ativar a política Host to client redirection, 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>
<!--NeedCopy-->
```

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 o seu arquivo ServerFTAdefaultPolicy.xml.

> **Nota:**

> Se um servidor Citrix não tiver as configurações da política de grupo, o Windows solicitará que os usuários 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 a configuração do cliente. Crie a seguinte chave de registro e os valores no cliente Windows.

> **Nota:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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. Tenha o cuidado 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 de valor: especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade do URL. Por exemplo:
  `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL somente para clientes Windows. Os clientes que não têm as configurações de registro acima rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para lidar com os tipos de URL especificados.

Para remover os tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e os valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD
- Dados de valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados de 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 de host para 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 de valor: especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNS). Digite vários FQDNS em linhas separadas. Inclua somente o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este caractere curinga combina um único nível de domínio, que é consistente com as regras no RFC 6125. Por exemplo:

```
www.exmaple.com
*.example.com
```

> **Nota:**
>
> Você não pode usar a chave **ValidSites** em combinação com as chaves **DisableServerFTA** e **NoRedirectClasses**.

Configuração do navegador padrão de VDA do servidor

Ativar o redirecionamento de host para cliente, conforme mencionado nesta seção, substitui qualquer configuração padrão anterior do navegador no VDA do servidor. Se um URL da Web não for redirecionado, o Citrix Launcher passa a 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 de VDA do servidor na lista de recursos gerenciados através registro.

Redirecionamento de conteúdo bidirecional

September 16, 2022

O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS presentes em navegadores da Web, ou incorporados em aplicativos, sejam encaminhados entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Um URL inserido em um navegador em execução na sessão Citrix pode ser aberto por meio do navegador padrão do cliente. Por outro lado, um URL inserido em um navegador em execução no cliente pode ser aberto em uma sessão Citrix, tanto com um aplicativo publicado quanto uma área de trabalho. Alguns casos de uso comuns para redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da Web nos casos em que o navegador inicial não tem acesso de rede à fonte.
- Redirecionamento de URLs da web por motivos de segurança e compatibilidade do navegador.
- Não é desejável o redirecionamento de URLs da Web incorporados em aplicativos durante a execução de um navegador da Web na sessão Citrix ou no cliente.

Requisitos do sistema

- VDAs de SO de sessão única ou multissessão
- Aplicativo Citrix Workspace para Windows

Navegadores:

- Internet Explorer 11
- Extensão de redirecionamento do Google Chrome com Citrix Browser (disponível na Google Chrome Web Store)
- Microsoft Edge (Chromium) com extensão de redirecionamento de navegador Citrix (disponível na Google Chrome Web Store)

Configuração

O redirecionamento de conteúdo bidirecional deve ser ativado usando a política da Citrix no VDA e no cliente para que o redirecionamento funcione. O redirecionamento de conteúdo bidirecional está desativado por padrão.

Quanto à configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações de política do ICA.

Quanto à configuração do cliente, consulte Redirecionamento de conteúdo bidirecional na documentação do aplicativo Citrix Workspace para Windows.

As extensões do navegador devem ser registradas por meio dos 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 o `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` com a opção de navegador necessária, conforme mostrado nos exemplos seguintes:

```
%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 do navegador, use a opção `/unreg<browser>`, como no exemplo mostrado:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Para registrar as extensões do navegador no cliente, abra um prompt de comando e execute o `%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 a primeira inicialização. A extensão do navegador também pode ser instalada manualmente por meio da Google Chrome Web Store.

Redirecionamento com curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de caracteres curinga para definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional,

consulte as instruções de configuração.

No Citrix Studio, defina o URL curinga em **Allowed URLs to be redirected to Client**. O asterisco (*) é o caractere curinga.

> **NOTA:**
>
> - Não defina **Allowed URLs to be redirected to VDA** na política do cliente. Certifique-se de que os sites tenham definido **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 são redirecionados.

Redirecionamento de protocolo personalizado do VDA para o cliente

O redirecionamento de conteúdo bidirecional suporta o 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 lidar com o protocolo. Caso contrário, a URL será redirecionada para o cliente e não será iniciada.
> - URLs de protocolos personalizados que você insere ou inicia nos navegadores Chrome e Edge não são compatíveis e não são redirecionados.
> - 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 o URL é aberto após um redirecionamento bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, apenas no VDA é necessária uma configuração de navegador com suporte. Por outro lado, ao redirecionar URLs do cliente para um VDA, apenas no cliente é necessária uma configuração de navegador com suporte. Os URLs redirecionados são transferidos para o navegador padrão configurado na máquina de destino, o cliente ou o VDA, dependendo da direção. Não é necessário usar o mesmo tipo de navegador no VDA e no cliente.
- Verifique se as regras de redirecionamento não resultam em uma configuração em loop. Por exemplo, uma política de VDA é definida para redirecionar o `https://www.citrix.com` e

a política de cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Somente URLs do protocolo HTTP/HTTPS têm suporte. Não há suporte para encurtadores de URL.
- 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, o URL redirecionado será aberto em uma nova guia. Caso contrário, o URL será aberto em uma nova janela do navegador.
- O redirecionamento de conteúdo bidirecional não funciona quando o LAA (Local App Access) está ativado.

Acesso a aplicativo local e redirecionamento de URL

June 24, 2022

Introdução

O Local App Access integra perfeitamente os aplicativos do Windows instalados localmente em um ambiente de trabalho hospedado sem mudar de uma área de trabalho para outra. Com o acesso ao aplicativo local, você pode:

- Acessar aplicativos instalados localmente em um laptop, PC ou outro dispositivo físico 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 comportam como se estivessem instalados em uma área de trabalho virtual.
- Elimine 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.
- Use aplicativos como:
  - Software de videoconferência, como o GoToMeeting.
  - Aplicações especializadas ou de nicho que ainda não estão virtualizadas.
  - 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 do usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops, as sessões de desktop hospedadas usam o redirecionamento de URL para iniciar aplicativos de acesso ao aplicativo local. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de

bloqueios de URL do navegador) selecionando links incorporados dentro de um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueios, 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 aplicativos. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo do host para o cliente, que é um tipo de redirecionamento FTA (File Type Association) do servidor. Este FTA reorienta determinados 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 lista de bloqueio de URL ou suporte de lista de permissão.

Quando o acesso ao aplicativo local estiver habilitado, as URLs que são exibidas 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 ao computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento do 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 cadeias de caracteres que especificam as configurações de política de redirecionamento de URL. Para obter mais informações, consulte as Configurações da política de acesso ao aplicativo local.

Os URLs podem ser renderizados no VDA com as seguintes exceções:

- Informações sobre geografia/localidade —Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na área geográfica). Por exemplo, se o VDA for provisionado a partir 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 —Os sites que contêm conteúdo de mídia avançada, 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 o Silverlight. Este processo está em um ambiente seguro. Ou seja, os URLs que o administrador aprova são executados no cliente quando o resto dos URLs for reorientado ao VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento de FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, o aplicativo local deve 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 drive do 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 através do ICA para abrir o arquivo.

Requisitos, considerações e limitações

Damos suporte a acesso ao aplicativo local nos sistemas operacionais válidos para VDAs para SO Windows multi-sessões e para VDAs para SO Windows de sessão única. O acesso ao aplicativo local requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são compatíveis:

- Edge, versão mais recente
- Firefox, versão mais recente e versão com suporte estendido
- Chrome, versão mais recente

Leia as seguintes considerações e limitações ao usar o acesso a aplicativos locais e o redirecionamento de URL.

- O acesso ao aplicativo local foi concebido para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o acesso ao aplicativo local com uma área de trabalho virtual executada no modo janela ou que não cobre todos os monitores.
  - Vários monitores —Quando um monitor é maximizado, ele se torna a área de trabalho padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo se os aplicativos subsequentes tipicamente começarem em outro monitor.
  - O recurso suporta um VDA. Não há integração com vários VDAs simultâneos.
- Alguns aplicativos podem se comportar inesperadamente, afetando os usuários:
  - As letras da unidade podem confundir usuários, como a unidade C: local em vez de área de trabalho virtual C:.
  - As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
  - Os aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados pelo cliente.
  - Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).
  - Os aplicativos locais aparecem com o tema Windows da máquina local.

  - Os aplicativos de tela cheia não têm suporte. Esses aplicativos incluem aplicativos que se abrem para uma tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem toda a área de trabalho.
  - O acesso ao aplicativo local copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
  - Os aplicativos que personalizam como a ordem de janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
  - Os atalhos não têm suporte, incluindo Meu computador, Lixeira, Painel de controle, atalhos da unidade de rede e atalhos de pasta.
  - Os seguintes arquivos e tipos de arquivo não têm suporte: tipos de arquivos personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
  - O agrupamento da barra de tarefas não tem suporte o para aplicativos mistos de 32 bits e 64 bits hospedados no cliente ou VDA. Ou seja, agrupando aplicativos locais de 32 bits com aplicativos VDA de 64 bits.
  - Os aplicativos não podem ser iniciados por meio de COM. Por exemplo, se você clicar em um documento do Office incorporado dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local será malsucedida.

- Cenários de salto duplo, em que um usuário está iniciando uma área de trabalho virtual a partir de outra sessão de desktop virtual, não têm suporte.
- O redirecionamento de URL suporta apenas URLs explícitas (isto é, URLs que aparecem na barra de endereços do navegador ou encontrados usando a navegação no navegador, dependendo do navegador).
- O redirecionamento de URL funciona apenas com sessões de área de trabalho, não com sessões de aplicativos.
- A pasta local da área de trabalho em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução local se comportam de acordo com as configurações da barra de tarefas estabelecidas para a área de trabalho virtual. No entanto, os atalhos para aplicativos em execução local 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 da área de trabalho, os aplicativos podem não ser iniciados de forma uniforme por meio desses atalhos.
- Se você definir a configuração de política **Allow local app access** como **Enabled**, o redirecionamento de conteúdo do navegador não tem suporte.

Interação com o Windows

A interação acesso ao aplicativo local 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 de acesso ao aplicativo local.
  - Os arquivos de imagem e vídeo são abertos por padrão por meio do aplicativos da loja do Windows. No entanto, o acesso ao aplicativo local enumera os aplicativos de armazenamento do Windows e abre atalhos com aplicativos de desktop.
- Programas Locais
  - No Windows 7, a pasta está disponível no menu Iniciar.
  - No Windows 8, os Programas Locais só estão disponíveis quando o usuário escolhe **All Apps** 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 estão restritos à área de trabalho e são cobertos pela tela inicial e pelos aplicativos de estilo do Windows 8.
  - Os aplicativos Local App Access não se comportam como aplicativos de desktop no modo multi-monitor. No modo multi-monitor, a tela Iniciar e a área de trabalho são exibidos em monitores diferentes.
- Windows 8 e redirecionamento de URL de acesso ao aplicativo local
  - Como o Windows 8 Internet Explorer não tem complementos habilitados, use o Internet Explorer para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desativa os complementos por padrão. Para implementar o redirecionamento de URL, desative 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 o acesso ao aplicativo local e o 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 no computador cliente local. Você pode habilitar ambos os recursos durante a instalação do aplicativo Citrix Workspace ou habilitar o modelo Acesso a aplicativos locais usando o editor de política de grupo.

- Defina a configuração **Allow local app access** como **Enabled**. Você também pode configurar configurações de política de lista de permissão de URL e lista de bloqueios para redirecionamento de URL. Para obter mais informações, consulte as Configurações da política de acesso ao aplicativo local.

Habilitar o acesso a aplicativo local e redirecionamento de URL

Para habilitar o acesso ao aplicativo local para todos os aplicativos locais, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **Policies** no painel esquerdo.
2. Selecione **Create Policy** na barra de ações.
3. Na janela Criar política, digite "Allow Local App Access"na caixa de pesquisa e clique em **Select**.
4. Na janela Edit Setting, selecione **Allowed**. Por padrão, a política **Allow local app access** 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 devem estar ativados 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 todo o computador e à política de redirecionamento de URL.
5. Na janela Criar política, digite "URL redirection allow list"na caixa de pesquisa e clique em **Select**. A lista de permissões de redirecionamento de URL especifica as URLs que devem ser abertas no navegador padrão da sessão remota.
6. Na janela Edit setting, clique em **Add** para adicionar os URLs e clique em **OK**.
7. Na janela Create Policy, digite "URL redirection block list"na caixa de pesquisa e clique em **Select**. A lista de bloqueios de redirecionamento de URL especifica URLs que são redirecionados para o navegador padrão em execução no ponto de extremidade.
8. Na janela Edit setting, clique em **Add** para adicionar os URLs e clique em **OK**.
9. Na página Settings, clique em **Next**.
10. Na página Users and Machines, atribua a política aos grupos de entrega aplicáveis e clique em **Next**.
11. Na página Summary, revise as configurações e clique em **Finish**.

Para habilitar o redirecionamento de URL para todos os aplicativos locais durante a instalação do aplicativo Citrix Workspace, siga as etapas abaixo:

1. Ative o redirecionamento de URL ao instalar o aplicativo Citrix Workspace para todos os usuários em um computador. 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 Acesso ao aplicativo local usando o editor de política de grupo

> **Nota:**
>
> - Antes de ativar o modelo 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 a Introdução e procure pelo *modelo administrativo do objeto de política de grupo*.
> - Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Administrative Templates > Citrix Components > Citrix Workspace** somente quando você adiciona `CitrixBase.admx/CitrixBse.adml` à pasta %systemroot%\policyDefinitions.

Para habilitar o modelo acesso ao aplicativo local usando o editor de política de grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá até **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User Experience**.
3. Clique em **Local App Access settings**.
4. Selecione **Enabled** e depois selecione **Allow URL Redirection**. Para redirecionamento de URL, registre complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais abaixo neste artigo.

Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o PowerShell SDK.

Para o Editor do Registro, consulte O Local App Access para aplicativos publicados na lista de recursos gerenciados através do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina em que o Delivery Controller está sendo executado.
2. Digite o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEn "-value "true"`.

Para ter acesso a **Add Local App Access Application** em uma implantação do Citrix DaaS, use o SDK do PowerShell remoto do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte SDK do PowerShell remoto 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. Digite o seguinte comando: `set-configsitemetadata -name “studio_clientHostedAppsEn” -value “true”`.

Depois de concluir as etapas anteriores aplicáveis, siga estas etapas para continuar.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo.
2. No painel central superior, clique com o botão direito do mouse na área em branco e selecione **Add Local App Access Application** do menu. Você também pode clicar em **Add Local App Access Application** no painel Actions. Para exibir a opção Add Local App Access Application no painel Actions, clique em **Refresh**.
3. Publique o aplicativo Local App Access.

   - O assistente de Acesso a Aplicativos Locais é iniciado com uma página Introdução, que você pode remover de inicializações futuras do assistente.
   - O assistente orienta você pelas páginas Groups, Location, Identification, Delivery e Summary descritas abaixo. Quando terminar cada página, clique em **Next** até chegar à página Summary.
   - Na página Groups, selecione um ou mais grupos de entrega onde os novos aplicativos serão adicionados e clique em **Next**.
   - Na página Location, 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 Identification, aceite os valores padrão ou digite as informações desejadas e clique em **Next**.
   - Na página Delivery, configure como esse aplicativo é fornecido aos usuários e 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 estará visível no menu Iniciar, na área de trabalho ou em ambos.
   - Na página Summary, revise as configurações e clique em **Finish** para sair do assistente Local Application Access.

Registrar complementos do navegador

> **Nota:**
>
> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente quando você instala 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: <*client-installation-folder*>\redirector.exe /reg<*navegador*r>
- Para cancelar o registro de complementos em um dispositivo cliente: <*client-installation-folder*>\redirector.exe /unreg<*navegador*>
- Para registrar complementos em um VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*navegador*>
- Para cancelar o registro de complementos em um VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*navegador*>

Onde <*navegador*> é Internet Explorer, Firefox, Chrome ou All.

Por exemplo, o comando a seguir registra complementos do Internet Explorer em um dispositivo que executa o aplicativo Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

O comando a seguir registra todos os complementos em um VDA com SO multissessão 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 bloqueios, mas o navegador ou site o redireciona para outro URL, o URL final não será redirecionado. Ele não é redirecionado mesmo se estiver na lista de bloqueios.

Para que o redirecionamento de URL funcione corretamente, ative o complemento quando solicitado pelo navegador. Se os complementos que estão usando as opções da Internet ou os complementos no prompt estiverem desativados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam os URLs.

Quando um complemento é instalado, o Firefox avisa para permitir ou impedir a instalação do complemento em uma nova página de guias. Permita que o complemento do recurso funcione.

- O complemento do Chrome sempre redireciona a URL final que é navegada e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desabilita 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 no logoff e na desconexão

> **Nota:**
>
> Se você não seguir estas etapas para configurar as configurações, 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 serão reintegrados se estiverem disponíveis na área de trabalho virtual.

Para configurar o comportamento do aplicativo local no logoff e na desconexão, consulte Comportamento do aplicativo local no logoff e na desconexão na lista de recursos gerenciados através do registro.

Considerações genéricas de redirecionamento USB e unidade de cliente

August 17, 2023

A tecnologia HDX fornece **suporte otimizado** para a maioria dos dispositivos USB mais difundidos. 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 têm suporte otimizado ou quando este é inadequado.

- O dispositivo USB tem 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 equipamentos 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 do 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 fornece suporte otimizado para esse tipo de dispositivo USB.

Com 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 suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as Configurações de política de dispositivos USB Citrix para o redirecionamento USB genérico e suporte otimizado.
> - A configuração de política Citrix nas Regras de otimização do dispositivo USB do cliente é uma configuração específica para o redirecionamento USB genérico, para um dispositivo USB específico. Não se aplica ao suporte otimizado conforme descrito aqui.
> - Ao intermediar uma sessão a uma Máquina Virtual do Azure usando o software Citrix, a Citrix fornece o melhor suporte possível para o redirecionamento USB à Máquina Virtual do Azure. Damos suporte à correção de problemas com o 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 e a largura de banda da rede 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 com links de baixa largura de banda de alta latência. Use suporte otimizado sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para que possam ser usados, por exemplo, um mouse 3D (usado com aplicativos 3D que normalmente também exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você pode ser capaz de 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 as Configurações da política de largura de banda, para o redirecionamento de dispositivo USB do cliente, e Configurações de políticas de conexões multistream.

Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartões inteligentes, leitores de impressões digitais e mesas gráficas para assinatura. Outros dispositivos USB,

como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser sensíveis.

Dispositivos USB são usados frequentemente para distribuir malware. A configuração do aplicativo Citrix Workspace e do Citrix Virtual Apps and Desktops pode reduzir, mas não eliminar, os riscos desses dispositivos USB. Esta situação se aplica se for usado o redirecionamento USB genérico ou suporte otimizado.

> **Importante:**
>
> Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX usando TLS ou IPsec.
>
> Ative apenas o suporte 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 uso seguro de dispositivos USB:
>
> - Use apenas dispositivos USB obtidos a partir de uma fonte confiável.
> - Não deixe dispositivos USB desacompanhados em ambientes abertos - por exemplo, uma unidade flash em um internet café.
> - Explique os riscos de usar um dispositivo USB em mais de um computador.

Compatibilidade com redirecionamento USB genérico

O redirecionamento USB genérico é suportado para dispositivos USB 2.0 e anteriores. O redirecionamento USB genérico também é suportado para dispositivos USB 3.0 conectados a uma porta USB 2.0 ou USB 3.0. O redirecionamento USB genérico não suporta recursos USB introduzidos no USB 3.0, como super velocidade.

Esses aplicativos do Citrix Workspace oferecem suporte ao redirecionamento USB genérico:

- Aplicativo Citrix Workspace para Windows, consulte Configuração da entrega de aplicativos.
- Aplicativo Citrix Workspace para Mac, consulte Aplicativo Citrix Workspace para Mac.
- Aplicativo Citrix Workspace para Linux, consulte Otimizar.
- Aplicativo Citrix Workspace para Chrome OS, consulte Aplicativo Citrix Workspace para Chrome.

Para ver as 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 que o redirecionamento USB genérico tem suporte. Consulte a documentação do aplicativo Citrix Workspace para saber sobre as restrições aos tipos de dispositivos USB compatíveis.

O redirecionamento USB genérico é suportado para sessões de desktop do VDA para o sistema operacional de sessão única versão 7.6 até a atual.

O redirecionamento USB genérico tem suporte para sessões de desktop do VDA para a versão 7.6 do SO multissessão até a atual, com estas restrições:

- O VDA deve estar executando o Windows Server 2012 R2, o Windows Server 2016, o Windows Server 2019 ou o Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o RDSH (Remote Desktop Session Host) para o sistema operacional VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não têm suporte para 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 manipulados individualmente.
- Portas USB COM virtuais. Use o redirecionamento da porta COM em vez de redirecionamento USB genérico.

Para obter informações sobre dispositivos USB que foram testados com 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 Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações da política de dispositivos USB na referência de configurações de políticas
- No aplicativo Citrix Workspace, usando mecanismos dependentes de aplicativos do Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações do 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 outros. Para obter mais informações, consulte Configure na documentação do aplicativo Citrix Workspace para Windows.

Esta configuração separada fornece 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.

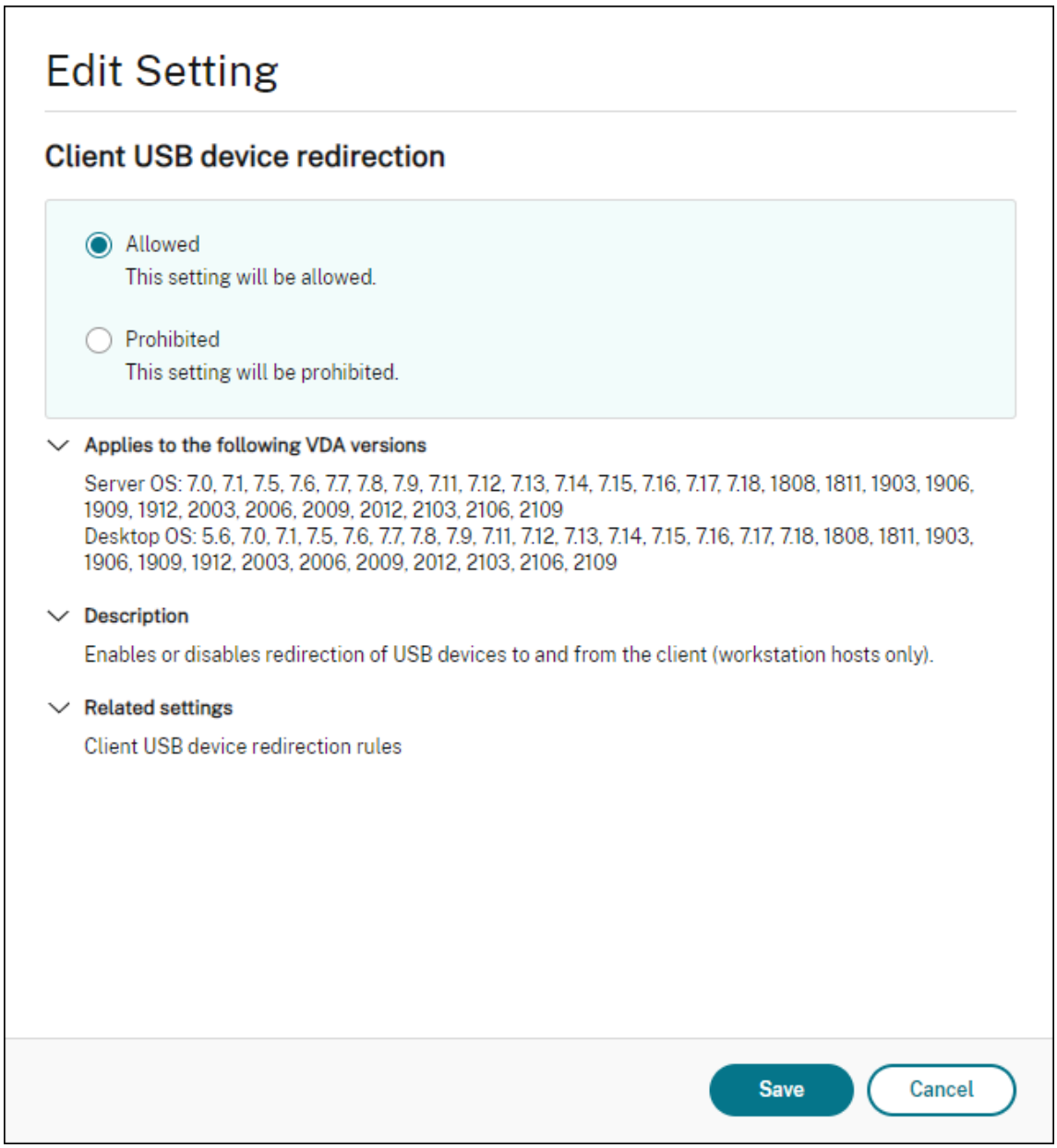
- As configurações de política do Citrix podem controlar dispositivos USB permitidos apenas para determinados usuários ou para usuários que se conectam somente por uma LAN (em vez de usar o Citrix Gateway).

Enable generic USB redirection

Para habilitar o redirecionamento USB genérico e não exigir o redirecionamento manual pelo usuário, faça as configurações de política Citrix e as preferências de conexões do aplicativo Citrix Workspace.

Nas configurações da política Citrix:

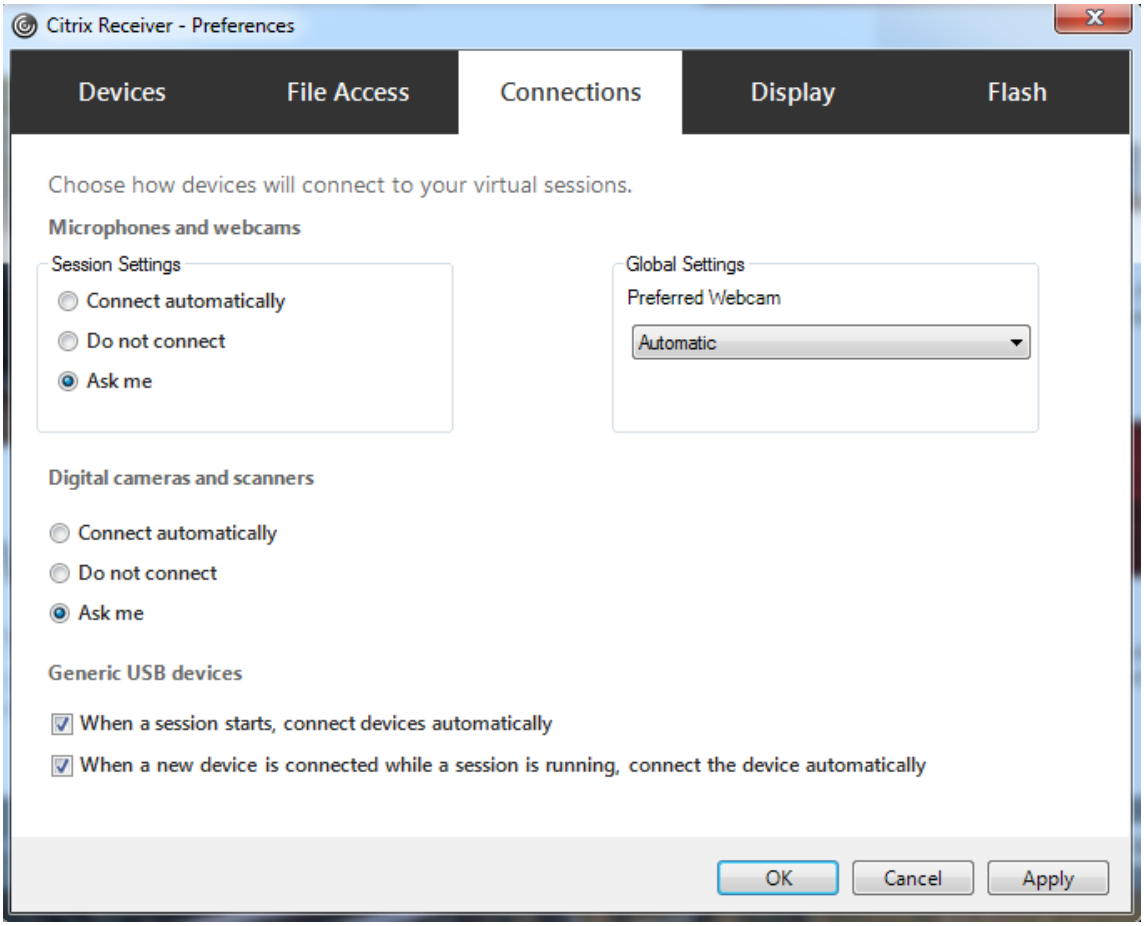
1. Adicione Client USB device redirection a uma política e defina seu valor como **Allowed**.



2. (Opcional) Para atualizar a lista de dispositivos USB disponíveis para redirecionamento, adicione a configuração Client USB device redirection rules a uma política e especifique as regras de política USB.

   No aplicativo Citrix Workspace

3. Especifique se os dispositivos são conectados automaticamente sem redirecionamento manual. Você pode fazer isso usando um modelo administrativo ou no aplicativo Citrix Workspace para Windows > Preferences > Connections.



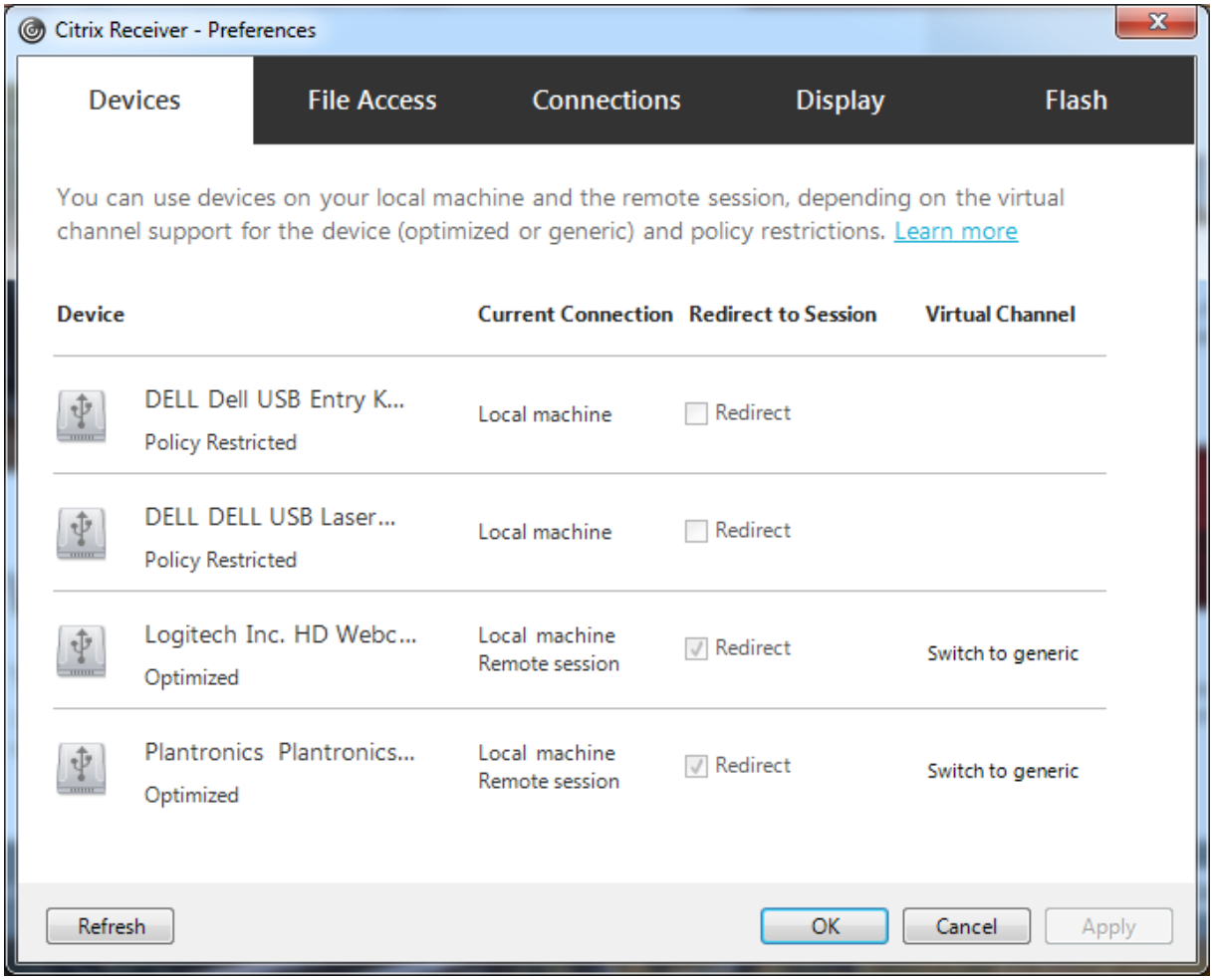
Se você especificou as regras de política USB para o VDA na etapa anterior, especifique as mesmas regras de política para o aplicativo Citrix Workspace.

Para clientes finos, consulte o fabricante para obter detalhes sobre o suporte USB e a configuração necessária.

Configuração dos 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 são 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 da ajuda do usuário do aplicativo Citrix Workspace para Windows Exibir seus dispositivos no Desktop Viewer.



Para usar o redirecionamento USB genérico em vez de suporte otimizado, você pode:

- No aplicativo Citrix Workspace, selecione manualmente o dispositivo USB para usar o redirecionamento USB genérico, escolha **Switch to generic** na guia Devices da caixa de diálogo Preferences.

- 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 automaticamente dispositivos USB. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

> **Nota:**
>
> Apenas configure o redirecionamento USB genérico para uso com uma webcam se a webcam for considerada incompatível com o redirecionamento multimídia de HDX.

Para evitar que dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e para o VDA.

Para redirecionamento USB genérico, você precisa saber pelo menos a classe de dispositivo USB e a subclasse. Nem todos os dispositivos USB usam sua classe de dispositivo USB e subclasse óbvias. Por exemplo:

- As canetas usam a classe dispositivo mouse.
- Os leitores de cartões inteligentes podem usar a classe de dispositivo definido 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 do dispositivo USB que não correspondem ao uso pretendido. As regras do dispositivo não se destinam a impedir esse comportamento.

Você controla os dispositivos USB disponíveis para redirecionamento USB genérico especificando regras de redirecionamento de dispositivos USB para o aplicativo VDA e Citrix Workspace, para substituir as regras de política USB padrão.

Para o VDA:

- Edite as regras de substituição do administrador para os computadores do SO multi-sessão 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

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 através da política de grupo do Active Directory:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado 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 estas regras padrão do produto. Em vez disso, use-os como um guia para criar regras de substituição de 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\Generic
As regras de política de GPO assumem o formato **{Allow: | Deny:}** seguido por um conjunto de expressões *tag=value* separadas por espaço em branco.

As seguintes marcas têm suporte:

Marca	Descrição
VID	ID do fornecedor do descritor de dispositivo
PID	ID do produto do descritor do dispositivo
REL	Liberar ID do descritor de dispositivo
Class	Classe do descritor de dispositivo ou de um descritor de interface; consulte o site USB em http://www.usb.org/ para códigos de classe USB disponíveis
SubClass	Subclasse do descritor de dispositivo ou de um descritor de interface
Prot	Protocolo do descritor de dispositivo ou de um descritor de interface

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas e minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por #. Não é obrigatório usa delimitador, e o comentário é ignorado para fins de correspondência.

- As linhas em branco ou puramente de comentários são ignoradas.
- O espaço em branco é usado como separador, mas não pode 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 marcas devem usar o operador correspondente =. 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 redirecionando corretamente, você pode tentar resolver o problema aguardando para conectar o dispositivo até que a sessão virtual seja 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

É fornecido suporte otimizado para dispositivos de armazenamento em massa USB. Esse suporte faz parte do mapeamento da unidade cliente Citrix Virtual Apps and Desktops. As unidades no disposi-

tivo do usuário são mapeadas automaticamente para letras de unidades 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 da unidade cliente, use a configuração **Client removable drives**. Essa configuração está na seção Configurações da política de redirecionamento de arquivos das configurações de política ICA.

Com dispositivos USB de armazenamento em massa, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados pelas políticas da Citrix. Controle-os usando as políticas Citrix. As principais diferenças são:

Recurso	Client drive mapping	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 de o dispositivo ser acessado	Sim
Dispositivos BitLocker To Go	Não	Não
Exclusão segura do dispositivo durante uma sessão	Não	Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura

Se o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estiverem ativados e um dispositivo de armazenamento em massa for inserido antes ou depois que uma sessão seja iniciada, ele será redirecionado por meio do mapeamento da unidade cliente. Quando o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estão ativadas e um dispositivo é configurado para redirecionamento automático e um dispositivo de armazenamento em massa é inserido antes ou depois que uma sessão seja iniciada, ele é redirecionado por meio do redirecionamento USB genérico. Para obter mais informações, consulte o artigo do Knowledge Center CTX123015.

> **Nota:**
>
> O redirecionamento USB tem suporte em conexões de largura de banda mais baixa, por exemplo, 50 Kbps. No entanto, copiar arquivos grandes não funciona.

Gerenciar

July 7, 2022

A Citrix gerencia as implantações de serviços do Citrix Virtual Apps and Desktops instalando e mantendo os principais componentes e recursos do Citrix Cloud.

Você cuida das máquinas (VDAs) em locais de recursos que fornecem aplicativos e desktops. Você também gerencia conexões com esses locais de recursos, além de aplicativos, áreas de trabalho e usuários.

- **AutoScale:** Uma solução uniforme e de alto desempenho para gerenciar proativamente suas máquinas.
- **Aplicativos:** Gerencie aplicativos em grupos de entrega.
- **IP virtual e loopback virtual:** O recurso de endereço IP virtual da Microsoft fornece um aplicativo publicado com um endereço IP atribuído dinamicamente e exclusivo para cada sessão. Com o recurso de loopback virtual da Citrix, você pode configurar aplicativos que dependem das 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 do Cloud Connector usando vários métodos, descritos neste artigo. À medida que você adiciona Cloud Connectors, os VDAs precisam ter informações atuais.
- **Sessões:** Manter a atividade da sessão é fundamental para oferecer a melhor experiência de usuário. Vários recursos podem otimizar a confiabilidade das sessões e reduzir transtornos, tempo de inatividade e perda de produtividade.
- **Uso da pesquisa:** Para exibir informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou grupos de entrega na interface de gerenciamento Full Configuration, use o recurso de pesquisa flexível.
- **Suporte a IPv4/IPv6:** O Citrix Virtual Apps and Desktops oferece suporte a implantações de IPv4 puro, IPv6 puro e pilha dupla que usam redes IPv4 e IPv6 sobrepostas. Este artigo descreve e ilustra essas implantações. Ele também descreve as configurações da política da Citrix que controlam o uso de IPv4 ou IPv6.
- **Gerenciamento de perfis:** O Citrix Profile Management pode ser instalado quando você instala um VDA. Se você usar essa solução de perfil de usuário, revise a 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 pode se comunicar com o Citrix Cloud. Também são fornecidas Considerações de escala, tamanho e outras considerações de configuração.
- **Administração delegada:** Com a administração delegada, você pode configurar as permissões de acesso de que todos os administradores precisam, de acordo com a função deles na organização.
- **Log de configuração:** O log de configuração rastreia as alterações de configuração e as atividades administrativas.
- **Logs de evento:** Os serviços dentro do Citrix Virtual Apps and Desktops registram no log os eventos que ocorrem. Os logs de eventos podem ser usados para monitorar e solucionar problemas de operação.
- **Licenças:** Você pode visualizar as informações de uso da licença Citrix para este serviço no console do Citrix Cloud.
- **Máquinas de balanceamento de carga:** Você pode controlar como balancear a carga de máquinas.

Acesso adaptativo

July 1, 2022

Com as constantes mudanças de hoje, a segurança dos aplicativos é vital para qualquer empresa. Tomar decisões de segurança fazendo o reconhecimento de contexto para habilitar o acesso aos aplicativos reduz os riscos associados, ao mesmo tempo que permite o acesso aos usuários.

O recurso de acesso Adaptativo oferece uma abordagem abrangente de acesso Confiança Zero que fornece acesso seguro aos aplicativos. O acesso adaptativo permite que os administradores forneçam acesso de 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 (desktop ou dispositivos móveis)
- Localização (geolocalização ou localização da rede)
- Postura do dispositivo (verificação da postura do dispositivo)
- Risco (pontuação de risco do usuário)

Postura do dispositivo

November 21, 2023

O serviço Citrix Device Posture é uma solução baseada em nuvem que ajuda os administradores a impor determinados requisitos que os dispositivos finais devem atender para obter acesso ao Citrix DaaS (Citrix Virtual Apps and
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

July 1, 2022

Os clientes do Citrix Cloud podem usar o Citrix Workspace para fornecer Autenticação Adaptativa ao Citrix DaaS. Autenticação Adaptativa é um serviço do Citrix Cloud que permite a autenticação avançada para clientes e usuários que efetuam login no Citrix Workspace. O serviço de Autenticação Adaptativa é um ADC gerenciado pela Citrix e hospedado no Citrix Cloud que fornece todos os recursos avançados de autenticação, como:

- Autenticação multifator usando diferentes métodos de autenticação, como AD, RADIUS, certificado, vários IdPs de terceiros usando SAML 2.0, OAuth, OIDC, Google Captcha.
- Verificação da identidade do usuário e dos níveis de autorização com base em fatores como localização, status do dispositivo e grupo de usuários.
- Permite o acesso inteligente ou contextual a DaaS (virtualizado) e SPA (recursos não virtualizados, como aplicativos Web e SaaS).
- Personalização da página de login

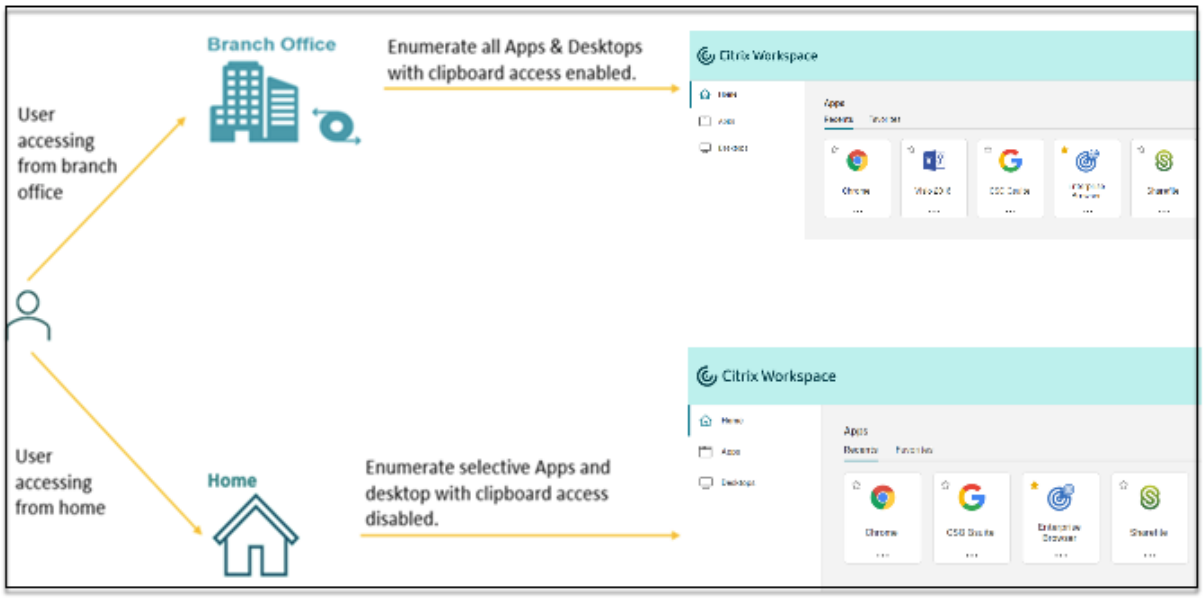
Para obter detalhes completos sobre a Autenticação Adaptativa, consulte Serviço de Autenticação Adaptativa.

Acesso adaptável com base na localização da rede do usuário

November 21, 2023

O recurso de acesso adaptável do Citrix Workspace usa infraestrutura de políticas avançadas para permitir o acesso ao Citrix DaaS com base na localização da rede do usuário. O local é definido usando o intervalo de endereços IP ou endereços de sub-rede.

Os administradores podem definir políticas para enumerar ou não enumerar áreas de trabalho e aplicativos virtuais com base na localização da rede do usuário. Os administradores também podem controlar as ações do usuário habilitando ou desabilitando o acesso à área de transferência, impressoras, mapeamento de unidades cliente e outros recursos, com base no local da rede do usuário. Por exemplo, os administradores podem configurar políticas para que os usuários que acessam os recursos em casa tenham acesso limitado aos aplicativos, e os usuários que acessam os recursos das filiais tenham acesso total.



Um administrador pode implementar as seguintes políticas para acessar os aplicativos:

- Enumerar alguns aplicativos confidenciais somente do local corporativo ou de suas filiais.
- Não enumerar aplicativos confidenciais se os funcionários estiverem acessando o espaço de trabalho de uma rede externa.
- Desativar o acesso à impressora 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 Adaptive Access está disponível para os clientes com as seguintes licenças.

- Implantação do Citrix DaaS com acesso por meio da plataforma Citrix Workspace.
- DaaS Premium/Premium Plus
- Secure Private Access Advanced

Pré-requisitos

- Certifique-se de que o recurso **Adaptive Access** esteja ativado em (**Citrix Workspace Access > Adaptive Access**). Para obter detalhes, consulte Ativar o recurso Adaptive Access.

  Quando o acesso adaptável está ativado, as políticas de acesso do DaaS são atualizadas para usar a opção **Connections through Citrix Gateway**.

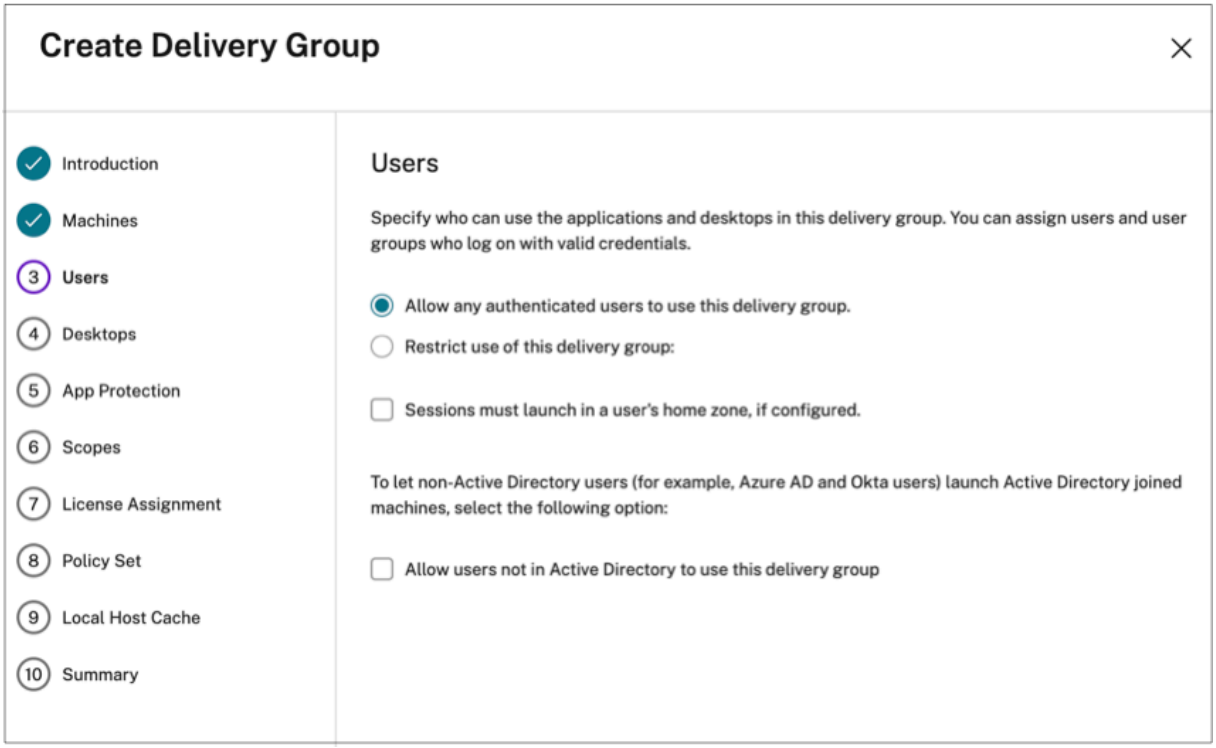
  > **Nota:**
  >
  > O NetScaler Gateway é necessário para adicionar tags de acesso inteligentes nas políticas de acesso do DaaS. No entanto, como o DaaS consome tags dos serviços Device Posture, Adaptive Access e Adaptive Authentication, não é necessário ter um NetScaler Gateway configurado em sua configuração.

- Compreensão das marcas de localização. Para obter detalhes, consulte Marcas de localização de rede.

Pontos a serem observados

Os pontos a seguir só são aplicáveis se você quiser restringir a enumeração de aplicativos com base na localização. Se você planeja usar o acesso adaptável para restringir os controles do usuário, como desabilitar o acesso à área de transferência, redirecionamento de impressora ou mapeamento de unidade cliente, com base na localização da rede, você pode ignorar essas diretrizes.

- Ao criar um grupo de entrega, se você selecionar a opção **Leave user management to Citrix Cloud**, você não poderá aplicar políticas de acesso inteligente (por exemplo, acesso adaptável ao Citrix DaaS com base na localização da rede). Isso ocorre porque os grupos de entrega se tornam ofertas de biblioteca e, portanto, não são gerenciados pelo Web Studio.
- Se você planeja enumerar o Citrix DaaS seletivamente com base na localização da rede, o gerenciamento de usuários desses grupos de entrega deve ser realizado usando as políticas do Citrix Studio em vez do espaço de trabalho. Ao criar um grupo de entrega, em **Users setting**, escolha **Restrict use of this Delivery Group** ou **Allow any authenticated users to use this Delivery Group**. Isso permite que você configure o acesso adaptável na guia **Access Policy** em **Delivery Group**.

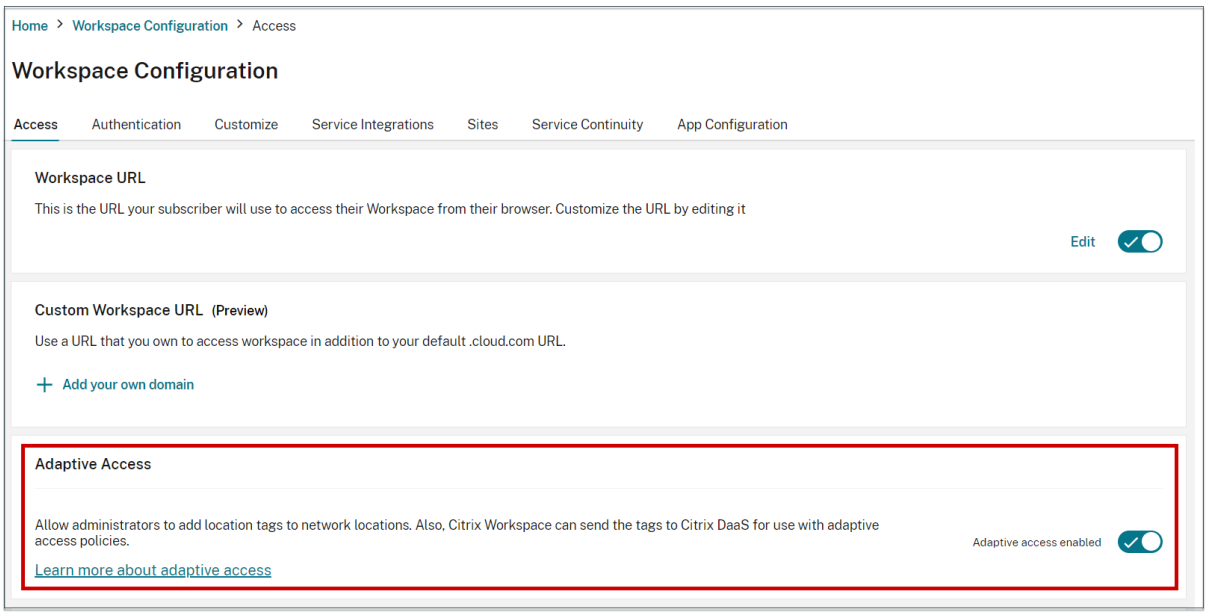


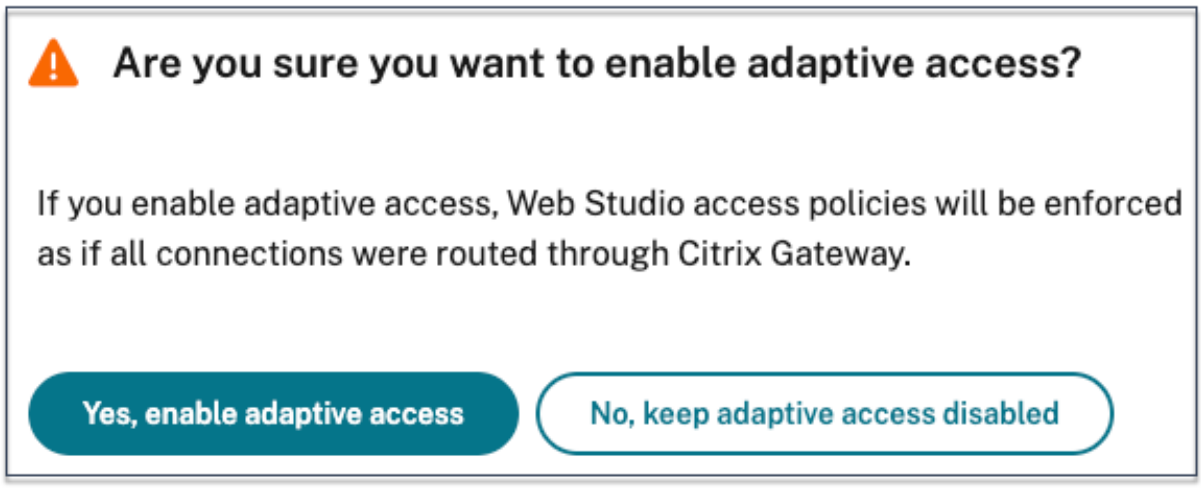
- Muda para Direct Workload Connection quando o acesso adaptável está ativado.
  - O campo **Location tags** fica visível em **Citrix Cloud > Network Locations > Add a Network Location > Location tags**.
  - As políticas Direct Workload Connection existentes funcionam conforme o esperado.
  - Novas políticas devem ser criadas no serviço Network Locations (sem definir tags) e também no grupo de entrega. Além disso, o tipo de conectividade de rede deve ser **Internal**.
  - Para novas políticas de Direct Workload Connection com marcações, as tags devem ser definidas no serviço Network Locations, e as mesmas tags 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 **Internal**. As marcações de localização não são relevantes para o Direct Workload Connection.
- O seguinte é recomendado ao testar sua implantação do Citrix DaaS.
  - Identifique um grupo de entrega de teste ou crie um grupo de entrega para implementar o recurso.
  - Crie uma política ou identifique uma política que pode ser usada com um grupo de entrega de teste.

Ativar o recurso Adaptive Access

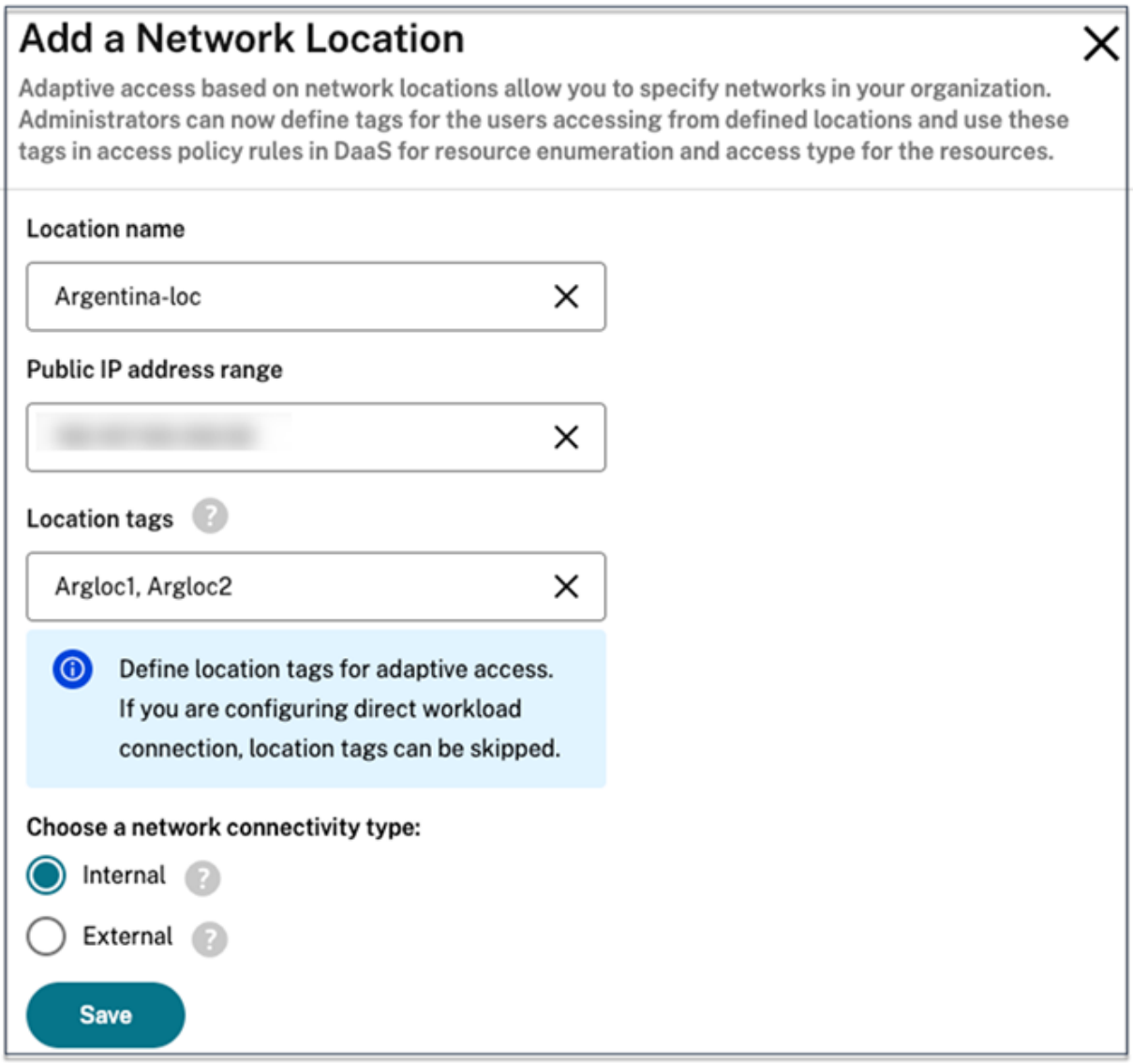
1. Faça logon no Citrix Cloud.

2. Selecione **Workspace Configuration** no menu de hambúrguer.
3. A opção **Adaptive Access** está desativada, por padrão. Ative o botão de alternância **Adaptive Access**.
4. Clique em **Yes, enable adaptive access** na mensagem de confirmação.

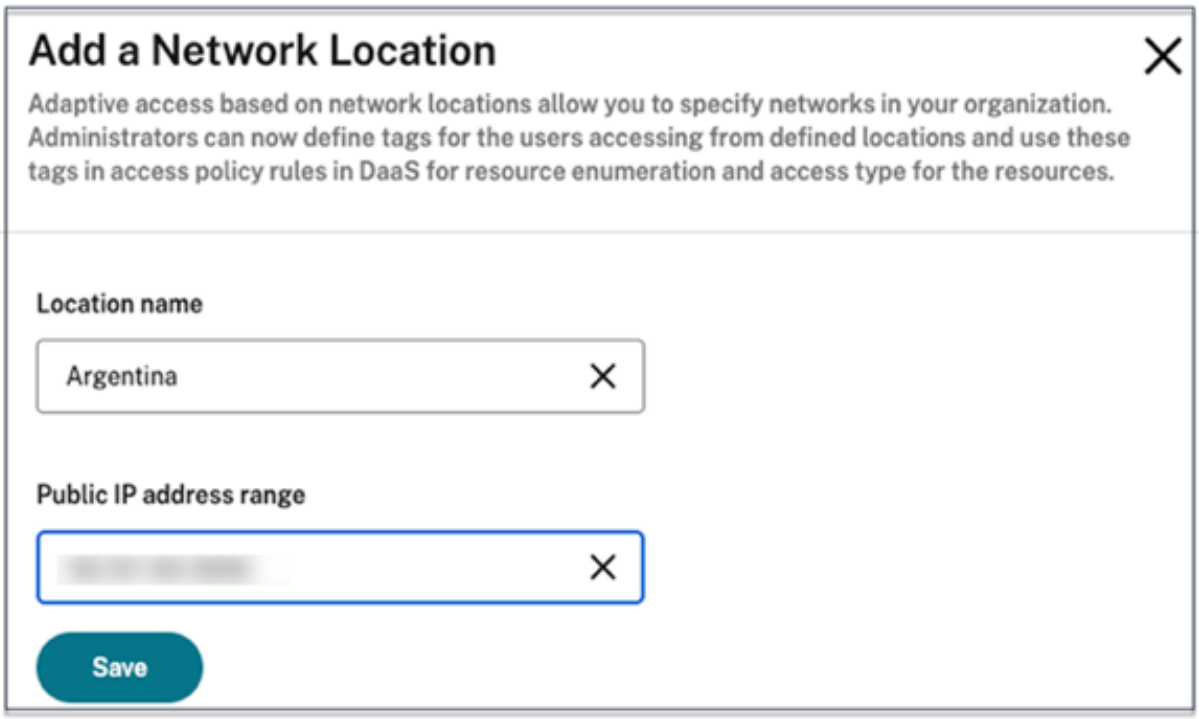




Quando o acesso adaptável está ativado, você pode definir as marcações de localização para o acesso adaptável (**Citrix Cloud > Network Locations > Add a Network Location > Location tags**).

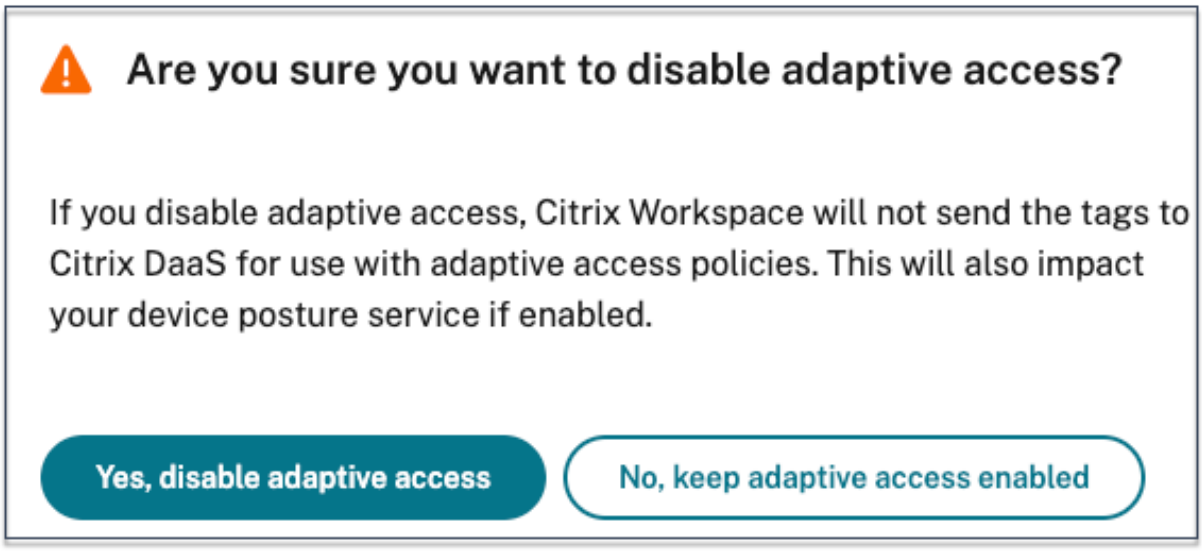


Quando o acesso adaptável está desativado, você não pode adicionar um local de rede. Nesse caso, as marcações de localização não são aplicáveis.



Importante:

Quando você tenta desativar o recurso Adaptive Access, a seguinte mensagem é exibida. Observe que o Workspace não envia as tags ao DaaS para o acesso adaptável quando o recurso está desativado.



Configurar o acesso adaptável

A configuração do acesso adaptável com base nas localizações de rede envolve as seguintes etapas de alto nível.

1. Defina as políticas de localização da rede
2. Defina as tags no DaaS Studio

Para exemplificar a configuração, dois tipos de usuário (usuários **BrancOffice** e usuários **WorkFromHome**) são selecionados para realizar o seguinte caso de uso.

- Os usuários BranchOffice devem poder acessar os aplicativos com todo o acesso.
- Os usuários WorkFromHome não devem ter acesso à área de transferência.

Nesse exemplo de configuração, **Home** e **Office** são usados como tags de marcação nos exemplos.

Configurar políticas de localização de rede

1. Faça login no Citrix Cloud.
2. Selecione **Network Locations** no menu de hambúrguer.
   Certifique-se de que a opção Adaptive Access esteja ativada. Caso contrário, a interface do usuário de Direct Workload Connection será exibida.
3. Clique em **Add network location**.
   - **Location name:** insira um nome apropriado para a política.

     Exemplo: BranchOffice ou WorkFromHome
   - **Public IP address range:** defina o intervalo de endereços IP públicos da sua rede.

     Exemplo: 172.9.2.1-172.9.2.30
   - **Location Tags:** defina as marcações da sua localização. Pode ser um nome que faça referência à sua localização. Essas marcas são usadas para configurar as políticas de acesso adaptável no Citrix Studio. Para obter detalhes, consulte **Definir marcações no Citrix Studio**.

     Exemplo: *Office* ou *Home*
   - **Connectivity type:** defina o tipo de inicialização do aplicativo.

   Internal –ignorar gateway ao iniciar aplicativo.
   External –usar serviço Citrix Gateway ou gateway tradicional ao iniciar aplicativo.
4. Clique em **Salvar**.

Agora você pode usar essas marcações no DaaS Studio para habilitar o acesso adaptável.

Definir marcações no Citrix Studio

Neste exemplo, as marcações são definidas nos grupos de entrega para restringir a enumeração do aplicativo dos usuários. Dois grupos de entrega são criados.

- Grupo de entrega de acesso adaptável —Para os usuários da localização **BranchOffice**. Esses usuários devem ver todos os aplicativos desse grupo de entrega.
- Grupo de entrega WFH —Para os usuários do local **WorkFromHome**. Esses usuários devem ver os aplicativos desse grupo de entrega.

1. Faça login no Citrix Cloud.
2. No bloco **Citrix DaaS**, clique em **Manage**.
3. Criar um grupo de entrega. Para obter detalhes, consulte Criar grupos de entrega.
4. Selecione o grupo de entrega que você criou e clique em **Edit Delivery Group**.
5. Clique em **Access Policy**.
6. Clique em **Add** e selecione o seguinte:

   - Farm: **Workspace**
   - Filter: **LOCATION_TAG_OFFICE**

   Da mesma forma, você pode criar uma marcação para o grupo de entrega WFH.
7. Clique em **Add** e selecione o seguinte:

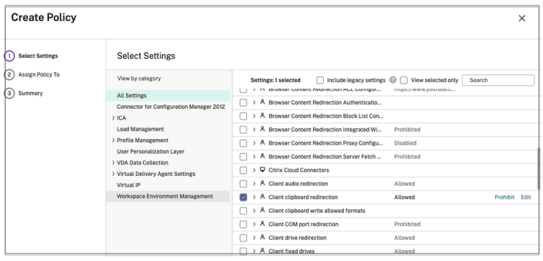
   - Farm: Workspace
   - Filter: **LOCATION_TAG_HOME**

Agora você pode usar essas marcações para restringir o acesso aos aplicativos.

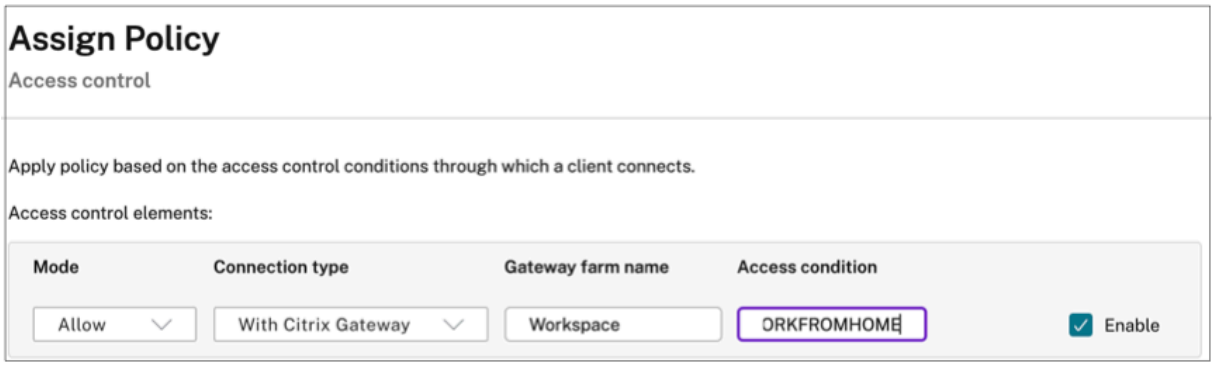
Restringir o acesso aos aplicativos

Neste exemplo, o redirecionamento da área de transferência do cliente está desativado para usuários do local WorkFromHome.

1. Faça login no Citrix DaaS.
2. Vá para **Policies** e clique **Create Policy**.
3. Selecione **Client clipboard redirection** e clique em **Prohibit**.
4. Clique em **Next**.



1. Na página Assign policy, selecione **Access control**.
2. Defina os seguintes valores para a política:
   - Mode: **Allow**
   - Connection type: **With Citrix Gateway**
   - Gateway farm name: **Workspace**
   - Access Condition: **LOCATION_TAG_HOME** (tudo em maiúsculas)



1. Clique em **Next**.
2. Insira um nome para a política e adicione uma descrição da política.
3. Clique em **Finish**.

Os usuários do local **WorkFromHome** não podem acessar a área de transferência aos recursos iniciados.

Marcações de localização de rede

O serviço Network Locations fornece as seguintes tags de marcação.

- **Tags padrão:** essas tags são definidas no serviço Network Locations. As seguintes tags padrão estão disponíveis.
  - **Location_internal:**** tag enviada por padrão quando o tipo de conectividade de rede é definido como INTERNAL**.
  - **Location_external:**** tag enviada por padrão quando o tipo de conectividade de rede é definido como EXTERNAL**.

  - **Location_undefined:** tag enviada a um endereço IP que não está definida na política, mas está vindo por meio do serviço Network Locations. A inicialização para esses usuários é a mesma definida no grupo de recursos.

- **Tags personalizadas:** os administradores podem definir o nome das tags personalizadas nas políticas. Exemplo: office, home, branch

Exemplos:

Tags padrão: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Tags personalizadas: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Observação:**
>
> Ao definir tags para o serviço Network Location, assegure-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.

Problemas conhecidos

Se você desativar o recurso Adaptive Access depois de ter sido ativado e as regras definidas (marcações e tipo de conectividade), isso não remove os locais da página Network Locations, embora as marcações de localização e as colunas de tipo de conectividade estejam ocultas. Mas esses locais estão desativados no back-end. Isso é um problema superficial.

Pacotes de aplicativos

July 4, 2023

A Microsoft fornece três tecnologias de empacotamento para entregar aplicativos aos usuários: App-V, MSIX e anexação de aplicativo MSIX. Este artigo explica como implantar e entregar esses pacotes de aplicativos em seu ambiente Citrix DaaS:

- Implementar e entregar aplicativos App-V
- Implementar e entregar aplicativos MSIX e de anexação de aplicativo MSIX

Implementar e entregar aplicativos App-V

Esta seção aborda as seguintes informações:

- Visão geral. Descreve os métodos de gerenciamento que o Citrix DaaS usa para entregar e gerenciar os pacotes do App-V.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

Esta seção descreve os métodos de gerenciamento que o Citrix DaaS usa para entregar e gerenciar os pacotes do App-V. Para obter mais informações sobre os componentes e conceitos com os quais você interage ao entregar aplicativos empacotados do App-V, consulte a documentação da Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

O Citrix DaaS entrega e gerencia pacotes App-V usando os seguintes métodos:

- **Administração dupla**. Os pacotes de aplicativos são configurados e gerenciados em servidores App-V. O Citrix DaaS e os servidores App-V trabalham em conjunto para entregar e gerenciar pacotes.

  Esse método exige que o Citrix DaaS atualize periodicamente a exibição do instantâneo do estado do servidor App-V. Isso resulta na sobrecarga de hardware, infraestrutura e administração. O Citrix DaaS e os servidores App-V devem permanecer sincronizados, especialmente as permissões de usuário.

  A Administração dupla funciona melhor nas implantações em que o App-V e o Citrix Cloud estão estreitamente ligados:

  - **Servidor de gerenciamento App-V**. Publica e gerencia o ciclo de vida dos pacotes App-V e os arquivos de configuração dinâmica.
  - **Componente Citrix Personalization** instalado em máquinas VDA. Gerencie o registro do servidor de publicação App-V apropriado necessário para inicializações de aplicativos.

  Esse método garante que o servidor de publicação App-V seja sincronizado para o usuário no momento apropriado. O servidor de publicação mantém outros aspectos do ciclo de vida do pacote, como atualizar no login e grupos de conexão.

- **Administração simples**. Os pacotes de aplicativos são armazenados em compartilhamentos de rede. O Citrix DaaS entrega e gerencia pacotes de forma independente.

  Esse método reduz a sobrecarga porque os servidores App-V e a infraestrutura de banco de dados não são necessários na implantação.

Nesse método, você armazena os pacotes App-V em um compartilhamento de rede e carrega seus metadados desse local para o Citrix Cloud. O componente Citrix Personalization instalado nas máquinas VDA gerencia e entrega os aplicativos da seguinte forma:

- Processam os arquivos de configuração de implantação e os arquivos de configuração do usuário quando um aplicativo for iniciado.
- Gerenciam todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Você pode usar os dois métodos de gerenciamento simultaneamente. Em outras palavras, quando você adiciona aplicativos aos grupos de entrega, os aplicativos podem vir de pacotes App-V presentes em servidores App-V ou em compartilhamentos de rede.

> **Nota:**
>
> Se você estiver usando os dois métodos de gerenciamento simultaneamente, e o pacote App-V tiver um arquivo de configuração dinâmica nos dois locais, o arquivo no servidor App-V (administração dupla) será usado.

Procedimentos

Para dar suporte à entrega dos aplicativos App-V, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization em máquinas VDA para obter detalhes.

Para fornecer aplicativos empacotados do App-V para seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos no Citrix Cloud.
3. Adicionar aplicativos a grupos de entrega.
4. Para habilitar a entrega automática de pacotes App-V interdependentes, crie grupos de isolamento.

Para que o Citrix DaaS reconheça e aplique os arquivos de configuração dinâmica do App-V no método de Administração simples, consulte este blog da Citrix.

Implementar e entregar aplicativos MSIX e de anexação de aplicativo MSIX

Esta seção aborda as seguintes informações:

- Visão geral. Descreve como o Citrix DaaS entrega e gerencia os pacotes de anexação de aplicativo MSIX e MSIX.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

O Citrix DaaS entrega aplicativos MSIX e de anexação de aplicativo MSIX aos usuários por meio do componente Citrix Personalization instalado em máquinas VDA. Este componente gerencia todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Para obter mais informações sobre MSIX e anexação de aplicativo MSIX, consulte a documentação da Microsoft: https://docs.microsoft.com/en-us/windows/msix/ e https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach, respectivamente.

Procedimentos

Para dar suporte à entrega dos pacotes MSIX e de conexão de aplicativo MSIX, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization em máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados MSIX e de anexação de aplicativo MSIX aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos no Citrix Cloud.
3. Adicionar aplicativos a grupos de entrega.

Instalar o componente Citrix Personalization em máquinas VDA

O componente Citrix Personalization gerencia o processo de publicação de pacotes de aplicativos nos formatos App-V, MSIX e de anexação de aplicativo MSIX. Este componente não é instalado por padrão quando você instala 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 formas:

- No assistente de instalação, vá para a página **Additional Components** e marque a caixa de seleção **Citrix Personalization for App-V - VDA**.
- Na interface da 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 do mouse em **Citrix Virtual Delivery Agent** e selecione **Alterar**.
2. No assistente exibido, vá para a página **Additional Components** e marque a caixa de seleção **Citrix Personalization for App-V - VDA**.

> **Nota:**
>
> O cliente Desktop Microsoft App-V é o componente que executa os aplicativos virtuais dos pacotes App-V nos dispositivos do usuário. O Windows 10 (1607 ou posterior), o Windows Server 2016 e o Windows Server 2019 já incluem esse software cliente App-V. Você só precisa habilitá-lo nas máquinas VDA. Para obter mais informações, consulte este artigo da documentação da Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

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 para obter detalhes.
2. Armazene pacotes de aplicativos em um local de rede:
   - Para **administração simples de App-V**: armazene os pacotes e os Arquivos de Configuração Dinâmica (App-V) correspondentes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
   - Para **administração dupla de App-V**: 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 anexação de aplicativo MSIX**: armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um compartilhamento de arquivos do Azure.
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 no domínio do AD, conceda à máquina VDA permissão de leitura ao caminho de armazenamento. Para isso, você pode conceder a permissão de leitura da conta do AD da máquina para o compartilhamento explicitamente ou incluir a conta em um grupo do AD que tenha essa permissão.
   - Se você armazenar pacotes em um Compartilhamento de Arquivos do Azure, primeiro conceda uma permissão de leitura de conta de usuário para o caminho de armazenamento no Azure. Em seguida, configure o `ctxAppVService` em execução na máquina VDA para usar essa conta de usuário para acessar o caminho de armazenamento do pacote. Consulte a seção a seguir para ver as etapas detalhadas.

Alterar a conta de logon do usuário

O VDA chama `ctxAppVService` para acessar os caminhos de armazenamento do pacote. Por padrão, `ctxAppVService` acessa os caminhos de armazenamento de pacotes usando a **conta do Sistema Local** da máquina. Esse tipo de autenticação de máquina funciona em domínios do AD. No entanto, não funciona nos cenários de integração do AD e do Azure AD, que exigem autenticação baseada em conta de usuário.

Se você armazenar pacotes em um Compartilhamento de Arquivos do Azure, altere a conta de logon de `ctxAppVService` para uma conta de usuário que tenha permissão de leitura no caminho de armazenamento do pacote. As etapas detalhadas são as seguintes:

1. Inicie o **Services**, clique com o botão direito do mouse em **ctxAppVService** e selecione **Properties**.
2. Na guia **Log on**, selecione **This account**, insira uma conta de usuário que tenha permissão de leitura para o caminho de armazenamento do pacote e, em seguida, digite a senha do usuário duas vezes.
3. Clique em **OK**.

Carregar pacotes de aplicativos no Citrix Cloud

Depois de armazenar os pacotes de aplicativos em um local de rede conforme necessário, carregue-os no Citrix Cloud para entrega. Use um dos seguintes métodos, conforme necessário:

- Carregar em massa
- Carregar um por um

Preparação

O Citrix DaaS usa uma máquina VDA para configurar a conexão com o local de rede para a descoberta de pacotes. Portanto, crie um grupo de entrega previamente e certifique-se de que pelo menos um VDA no grupo atenda aos seguintes requisitos:

- Versão VDA:
  - Para descobrir pacotes do App-V: 2203 ou posterior
  - Para descobrir os pacotes MSIX e de anexação de aplicativo MSIX: 2209 ou posterior
- Componente do Citrix Personalization for App-V: instalado
- Permissão ao local do pacote: Leitura (veja a Etapa 2: Armazenar pacotes de aplicativos em compartilhamentos de rede para obter detalhes.)
- Alimentação: ligado
- Estado: registrado

Funções necessárias

Por padrão, se você tiver a função Administrador de nuvem ou Administrador completo, pode carregar os pacotes de aplicativos para o Citrix Cloud. Você também pode criar funções personalizadas para realizar as ações de carregamento. A tabela a seguir lista as permissões exigidas por ação para os pacotes de aplicativos.

Ação	Permissão necessária
Adicionar pacote (carregar um por um)	Create Application Discovery Sessions
Adicionar origem (carregar em massa)	Create Application Discovery Profiles
Verificar se há atualizações de pacotes	Create Application Discovery Sessions
Remover origem	Remove Application Discovery Profiles

Carregar pacotes de aplicativos em massa

Carregue os pacotes em um local de rede para o Citrix Cloud. Certifique-se de ter os seguintes itens prontos antes do carregamento:

- Um grupo de entrega que atenda aos requisitos de Preparação
- O caminho da localização da rede

Para carregar pacotes em massa, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **App Packages** no painel esquerdo.
2. Na guia **Sources**, clique no botão **Add Source**. A página **Add Source** é exibida.
3. No campo **Name**, insira um nome descritivo para a origem do pacote.
4. No campo **Delivery group**, clique em **Select a delivery group**. Em seguida, selecione um grupo de entrega que atenda aos requisitos descritos na Preparação e clique em **OK**.
5. No campo **Location type**, selecione **Microsoft App-V server** ou **Network share** com base em onde você armazena os pacotes e, em seguida, preencha as configurações correspondentes:
    - Se você selecionar o **Microsoft App-V server**, 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 **Network share**, especifique as seguintes informações:

  - Insira o caminho UNC do compartilhamento de rede. Exemplo: `\\Package-Server\apps\`
  - Selecione os tipos de pacotes que deseja carregar. As opções incluem App-V, MSIX e anexação de aplicativo MSIX.
  - Especifique se deseja pesquisar pacotes nas subpastas.

6. Clique em **Add Source**.

   A página Add Source é fechada e a origem recém-adicionada aparece na lista de origens. O Citrix DaaS carrega os pacotes no Citrix Cloud usando um VDA no grupo de entrega. Após a conclusão do carregamento, o campo Status mostra *Import successful*. Os pacotes correspondentes aparecem na guia **Packages**.

   > **Nota:**
   >
   > Para verificar se há atualizações de pacotes em um local de origem e importá-las para o Citrix Cloud, selecione o local na lista de origem e clique em **Check for Package Updates**.

Carregar pacotes de aplicativos um por um

Carregue um pacote de aplicativos de um compartilhamento de rede para o Citrix Cloud. Antes do carregamento, verifique se você tem os seguintes itens prontos:

- Um grupo de entrega que atenda aos requisitos descritos em Preparação
- O caminho do local da rede.

Para carregar um pacote para o Citrix Cloud, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **App Packages** no painel esquerdo.
2. Na guia **Packages**, clique no botão **Add Package**. A página **Add Package** é exibida.
3. No campo **Delivery group**, clique em **Select a delivery group**. Em seguida, selecione um grupo de entrega que atenda aos requisitos descritos na Preparação e clique em **OK**.
4. No campo **Package full path**, insira um caminho conforme necessário:

   - Para fazer upload de vários pacotes ao mesmo tempo, 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. Clique em **Add Package**.

   O pacote do aplicativo aparece na guia **Packages**.

Adicionar aplicativos a grupos de entrega

Depois que um pacote de aplicativos for totalmente carregado, 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:**
>
> Os aplicativos empacotados podem ser atribuídos somente a grupos de entrega do tipo *Applications* ou *Desktops and Applications*.

Para adicionar um ou mais aplicativos em um pacote a vários grupos de entrega, siga estas etapas:

1. Em **Manage > Full Configuration**, selecione **App Packages** no painel esquerdo.
2. Na guia **Packages**, selecione um pacote conforme necessário.
3. Na barra de ações clique em **Add Delivery Groups**. A página Add Delivery Groups é exibida.
4. Selecione um ou mais aplicativos no pacote, conforme necessário, e clique em **Next**. Grupos de entrega do tipo de entrega *Applications* ou *Desktops and Applications* aparecem.
5. Na lista de grupos de entrega, selecione os grupos aos quais você deseja atribuir os aplicativos e clique em **Next**.
   Nota: Se você selecionou um pacote MSIX ou de anexação de aplicativo MSIX, somente grupos de entrega cujo nível funcional seja 2106 ou posterior serão mostrados na lista.
6. Clique em **Finish**.

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 Add applications.

(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:**
>
> Grupos de isolamento são compatíveis com o método de administração simples de App-V. Se estiver usando o método de administração dupla App-V, você pode 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: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

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 são idênticos aos grupos de conexão App-V. Um grupo de isolamento inclui dois tipos de pacotes:

- Pacotes de aplicativos **explícitos**. Aplicativos com requisitos específicos de licenciamento. 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 ou não adicionados aos 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, adicionar o pacote App-V de `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 em grupos de entrega. Se o usuário tiver permissão para acessar o aplicativo, todos os pacotes de aplicativos *automáticos* no mesmo grupo de isolamento são disponibilizados para o 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 para o usuário somente se estiver no mesmo grupo de entrega.

Para obter mais informações sobre grupos isolados, consulte este blog da Citrix.

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 **Isolation Groups**, clique em **Add Isolation Group**.
2. Insira um nome e uma descrição para o grupo de isolamento. Todos os pacotes de aplicativos no Citrix Cloud aparecem na lista **Available Packages**.
3. Na lista **Available Packages**, selecione um aplicativo, conforme necessário, e clique na seta para a direita. O aplicativo selecionado aparece na lista **Packages in Isolation Group**.
4. No campo **Deployment**, selecione **Explicit** ou **Automatic** para o aplicativo.
5. Repita as etapas 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 apenas em um grupo de conexão ativo por vez. Recomendamos que você evite adicionar o mesmo pacote a dois grupos de isolamento diferentes que estão adicionados ao mesmo grupo de entrega.

AutoScale

September 5, 2023

O AutoScale fornece uma solução consistente e de alto desempenho para gerenciar a energia de suas máquinas de forma proativa. O objetivo é equilibrar os custos e a experiência do usuário. O AutoScale incorpora a tecnologia preterida do Smart Scale na solução de gerenciamento de energia do console **Manage**.

O AutoScale permite o gerenciamento proativo de energia de todas as máquinas registradas com SO de sessão única e multissessão em um grupo de entrega.

Os recursos do AutoScale incluem:

- Configurações baseadas em agendamento e carga
- Tempo limite de sessão dinâmica
- Máquinas marcadas no AutoScale (intermitência da nuvem)
- Provisionamento dinâmico de máquinas
- Notificações de logoff do usuário

Plataformas de hospedagem VDA suportadas

O AutoScale é compatível com todas as plataformas compatíveis com o Citrix DaaS. Isso inclui várias plataformas de infraestrutura, incluindo Citrix Hypervisor, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e muito mais. Para obter uma lista completa das plataformas suportadas, consulte os Requisitos do sistema do Citrix DaaS.

Cargas de trabalho suportadas

O AutoScale oferece suporte a grupos de entrega com SO multissessão e SO de sessão única. Existem três interfaces de usuário que você deve conhecer:

- Interface de usuário do AutoScale para grupos de entrega de SO multissessão (anteriormente grupos de entrega do RDS)
- Interface de usuário do AutoScale para grupos de entrega aleatórios (em pool) de SO de sessão única (anteriormente grupos de entrega de VDI em pool)
- Interface de usuário do AutoScale para grupos de entrega estáticos de SO de sessão única (anteriormente grupos de entrega de 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:

- Fornece um mecanismo único e consistente para gerenciar a energia das máquinas em um grupo de entrega.
- Garante a disponibilidade e controla os custos ao alimentar as máquinas usando o gerenciamento de energia baseado em carga ou programação, ou uma combinação de ambos.
- Para monitorar métricas, como economia de custos e utilização da capacidade, e ativar notificações, use o Director, disponível na guia **Monitor**.

Assista a um vídeo de 2 minutos

O vídeo a seguir fornece um rápido tour pelo AutoScale.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

Introdução ao AutoScale

November 9, 2023

O AutoScale funciona no nível de grupo de entrega. Ele gerencia de forma proativa as máquinas em um grupo de entrega com base nos cronogramas que você define.

O AutoScale se aplica a todos os tipos de grupos de entrega:

- SO de sessão única estático
- SO de sessão única aleatório
- SO multissessão aleatório

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, conheça os seguintes conceitos básicos em AutoScale:

- Schedules
- Capacity buffer
- Índice de carga

Schedules

O AutoScale liga e desliga as máquinas em um grupo de entrega com base em um cronograma definido por você.

O cronograma inclui o número de máquinas ativas para cada intervalo de tempo, com horários de pico e fora do pico definidos.

As configurações de Schedule variam de acordo com o tipo de grupo de entrega. Para obter mais informações, consulte:

- Grupos de entrega com SO multissessão
- Grupos de entrega aleatórios com SO de sessão única
- Grupos de entrega estáticos com SO de sessão única

Capacity buffer

O buffer de capacidade é usado para adicionar capacidade de reserva à demanda atual para contabilizar aumentos de carga dinâmica. Há dois cenários que devem ser considerados:

- Para grupos de entrega com SO multissessão, 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 com SO de sessão única, o valor em capacity buffer é definido como uma porcentagem do número total de máquinas no grupo de entrega.

Índice de carga

> **IMPORTANTE:**
>
> O índice de carga se aplica somente a grupos de entrega multissessão.

A métrica do índice de carga determina a probabilidade de uma máquina receber solicitações de login do usuário. Ela é calculada usando as configurações da **política do Citrix Load Management** definidas para o uso simultâneo de logon , sessão, CPU, disco e memória.

O valor de load index varia de 0 a 10.000. Por padrão, uma máquina é considerada com carga total quando está hospedando 250 sessões.

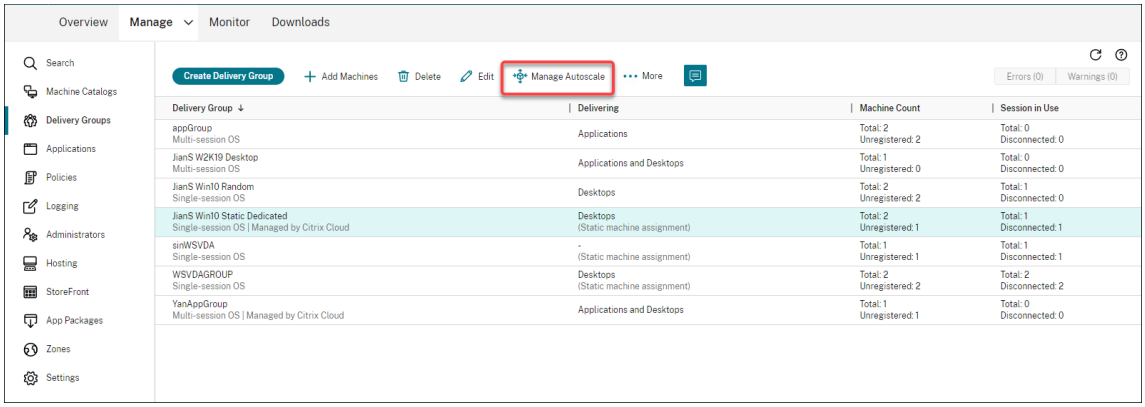
- O dígito "0"indica uma máquina descarregada. Uma máquina com um valor de índice de carga de 0 está a uma carga de linha de base.
- O dígito "10.000"indica uma máquina totalmente carregada que não pode executar mais sessões.

Ativar AutoScale para um grupo de entrega

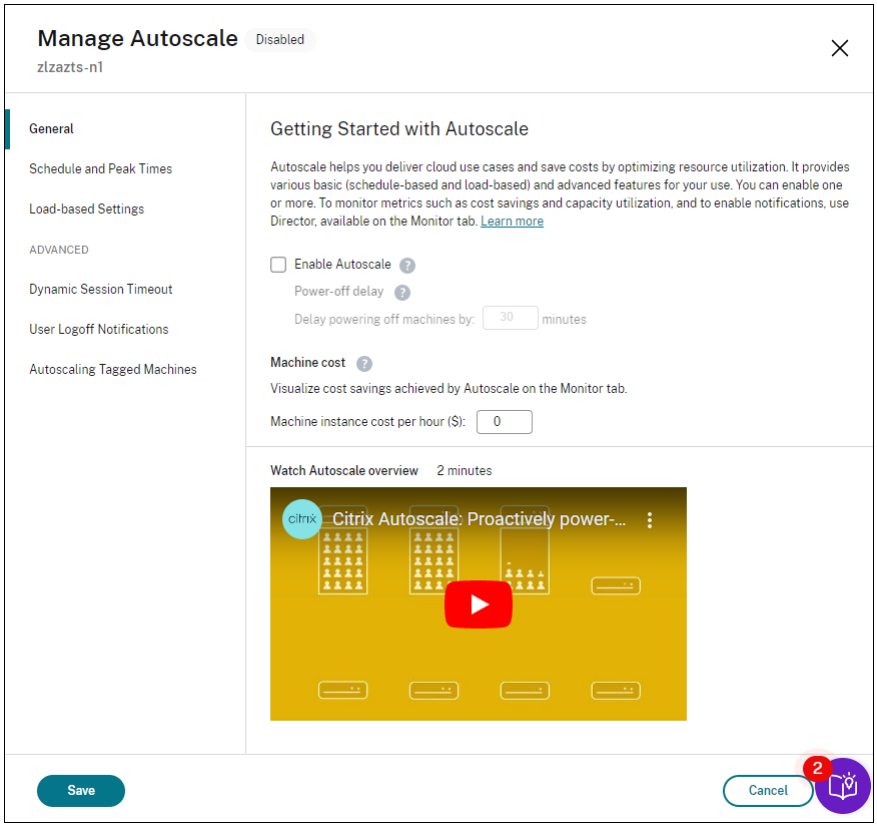
O AutoScale é desativado por padrão quando você cria um grupo de entrega. Para ativar e configurar o AutoScale para um grupo de entrega usando a interface Full Configuration, siga estas etapas:

Você também pode usar comandos do PowerShell para ativar e configurar o AutoScale para um grupo de entrega. Para obter mais informações, consulte Comandos do Broker PowerShell SDK.

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo.
2. Selecione o grupo de entrega que deseja gerenciar e clique em **Manage AutoScale**.



3. Na página **Manage Autoscale**, marque a caixa de seleção **Enable Autoscale** para ativar o AutoScale. Depois de ativar 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:

   - Programe os horários
   - Para desligar máquinas inativas com mais eficiência, use Dynamic session timeouts e User logoff notifications
   - Para gerenciar a energia de um subconjunto de máquinas no grupo de entrega, use Autoscaling tagged machines

Para desativar o AutoScale, desmarque a caixa de seleção **Autoscale**. As opções na página ficam acinzentadas para indicar que o AutoScale está desativado para o grupo de entrega selecionado.

> **Importante:**
>
> - Se você desativar o AutoScale, todas as máquinas gerenciadas pelo AutoScale permanecem no estado original no momento da desativação.
> - Depois de desativar o AutoScale, as máquinas no estado de esvaziamento são retiradas do estado de esvaziamento. Para obter mais informações sobre o estado de esvaziamento, consulte Estado de esvaziamento.

Você pode provisionar máquinas dinamicamente para o grupo usando um script do PowerShell. Para obter mais informações, consulte Provisionamento dinâmico de máquinas.

Monitorar métricas

Depois de ativar o AutoScale para um grupo de entrega, você pode monitorar as seguintes métricas de máquinas gerenciadas pelo AutoScale na guia **Monitor**.

- Uso da máquina
- Economia estimada
- Notificações de alerta de máquinas e sessões
- Status da máquina
- Tendências de avaliação de carga

> **Nota:**
>
> Quando você ativa inicialmente o AutoScale para um grupo de entrega, pode demorar alguns minutos para exibir os dados de monitoramento desse grupo de entrega.
> Os dados de monitoramento permanecem disponíveis se o AutoScale for ativado e depois desativado para o grupo de entrega. O AutoScale coleta dados de monitoramento a intervalos de 5 minutos.

Para obter mais informações sobre as métricas, consulte Monitorar máquinas gerenciadas por AutoScale.

É bom saber

O AutoScale funciona no nível de grupo de entrega. Ele é configurado por grupo de entrega. Ele gerencia a energia apenas das máquinas no grupo de entrega selecionado.

Registro de capacidade e máquina

O AutoScale inclui somente máquinas registradas no site ao determinar a capacidade. As 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.

Dimensionamento em vários catálogos de máquinas

Em alguns sites, vários catálogos de máquinas podem estar associados a um único grupo de entrega. O AutoScale liga as máquinas de cada catálogo aleatoriamente para atender aos requisitos de demanda de sessão ou agendamento.

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, ela poderá ligar uma máquina do Catálogo A ou do Catálogo B.

Provisionamento de máquinas e demanda da 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 da sessão exceder o número total de máquinas registradas no grupo de entrega, o AutoScale garante que todas as máquinas registradas sejam ligadas. Entretanto, o **AutoScale não provisiona máquinas adicionais**.

Para superar esse gargalo, você pode usar um script do PowerShell para criar máquinas e excluí-las dinamicamente. Para obter mais informações, consulte Provisionamento dinâmico de máquinas

Considerações sobre o tamanho da instância

Você pode otimizar seus custos se dimensionar adequadamente as suas instâncias em nuvens públicas. Recomendamos que você provisione as instâncias menores, desde que elas correspondam aos requisitos de desempenho e capacidade da carga de trabalho.

Instâncias menores hospedam menos sessões de usuário do que instâncias maiores. Portanto, o AutoScale coloca as máquinas em estado de esvaziamento muito mais rápido porque leva menos tempo para que seja feito o logoff da última sessão. Como resultado, o AutoScale desliga as instâncias menores mais cedo, reduzindo assim os custos.

Estado de esvaziamento

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 excedentes com o menor número de sessões em "estado de esvaziamento"e as desliga quando é feito o logoff de todas as sessões. Esse comportamento ocorre quando a demanda da sessão diminui e a programação exige menos máquinas do que as que estão ligadas.

O AutoScale coloca as máquinas excedentes em "estado de esvaziamento", uma a uma:

- Se duas ou mais máquinas tiverem o mesmo número de sessões ativas, o AutoScale esvaziará a máquina que foi ligada para o atraso de desligamento especificado.

  Isso evita colocar máquinas recém-ligadas no estado de esvaziamento, porque essas máquinas provavelmente terão o menor número de sessões.

- Se duas ou mais máquinas tiverem sido ligadas para o atraso de desligamento especificado, o AutoScale esvaziará essas máquinas uma a uma, aleatoriamente.

As máquinas em estado de esvaziamento não hospedam mais inicializações de novas sessões e aguardando pelo logoff das sessões existentes. Uma máquina se torna candidata ao desligamento somente quando é feito o logoff de todas as sessões. No entanto, se não houver máquinas imediatamente disponíveis para inicializações de sessão, o AutoScale prefere direcionar as inicializações de sessão para uma máquina em estado de esvaziamento a ligar uma máquina.

Uma máquina é retirada do estado de esvaziamento quando uma das seguintes condições é atendida:

- A máquina está desligada.
- O AutoScale está desativado 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. Esse caso ocorre quando a programação (dimensionamento baseado em agendamento) ou a demanda atual (escalonamento baseado em carga) requer mais máquinas do que o número de máquinas que estão atualmente ligadas.

> **Importante:**
>
> Se não houver máquinas imediatamente disponíveis para inicializações de sessão, o AutoScale prefere direcionar as inicializações de sessão para uma máquina em estado de esvaziamento a ligar uma máquina. Uma máquina em estado de esvaziamento que hospeda a inicialização de uma sessão permanece em estado de esvaziamento.

Para descobrir quais máquinas estão no estado de esvaziamento, use o comando `Get-BrokerMachine` do PowerShell. Por exemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Como alternativa, você pode usar o console Manage. Consulte Exibir máquinas em estado de esvaziamento.

Exibir máquinas em estado de esvaziamento

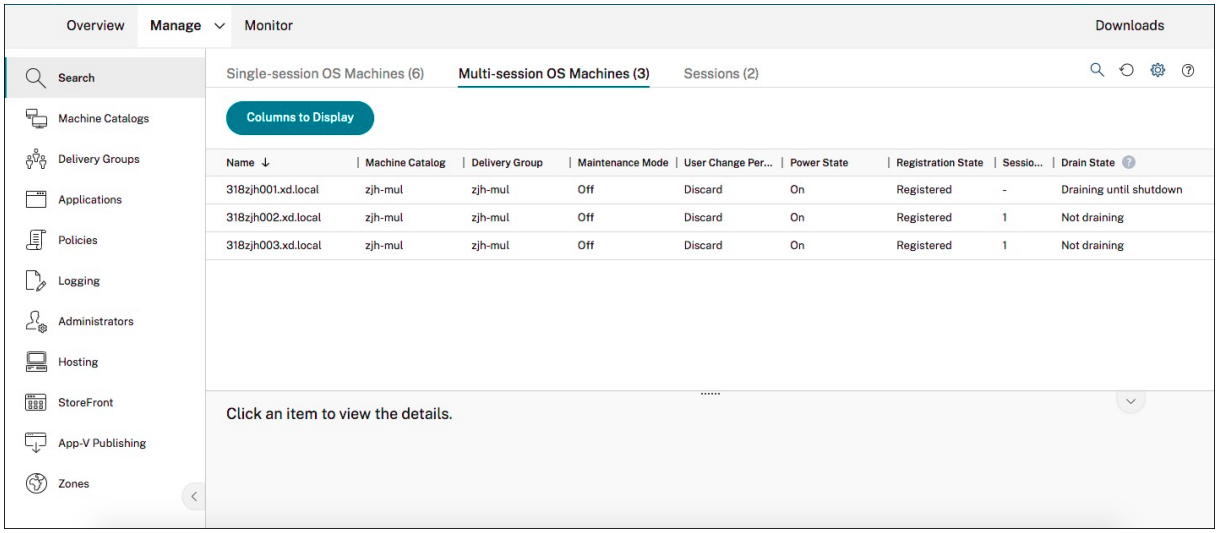
> **Nota:**
>
> Esse recurso se aplica somente a máquinas multissessão.

Em **Manage > Full Configuration**, você pode exibir as máquinas que estão no estado de esvaziamento, informando quais máquinas estão prestes a desligar. Conclua as seguintes etapas:

1. Navegue até o nó **Search** e clique em **Columns to Display**.
2. Na janela **Columns to Display**, marque a caixa de seleção ao lado de **Drain State**.
3. Clique em **Save** para sair da janela **Columns to Display**.

A coluna **Drain State** pode exibir as seguintes informações:

- **Draining until shutdown.** Aparece quando as máquinas estão no estado de esvaziamento até serem desligadas.
- **Not draining.** Aparece quando as máquinas ainda não estão no estado de esvaziamento.



Mais informações

Para obter mais informações sobre AutoScale, consulte Citrix Autoscale na Tech Zone.

Configurações baseadas em agendamento e carga

November 9, 2023

Como a energia de AutoScale gerencia as máquinas

O AutoScale liga e desliga as máquinas com base na programação selecionada. O AutoScale permite definir várias agendas que incluem dias específicos da semana e ajustar 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 proporcionar uma experiência otimizada. Observe que essas máquinas serão ligadas durante a programação agendada, independentemente de haver ou não sessões em execução nelas.

> **Nota:**
>
> O AutoScale é compatível com qualquer máquina com gerenciamento de energia.

A programação é baseada 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.

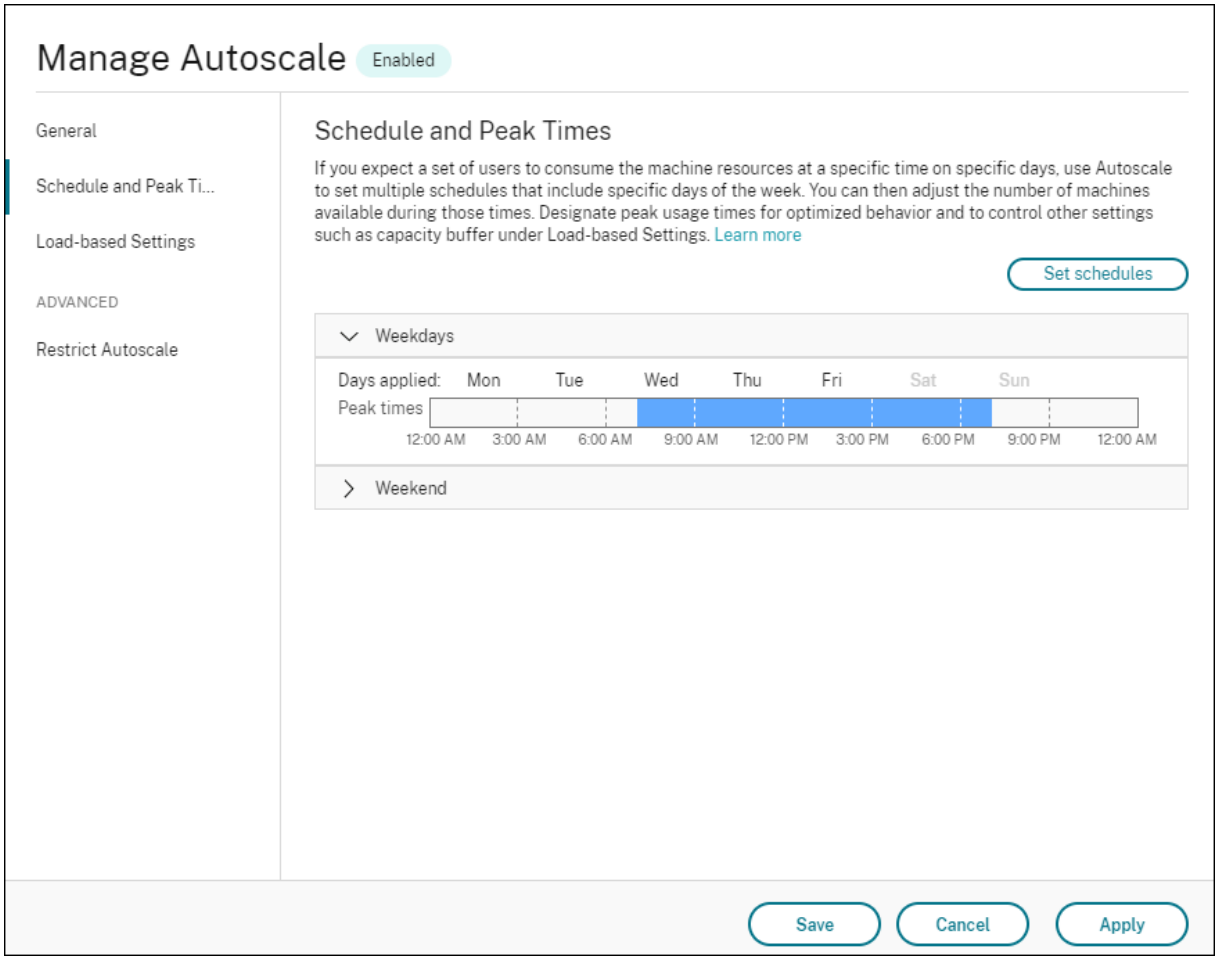
O AutoScale tem duas programações padrão: *Weekdays* (de segunda a sexta-feira) e *Weekend* (sábado e domingo). Por padrão, a programação **Weekdays** mantém uma máquina ligada das 7h00 às 18h30 durante os horários de pico e nenhuma máquina fora dos horários de pico. O buffer de capacidade padrão é definido como 10% durante os horários de pico e fora de pico. Por padrão, a programação de **Weekend** não mantém nenhuma máquina ligada.

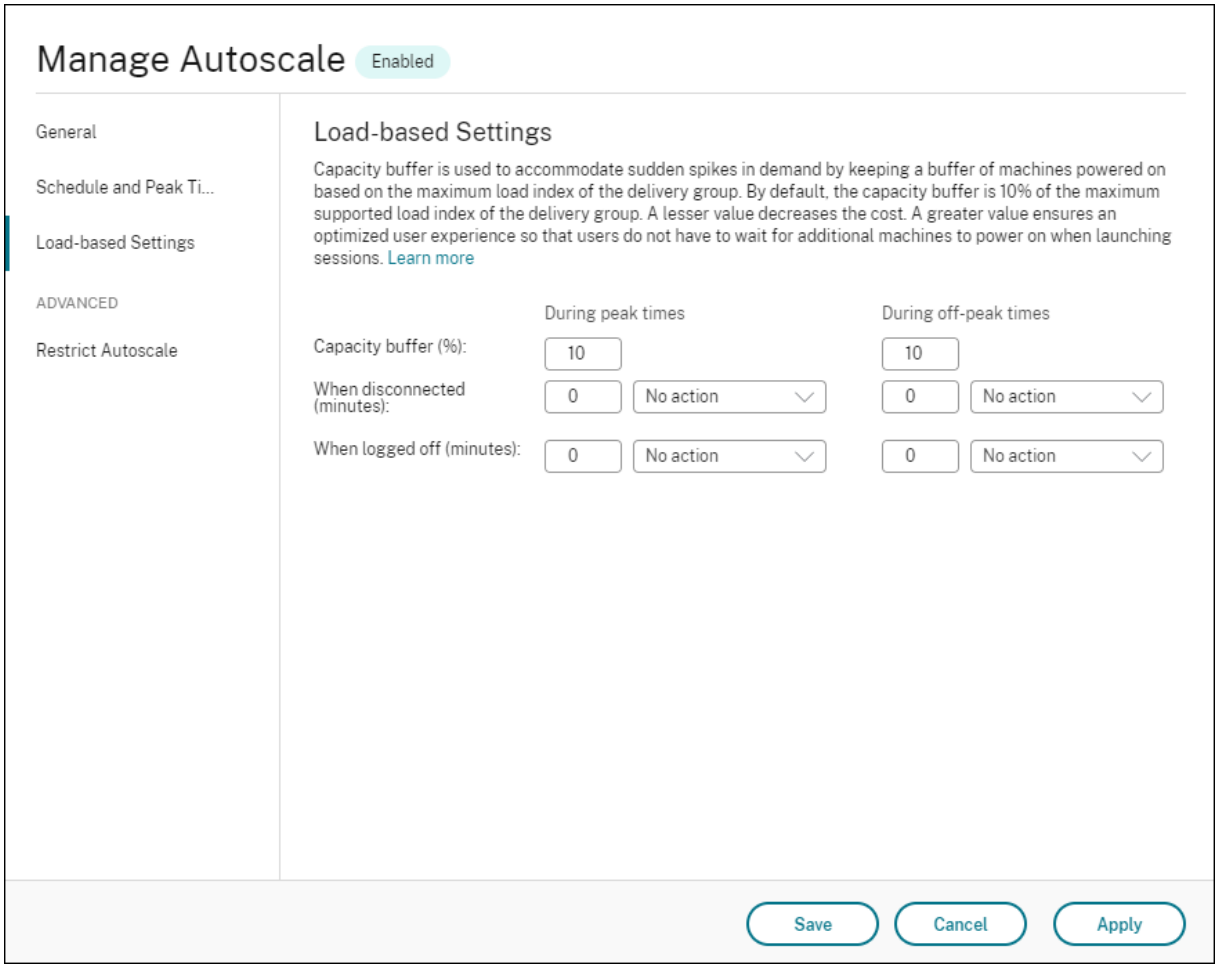
> **Nota:**
>
> O AutoScale trata apenas as máquinas registradas no site como parte da capacidade disponível nos cálculos que ele faz. "Registrada"significa que a máquina está disponível para uso ou já está em uso. Isso garante que apenas as máquinas que podem aceitar sessões de usuário sejam incluídas na capacidade do grupo de entrega.

Interfaces de usuário

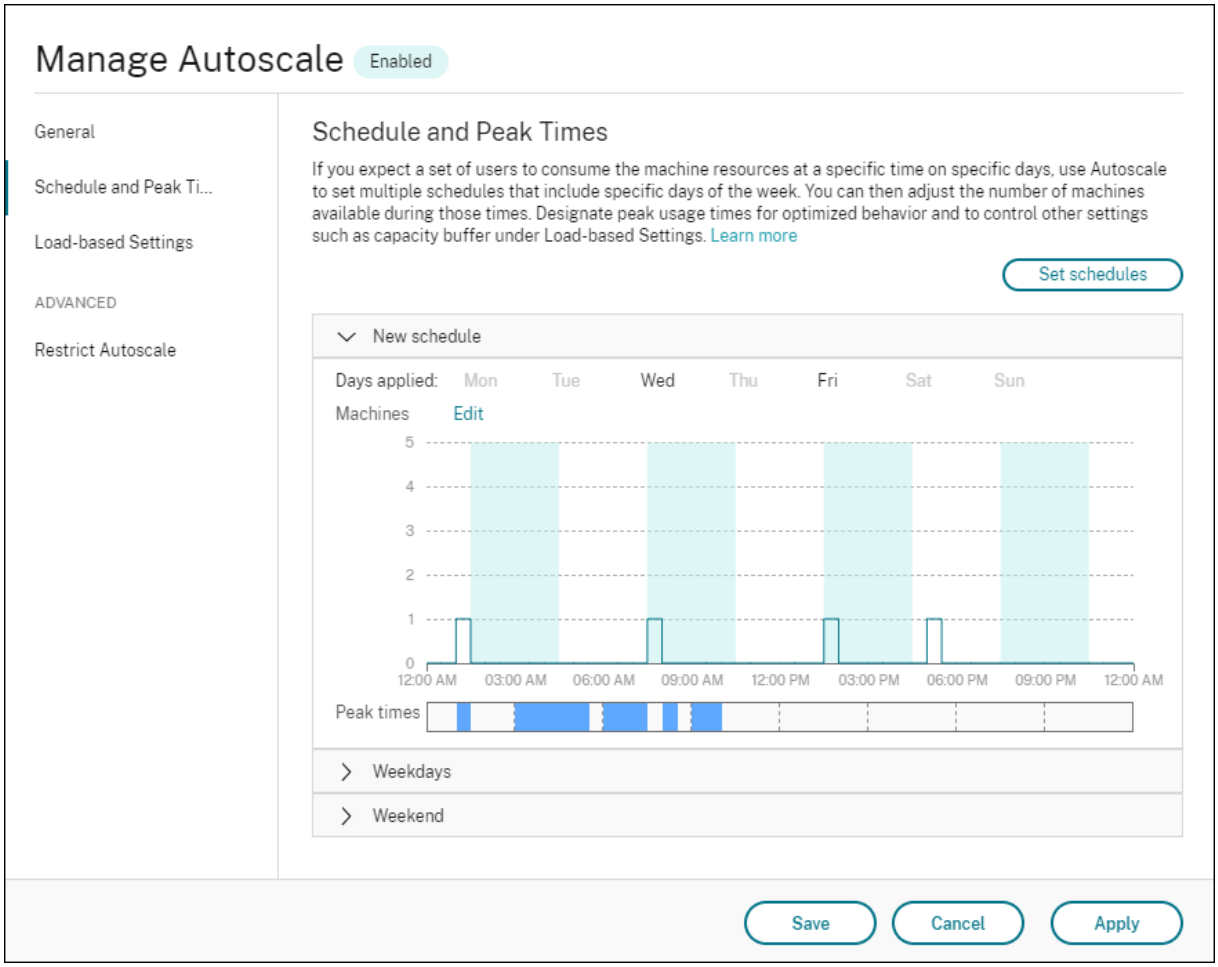
Existem três tipos de interfaces de usuário que você deve conhecer.

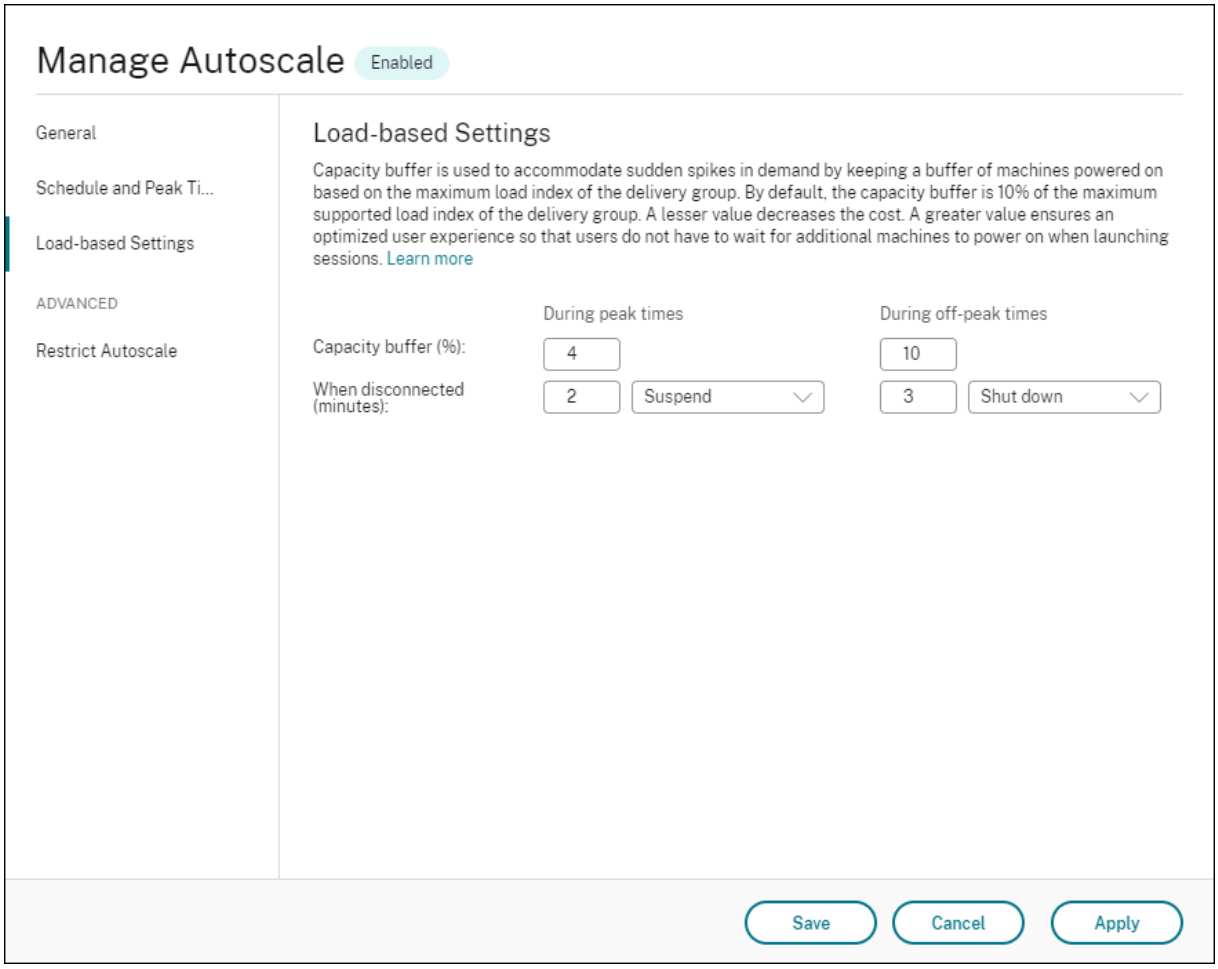
Interface de usuário para *grupos de entrega estáticos com SO de sessão única*:



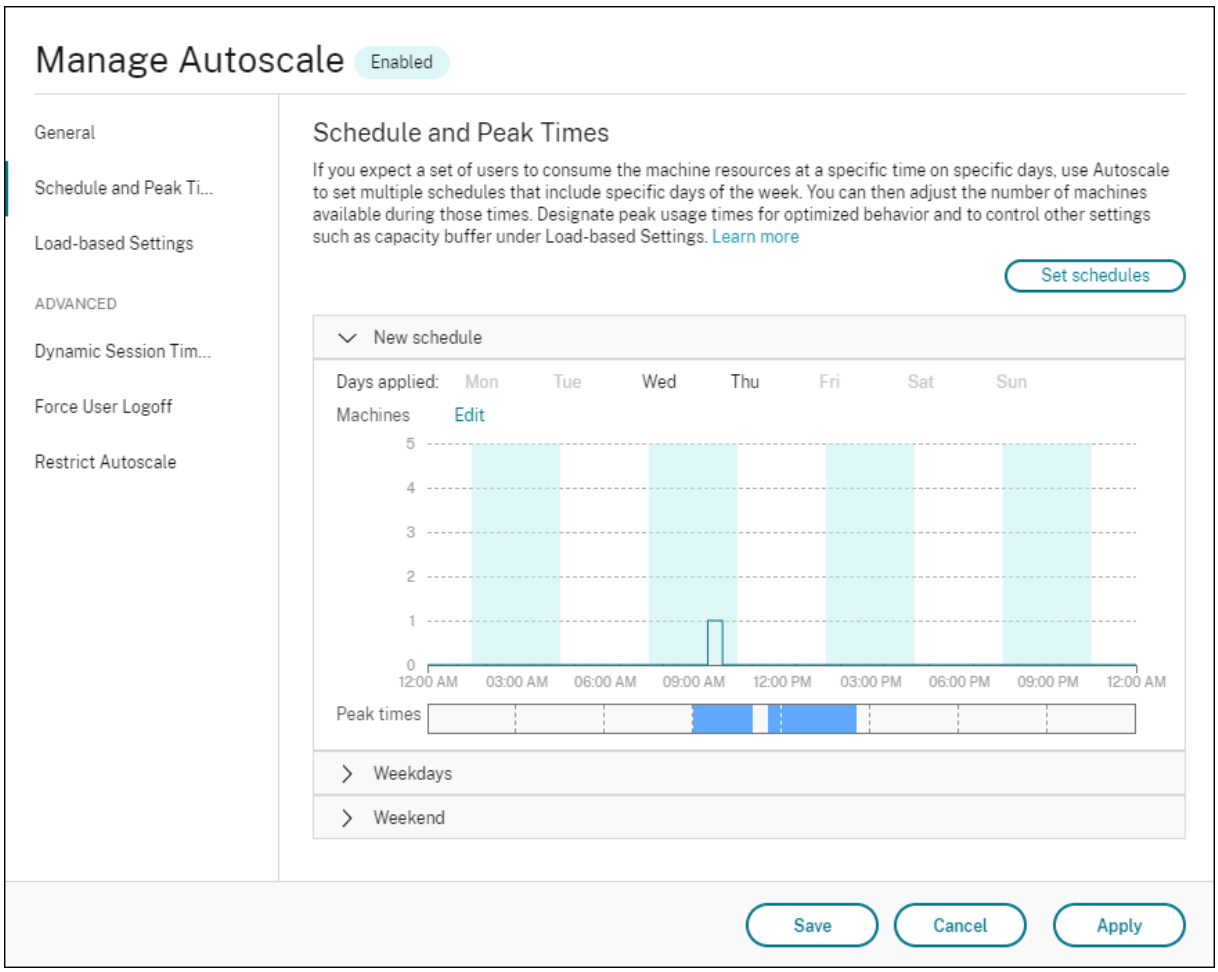


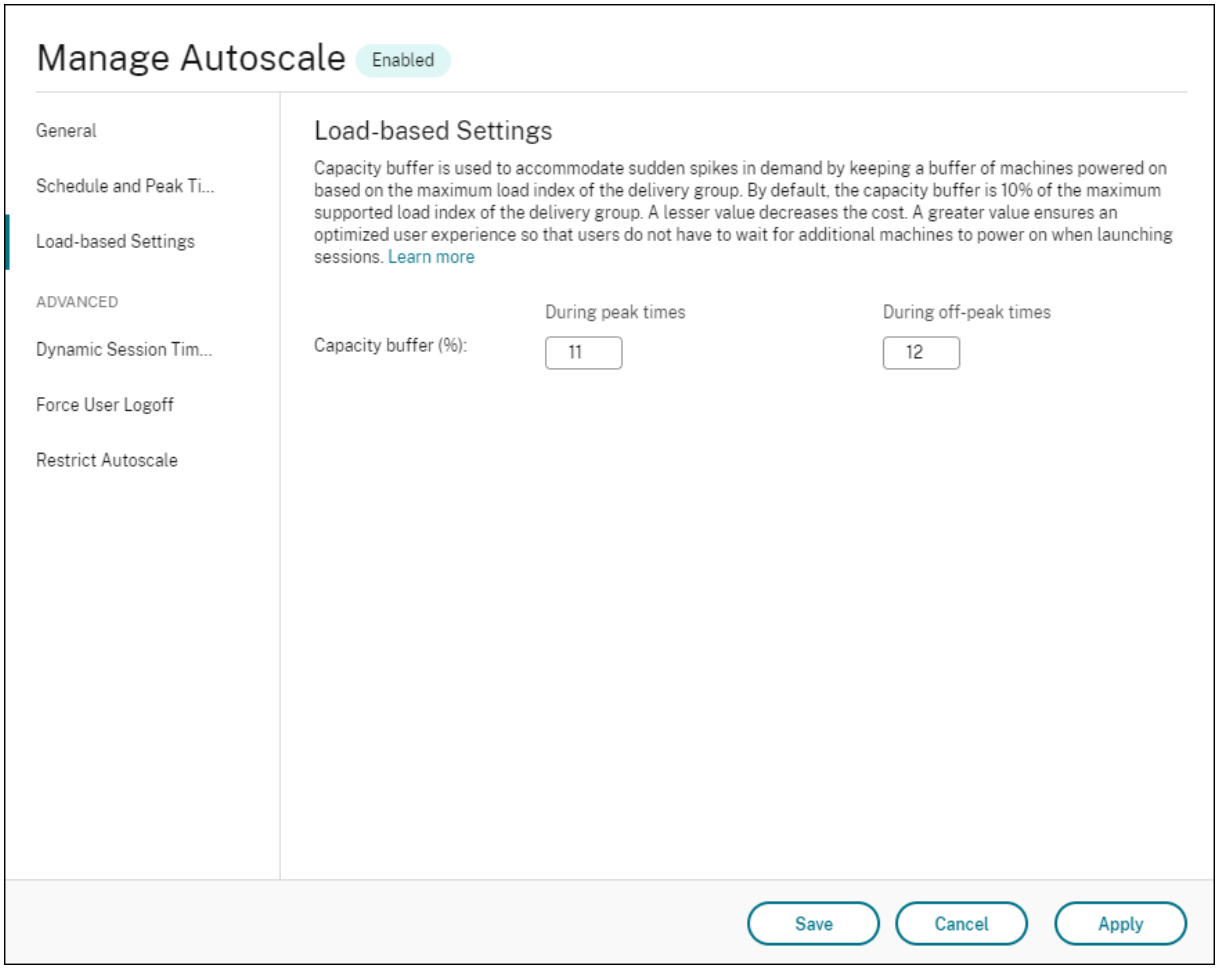
Interface de usuário do AutoScale para *grupos de entrega aleatórios de SO de sessão única*:





Interface de usuário do AutoScale para *grupos de entrega de SO multissessão*:





Configurações baseadas em agendamento

Autoscale schedule. Permite adicionar, editar, selecionar e excluir agendamentos.

Days applied. Destaca os dias em que você se registrou no agendamento selecionado. Os dias restantes ficam acinzentados.

Edit. Permite atribuir as máquinas a cada hora inteira ou a cada meia hora. Você pode atribuir as máquinas por números e por porcentagens.

> **Nota:**
>
> - Essa opção está disponível somente nas interfaces de usuário do AutoScale para grupos de entrega aleatórios com SO de sessão única e SO multissessão.
> - O histograma ao lado de **Edit** representa graficamente o número ou a porcentagem de máquinas que estão sendo executadas em diferentes intervalos de tempo.
> - Você pode **atribuir máquinas** a cada intervalo de tempo clicando em **Edit** acima de **Peak times**. Dependendo da opção selecionada no menu da janela **Machines to start**, você

pode atribuir as máquinas por números ou por porcentagens.
- Para grupos de entrega de SO multissessão, 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 com 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 horários, siga estes passos:

1. Na página **Schedule and Peak Times** da janela **Manage Autoscale**, clique em **Set schedules**.
2. Na janela **Edit Autoscale Schedules**, selecione os dias que você deseja aplicar a cada agendamento. Você também pode excluir agendamentos conforme aplicável.
3. Clique em **Done** para salvar os horários e retornar à página **Schedule and Peak Times**.
4. Selecione a programação aplicável e configure-a conforme necessário.
5. Clique em **Apply** para sair da janela **Manage Autoscale** ou definir as configurações em outras páginas.

Importante:

- O AutoScale não permite que o mesmo dia se sobreponha em programações diferentes. Por exemplo, se você selecionar Segunda-feira na Programação-2 depois de selecionar Segunda-feira na Programação-1, a Segunda-feira será automaticamente removida da Programação-1.
- O nome de agendamento não diferencia maiúsculas de minúsculas.
- O nome de agendamento não deve ficar em branco nem conter apenas espaços.
- O AutoScale permite espaços em branco entre caracteres.
- O nome de agendamento não deve conter os seguintes caracteres: \ / ; : # . * ? = < > | [ ] ( ) { } “ “ ‘.
- O AutoScale não aceita nomes de agendamento duplicados. Insira um nome diferente para cada agendamento.
- O AutoScale não aceita 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.

Configurações baseadas em carga

Peak times. Permite definir os horários de pico para os dias que você aplicou na programação selecionada. Você pode fazer isso clicando com o botão direito do mouse no gráfico de barras horizontais. Depois de definir os horários de pico, os horários indefinidos restantes assumem como padrão os horários fora de pico. Por **padrão**, o horário das 7h00 às 19h00 é definido como horário de pico para os dias incluídos na programação selecionada.

> **Importante:**
>
> - Para grupos de entrega com SO multissessão, o gráfico de barras dos horários de pico é usado para o buffer de capacidade.
> - Para grupos de entrega com SO de sessão única, o gráfico de barras dos horários de pico é usado para o buffer de capacidade e controla as ações a serem disparadas após o logoff e/ou a desconexão.
> - Você pode definir os horários de pico para os dias incluídos em uma programação em um nível granular de 30 minutos para os grupos de entrega com SO multissessão e com SO de sessão única. Como alternativa, você pode usar o comando `New-BrokerPowerTimeScheme PowerShell`. Para obter mais informações, consulte Comandos do Broker PowerShell SDK.

Capacity buffer. 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 as máquinas adicionais sejam ligadas. Por padrão, o buffer de capacidade é de 10% para os horários de pico e fora de pico. Se você definir o buffer de capacidade como 0 (zero), os usuários terão que esperar que outras máquinas sejam ativadas ao iniciar as sessões. O AutoScale permite determinar o buffer de capacidade separadamente para os horários de pico e fora de pico.

Configurações diversas

> **Dica:**
>
> - Você pode optar por definir as configurações diversas usando o Broker PowerShell SDK. Para obter mais informações, consulte Comandos do Broker PowerShell SDK.
> - Para entender os comandos do SDK associados às configurações de desconexão e logoff, consulte https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

When disconnected. 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 será suspensa ou desligada quando o tempo de

desconexão especificado expirar, dependendo da ação que você configurou. Por padrão, nenhuma ação é atribuída a máquinas desconectadas. Você pode definir as ações separadamente para os horários de pico e fora de pico. Para isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **No action**. Se selecionada, a máquina permanece ligada após a desconexão da sessão. O AutoScale não realiza nenhuma ação.
- **Suspend**. Se selecionada, o AutoScale pausa a máquina sem desligá-la quando o tempo de desconexão especificado expira. A opção a seguir fica disponível depois que você seleciona **Suspend**.
  - **When no reconnection in (minutes)**. As máquinas suspensas permanecem disponíveis para os usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Para tornar as máquinas disponíveis novamente para lidar com todas as cargas de trabalho, desligue-as. Especifique o tempo limite, em minutos, após o qual o AutoScale as desliga.
- **Shut down**. Se selecionada, o AutoScale desliga a máquina quando o tempo de desconexão especificado expira.

> **Nota:**
>
> Essa opção está disponível somente nas interfaces de usuário do AutoScale para grupos de entrega aleatórios e estáticos com SO de sessão única.

When logged off. 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 será suspensa ou desligada quando o tempo de logoff especificado expirar, dependendo das ações que você configurou. Por padrão, nenhuma ação é atribuída a máquinas com logoff. Você pode definir as ações separadamente para os horários de pico e fora de pico. Para isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **No action**. Se selecionada, a máquina após o logoff da sessão permanece ligada. O AutoScale não realiza nenhuma ação.
- **Suspend**. Se selecionada, o AutoScale pausa a máquina sem desligá-la quando o tempo de logoff especificado expira.
- **Shut down**. Se selecionada, o AutoScale desliga a máquina quando o tempo de logoff especificado expira.

> **Nota:**
>
> Essa opção está disponível somente na interface de usuário do AutoScale para grupos de entrega estáticos com SO de sessão única.

Gerenciar a energia de máquinas com SO de sessão única em transição para um período de tempo diferente com sessões desconectadas

> **Importante:**
>
> - Esta melhoria aplica-se somente às máquinas com SO de sessão única com sessões desconectadas. Ela não se aplica às máquinas as máquinas com SO de sessão única com sessões em logoff.
> - Para que esse aprimoramento entre em vigor, você precisa ativar o AutoScale para o grupo de entrega aplicável. Caso contrário, as ações da política de desconexão de energia não são disparadas na transição do período.

Em versões anteriores, uma máquina com SO de sessão única fazendo a transição para um período em que era necessária uma ação (ação de desconexão="**Suspend**"ou "**Shutdown**"), tinha de permanecer ligada. Esse cenário ocorria se a máquina se desconectasse durante um período de tempo (horários de pico ou fora de pico) em que não era necessária nenhuma ação (ação de desconexão="**Nothing**").

A partir desta versão, o AutoScale suspende ou desliga a máquina quando o tempo de desconexão especificado é decorrido, dependendo da ação de desconexão configurada para o período de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega com SO de sessão única:

- Definir `PeakDisconnectAction` como "Nothing"
- Definir `OffPeakDisconnectAction` como "Shutdown"
- Definir 'OffPeakDisconnectTimeout'como "10"

> **Nota:**
>
> Para obter mais informações sobre a política de energia para a 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 com SO de sessão única com uma sessão desconectada durante os horários de pico permanecia ligada quando fazia a transição de pico para não pico. A partir desta versão, as ações da política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina com SO de sessão única na transição do período. Como resultado, a máquina é desligada 10 minutos após a transição para o horário fora de pico.

Nesse caso, se você quiser reverter para o comportamento anterior (ou seja, não aplicar nenhuma ação em máquinas que fazem a transição de horário de pico para não pico ou de horário de não pico para pico com sessões desconectadas), execute um destes procedimentos:

- Defina o valor do registro "LegacyPeakTransitionDisconnectedBehaviour"como 1 (true; habilita o comportamento anterior). Por padrão, o valor é 0 (false; dispara ações da política de energia de desconexão na transição do período).
  - Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dados: 0x00000001 (1)
- Configure o parâmetro usando o comando `Set-BrokerServiceConfigurationData` do PowerShell. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações de política de energia possam ser aplicadas a ela na transição do período:

- Ter uma sessão desconectada.
- Não ter ações pendentes de energia.
- Pertencer a um grupo de entrega com SO de sessão única que transita para um período de tempo diferente.
- Ter uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e transita para um período em que uma ação de energia é atribuída.

Como o buffer de capacidade funciona

O buffer de capacidade é usado para adicionar capacidade de reserva à demanda atual para contabilizar aumentos de carga dinâmica. Há dois cenários que devem ser considerados:

- Para grupos de entrega com SO multissessão, 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 com 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 em que você restringe o AutoScale às 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.

O AutoScale permite que você defina o buffer de capacidade separadamente para os horários de pico e fora de pico. Um valor menor no campo de buffer de capacidade diminui o custo porque o AutoScale

aciona menos capacidade de reserva. Um valor maior garante uma experiência otimizada para que os usuários não precisem esperar que máquinas adicionais sejam ligadas ao iniciar as sessões. Por padrão, o buffer de capacidade é de 10%.

> **Importante:**
>
> O buffer de capacidade faz com que as máquinas sejam ligadas quando a capacidade total de reserva cai para um nível abaixo de "X"por cento da capacidade total do grupo de entrega. Isso reserva a porcentagem necessária de capacidade de reserva.

Grupos de entrega com SO multissessão

Quando as máquinas são ligadas?

> **Importante:**
>
> Se um agendamento for selecionado, o AutoScale ativa todas as máquinas configuradas para serem ligadas na programação agendada. O AutoScale mantém esse número especificado de máquinas ligadas durante o período programado, independentemente da carga.

Quando o número de máquinas ligadas no grupo de entrega não consegue mais atender ao buffer necessário para suprir a capacidade do buffer em termos de índice de carga, o AutoScale aciona máquinas extras. Por exemplo, digamos que o seu grupo de entrega tenha 20 máquinas e 3 máquinas estejam programadas para serem acionadas como parte do dimensionamento de sessão, de acordo com o agendamento, e com um buffer com capacidade de 20%. Ocasionalmente, 4 máquinas estarão ligadas mesmo não havendo carga. Isso ocorre porque um índice de carga de 4 x 10k é necessário para o buffer; portanto, pelo menos 4 máquinas precisam estar ligadas. Esse caso pode ocorrer durante horários de pico, aumento da carga nas máquinas, início de novas sessões, e quando você adiciona novas máquinas ao grupo de entrega. Observe que o AutoScale liga somente as máquinas que atendem aos seguintes critérios:

- As máquinas não estão no modo de manutenção.
- O hipervisor no qual as máquinas estão sendo executadas não está no modo de manutenção.
- As máquinas estão desligadas no momento.
- As máquinas não têm ações de energia pendentes.

Quando as máquinas são desligadas?

> **Importante:**
>
> - Se uma programação for selecionada, o AutoScale desliga as máquinas com base na pro-

> gramação.
> - O AutoScale não desliga as máquinas configuradas na programação para ficarem ligadas durante o período agendado.

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. Esse caso pode ocorrer fora dos horários de pico, com a diminuição da carga nas máquinas e logoffs de sessão, e quando você remove máquinas do grupo de entrega. O AutoScale desliga somente as máquinas que atendem aos seguintes critérios:

- As máquinas e o hipervisor em que as máquinas estão sendo executadas não estão no modo de manutenção.
- As máquinas estão ligadas no momento.
- As máquinas estão registradas como disponíveis ou aguardando o registro após uma 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 ficaram ligadas por pelo menos “X”minutos, sendo “X”o atraso de desligamento especificado para o grupo de entrega.

Exemplos de cenário

Suponhamos 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 de AutoScale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída na programação selecionada.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões do usuário aumentam.
3. Mais sessões de usuário começam.
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 manipulada apenas por recursos locais.

Veja abaixo os detalhes sobre como o AutoScale funciona no cenário acima.

- Sem carga do usuário (estado inicial)
  - Uma máquina (por exemplo, M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Nesse 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 (o índice de carga é 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.
- Os usuários aumentam a carga
  - As sessões são balanceadas de acordo com a carga entre as máquinas M1 e M2. Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta.
  - A capacidade total de reserva 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 de acordo com a carga entre as máquinas (M1 e M2). Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta ainda mais.
  - Quando a capacidade total de reserva 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 de acordo com a carga entre as máquinas (M1 a M3). Como resultado, o índice de carga das máquinas ligadas (M1 a M3) aumenta.
  - A capacidade total de reserva 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 fazem logoff de suas sessões ou o tempo limite das sessões ociosas expira, a capacidade liberada nas máquinas M1 a M3 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade total de reserva aumenta para um nível acima de 10.000 em termos de índice de carga, o AutoScale coloca uma das máquinas (por exemplo, M3) no estado de esvaziamento. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina, a menos que ocorram novas alterações. Por exemplo, a carga do usuário final aumenta novamente ou outras máquinas ficam menos carregadas.
- A carga da sessão do usuário continua diminuindo
  - Depois que todas as sessões na máquina M3 forem encerradas e o atraso de desligamento especificado expirar, 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 total de reserva aumenta para um nível acima de 10.000 em termos de índice de carga, o AutoScale coloca uma das máquinas (por exemplo, M2) no estado de esvaziamento. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina.
- A carga da sessão do usuário continua diminuindo até que não haja sessões
  - Depois que todas as sessões na máquina M2 forem encerradas e o atraso de desligamento especificado expirar, 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 no estado de esvaziamento devido ao buffer de capacidade configurado.

> **Nota:**
>
> Para grupos de entrega com SO multissessão, todas as alterações na área de trabalho são perdidas quando os usuários fazem logoff das sessões. No entanto, se configurados, os parâmetros específicos do usuário são movidos juntamente com o perfil do usuário.

Grupos de entrega aleatórios com SO de sessão única

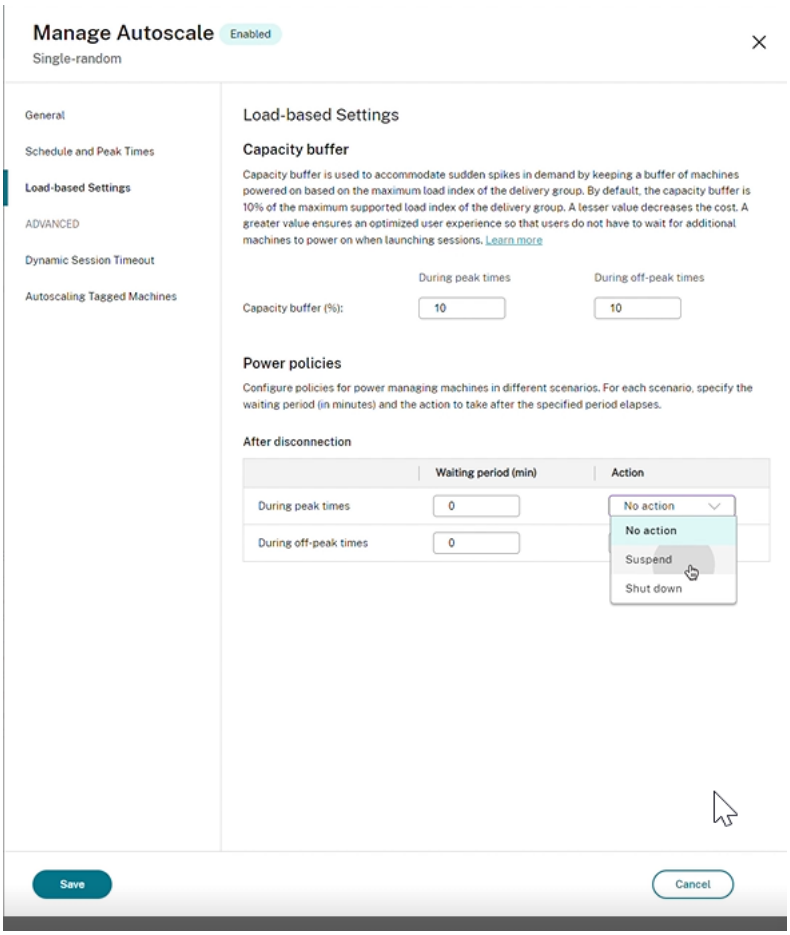
O buffer de capacidade é usado para acomodar picos repentinos na demanda, mantendo um buffer de máquinas ligado com base no número total de máquinas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas no grupo de entrega.

Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, serão ligadas máquinas adicionais 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 excedentes são encerradas ou suspensas, de acordo com as 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.

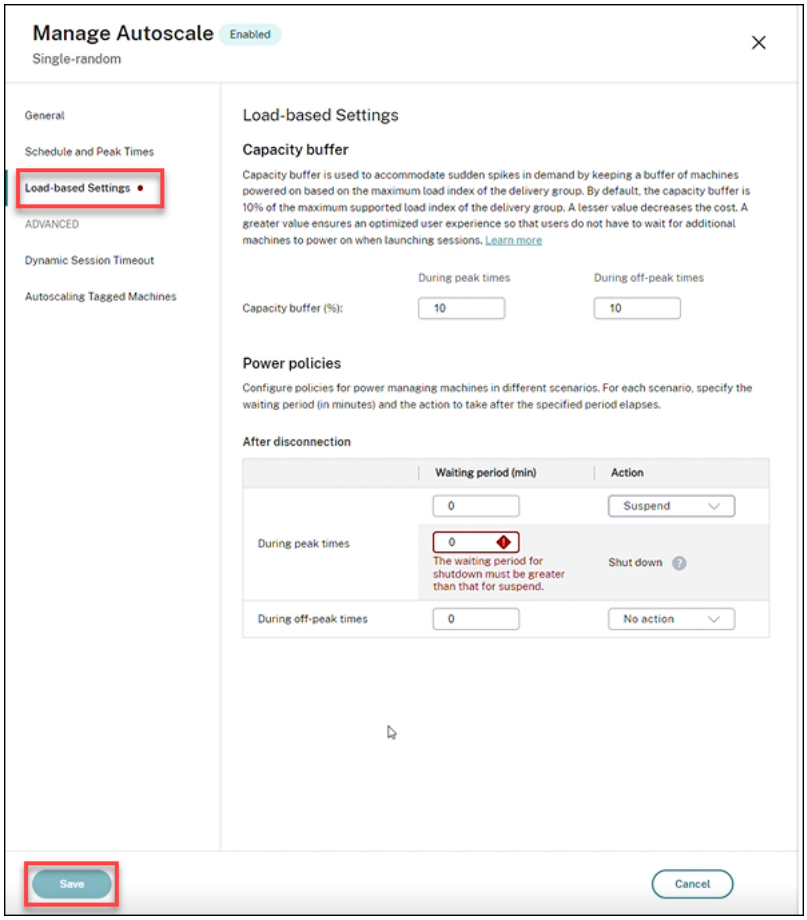


Após a desconexão, as seguintes configurações são aplicáveis tanto durante os horários de pico quanto fora dos horários de pico:

–Você pode definir o tempo de espera em minutos e ações no menu suspenso, como nenhuma ação, suspender ou desligar.

–Se você selecionar a ação de suspender, configure um tempo de espera adicional para desligar a máquina.

> **Nota:**
>
> - Durante os horários de pico e fora de pico, o tempo de espera da ação de desligar deve ser maior do que o tempo de espera da ação de suspender.
> - As máquinas suspensas só podem ser acessadas por usuários desconectados quando eles se reconectam. Para disponibilizar as máquinas suspensas para novos usuários, desligue-as.
> - Se as configurações de horário estiverem definidas incorretamente nos campos de suspender e desligar, a opção **Save** será desativada e um ponto vermelho também aparecerá 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, após o final de 12 minutos, a máquina continuará no estado ligada.
- Se você definir o tempo de espera para 15 minutos e escolher a primeira ação como suspender e definir o segundo tempo de espera para 20 minutos, ao final dos 15 minutos, a máquina será suspensa. Ao final 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, ao final dos 18 minutos, a máquina será desligada.

Exemplos de cenário

Suponhamos 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 de AutoScale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída na programação selecionada.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões do usuário aumentam.
3. Mais sessões de usuário começam.
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 manipulada apenas por recursos locais.

Veja abaixo os detalhes sobre como o AutoScale funciona no cenário acima.

- Sem carga do usuário (estado inicial)
  - Uma máquina (M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Nesse 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 em que um usuário faz logon para usar uma área de trabalho, lhe é atribuída uma área de trabalho de um pool de áreas de trabalho hospedadas em máquinas ligadas. Nesse caso, o usuário recebe uma área de trabalho 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 uma área de trabalho 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 uma área de trabalho 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 tempo limite da área de trabalho do usuário se esgota, 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 como 10%.
- Mais usuários fazem logoff até que não haja 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 estabelecida como capacidade de reserva.

> **Nota:**
>
> Para grupos de entrega aleatórios com SO de sessão única, todas as alterações na área de trabalho são perdidas quando os usuários fazem logoff das sessões. No entanto, se configurados, os parâmetros específicos do usuário são movidos juntamente com o perfil do usuário.

Grupos de entrega estáticos com SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos na demanda, mantendo um buffer de máquinas não atribuídas ligado 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 do grupo de entrega são atribuídas, o buffer de capacidade não desempenha nenhum papel na ativação ou desativação das máquinas.

Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais não atribuídas serão 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 com SO de sessão única, o AutoScale:

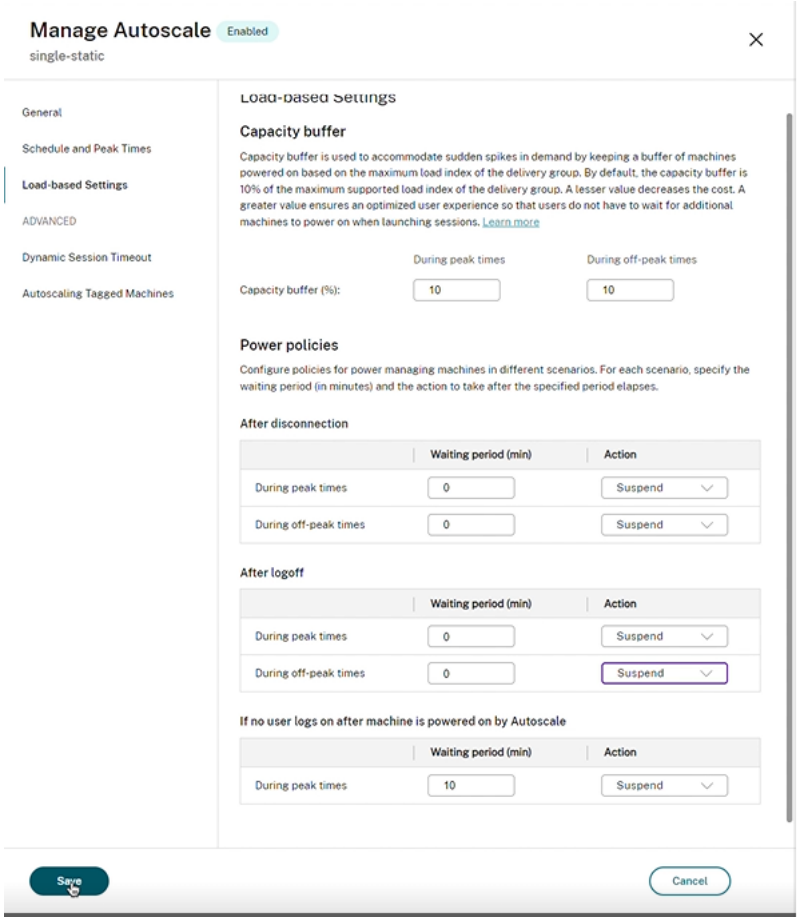
- Liga as máquinas atribuídas durante os horários de pico e desliga fora dos horários de pico somente quando a propriedade `AutomaticPowerOnForAssigned` do grupo de entrega com SO de sessão única aplicável é definida como true.
- Liga automaticamente uma máquina durante os horários de pico se ela estiver desligada e a propriedade `AutomaticPowerOnForAssignedDuringPeak` do grupo de entrega ao qual ela pertence estiver definida como true.

Para entender como o buffer de capacidade funciona com as 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 do grupo de entrega estão atribuídas), o buffer de capacidade não desempenha nenhum papel na ativação ou desativação das máquinas.
- A propriedade `AutomaticPowerOnForAssignedDuringPeak` determina se as máquinas atribuídas são ligadas durante os horários de pico. Se estiver definida como true, o AutoScale mantém as máquinas ligadas durante os horários de pico. O AutoScale também as ligará, caso 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 **After disconnection** e **After logoff**, as seguintes configurações são aplicáveis tanto durante os horários de pico quanto fora dos horários de pico:
Você pode definir o tempo de espera em minutos e ações no menu suspenso, como nenhuma ação, suspender ou desligar.

Se nenhum usuário fizer login depois que a máquina for ligada pelo Autoscale, as seguintes configurações serão aplicáveis somente durante os horários de pico:
Você pode definir o tempo de espera em minutos e ações como nenhuma ação, suspender ou desligar no menu suspenso durante os horários de pico.

Exemplos de cenário

Suponhamos 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 de AutoScale**
  - As máquinas M1 a M3 estão atribuídas e as máquinas M4 a M10 não estão atribuídas.

  - Buffer de capacidade definido como 10% para horários de pico e fora de pico.
  - De acordo com a programação selecionada, o AutoScale gerencia a energia das máquinas entre as 9h00 e as 18h00.

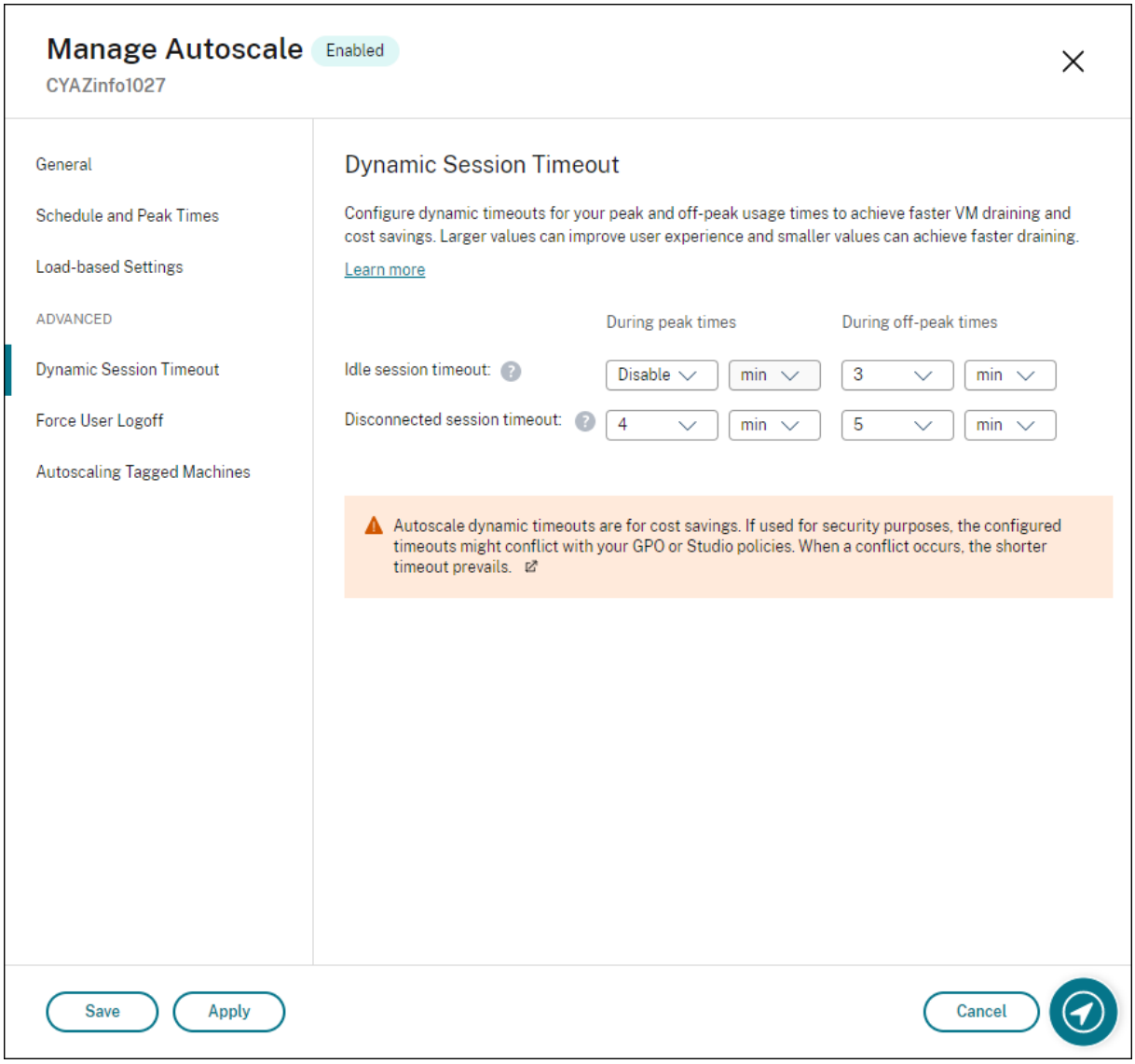
Veja abaixo os detalhes sobre como o AutoScale funciona no cenário acima.

- Início da programação agendada —9h00
  - 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 está atribuída.
- Um primeiro usuário faz logon
  - Na primeira vez em que um usuário faz logon para usar uma área de trabalho, lhe é atribuída uma área de trabalho de um pool de áreas de trabalho hospedadas em máquinas ligadas não atribuídas. Nesse caso, o usuário recebe uma área de trabalho da máquina M4. Os logons subsequentes desse usuário conectam-se à mesma área de trabalho que foi atribuída na primeira utilização.
  - 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 uma área de trabalho das máquinas ligadas não atribuídas. Nesse caso, o usuário recebe uma área de trabalho da máquina M5. Os logons subsequentes desse usuário conectam-se à mesma área de trabalho que foi atribuída na primeira utilização.
  - 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 suas áreas de trabalho ou o tempo limite das áreas de trabalho de esgota, o AutoScale mantém as máquinas M1 a M5 ligadas das 9h00 às 18h00. Quando esses usuários fizerem logon na próxima vez, eles se conectarão à mesma área de trabalho atribuída no primeiro uso.
  - A máquina M6 não atribuída está aguardando para servir como área de trabalho para um usuário não atribuído que entre.
- Fim da programação —18h00
  - Às 18h00, o AutoScale desliga as máquinas M1 a M5.
  - O AutoScale mantém a máquina não atribuída M6 ligada devido ao buffer de capacidade configurado. A máquina está aguardando para servir como área de trabalho para um usuário não atribuído que entre.
  - No grupo de entrega, as máquinas M6 a M10 são máquinas não atribuídas.

Tempo limite de sessão dinâmica

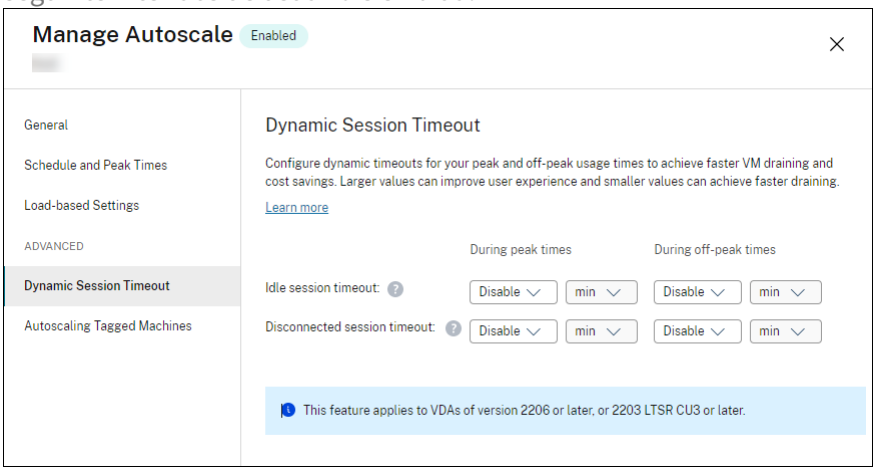
June 26, 2023

Esse recurso permite configurar tempos limite de sessão desconectada e ociosa para os horários de uso de pico e fora de pico para obter um esvaziamento mais rápido da máquina e economia de custos. Esse recurso se aplica a máquinas com SO de sessão única e multissessão. Um VDA relata tempos ociosos para sessões que ficaram ociosas por mais de 10 minutos, portanto, os tempos limite de sessão dinâmicos não poderão desconectar as sessões ociosas dentro de um intervalo de 10 minutos após ficarem ociosas. Um valor menor remove as sessões prolongadas mais cedo, reduzindo assim os custos.



Nota:

- Esse recurso está sempre disponível para grupos de entrega com SO multissessão.
- Para grupos de entrega de SO de sessão única, esse recurso se aplica aos VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Certifique-se de que os VDAs tenham se registrado no Citrix Cloud pelo menos uma vez. Quando não estiver disponível, a seguinte interface de usuário é exibida:



- Os tempos limite dinâmicos de AutoScale são para economia de custos. Se usado para fins de segurança, os tempos limite configurados podem entrar em conflito com seu objeto de política de grupo ou com as políticas do console Manage. Quando ocorre um conflito, o tempo limite mais curto prevalece.

Idle session timeout. Habilita ou desabilita um timer que especifica por quanto tempo uma conexão de usuário ininterrupta é mantida se não houver atividade pelo usuário. Quando o timer expira, a sessão é colocada no estado desconectado e aplica-se o que está definido em **Disconnected session timeout**. Se **Disconnected session timeout** estiver desativado, a sessão não será desconectada.

Importante:

- Se você especificar um valor menor ou igual a 10 minutos (600 segundos), AutoScale desconectará as sessões relevantes depois que elas estiverem ociosas por 10 minutos. Isso ocorre porque o AutoScale depende dos tempos ociosos da sessão relatados pelos VDAs. Os VDAs relatam tempos ociosos somente para sessões que ficaram 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 após atingir o tempo limite da sessão ociosa.

Disconnected session timeout. Ativa ou desativa um timer que especifica por quanto tempo uma área de trabalho desconectada permanece bloqueada antes que a sessão seja desconectada. Se ativado, a sessão desconectada é desconectada quando o timer expira.

Máquinas marcadas com tag no AutoScale (intermitência da nuvem)

March 3, 2023

> **Nota:**
>
> Anteriormente, esse era o recurso Restrict Autoscale.

Introdução

O AutoScale fornece a flexibilidade para gerenciar a energia de somente um subconjunto de máquinas em um grupo de entrega. Para isso, aplique uma marca a uma ou mais máquinas e, em seguida, configure o AutoScale para gerenciar somente as máquinas marcadas.

Esse recurso pode ser útil em casos de uso de intermitência da nuvem, em que você deseja usar recursos locais (ou instâncias de nuvem pública reservadas) para lidar com cargas de trabalho antes que os recursos baseados em nuvem abordem a demanda adicional (ou seja, cargas de trabalho intermitentes). Para permitir que as máquinas locais (ou instâncias reservadas) abordem as cargas de trabalho primeiro, você deve usar a restrição de marca juntamente com a preferência de zona.

A restrição de marca especifica as máquinas a terem sua energia gerenciada pelo AutoScale. A preferência de zona especifica máquinas na zona preferida para lidar com solicitações de inicialização do usuário. Para obter mais informações, consulte Marcas e Preferência de zona.

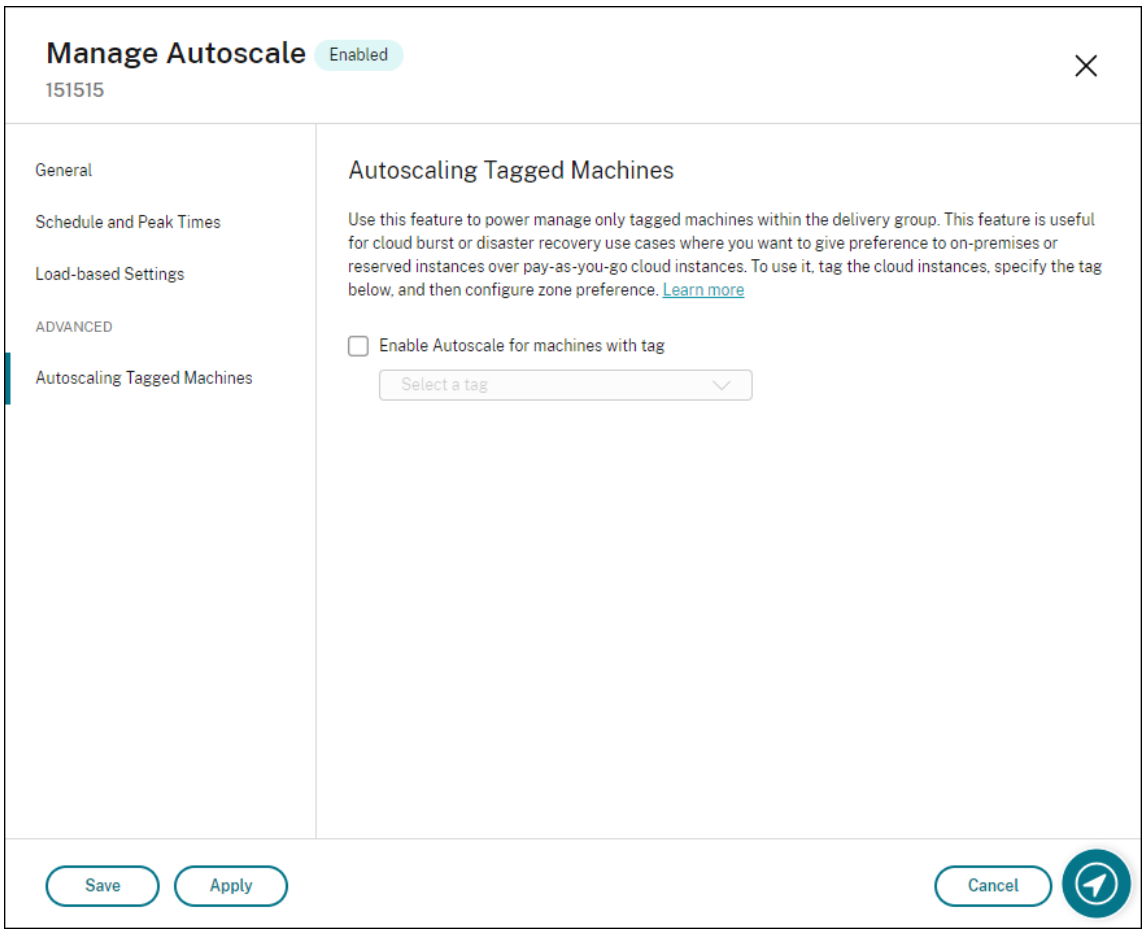
Para aplicar o AutoScale a determinadas máquinas marcadas, você pode usar o console Manage ou o PowerShell.

Usar o console Manage para aplicar o AutoScale a determinadas máquinas marcadas

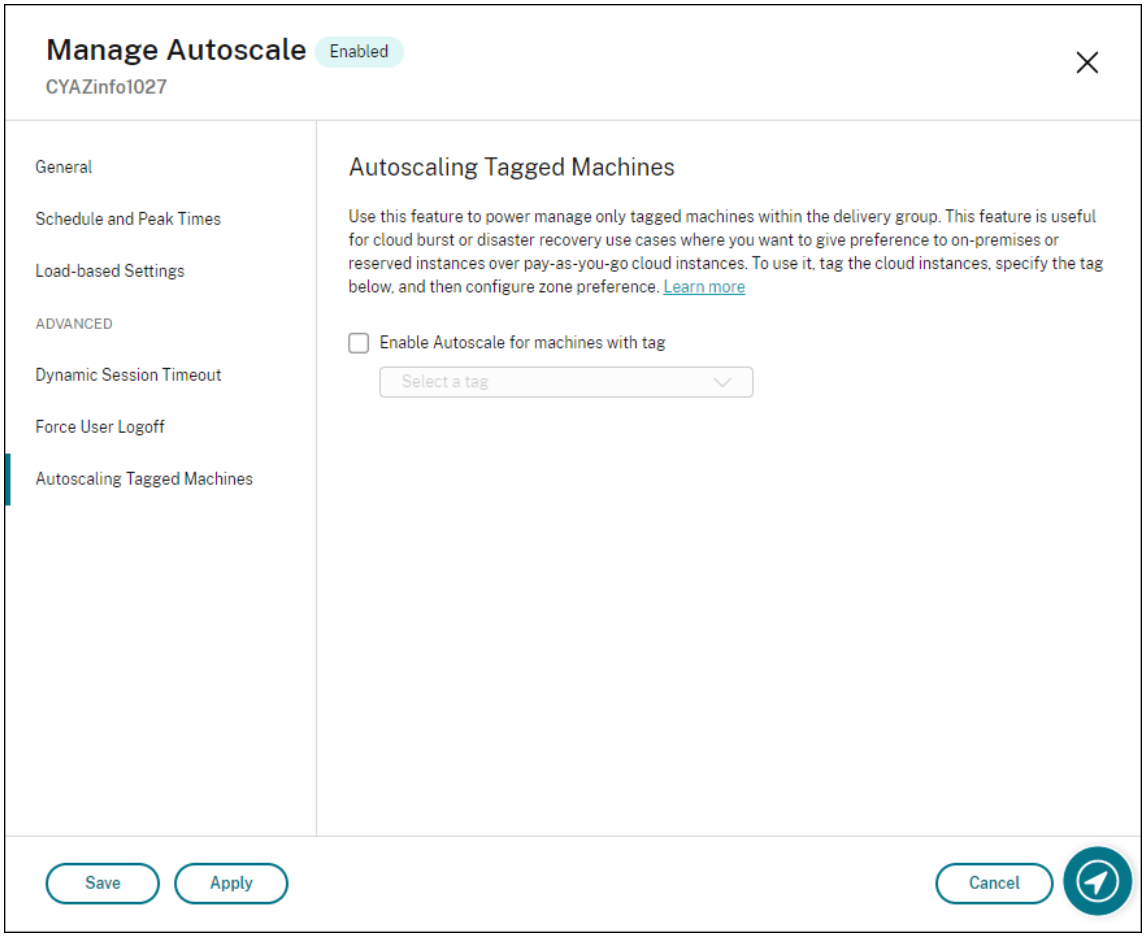
Para aplicar o AutoScale a determinadas máquinas marcadas, conclua as seguintes etapas:

1. Crie uma marca e aplique essa marca às máquinas aplicáveis no grupo de entrega. Para obter mais informações, consulte Gerenciar marcas e restrições de marca.
2. Selecione o grupo de entrega e, em seguida, abra o assistente **Manage AutoScale**.
3. Na página **Autoscaling Tagged Machines**, selecione **Enable Autoscale for machines with tag**, selecione uma marca na lista e clique em **Apply** para salvar as alterações.

   Interface do usuário para grupos de entrega *estáticos* e *aleatórios* com SO de sessão única:



Interface do usuário para *grupos de entrega com SO multissessão*:



> **Aviso:**
>
> - Aplicar o AutoScale a máquinas com uma marca específica pode fazer com que o histograma seja atualizado automaticamente para refletir o número de máquinas por marcação. Na página **Schedule and Peak Times**, você pode atribuir manualmente máquinas a cada intervalo de tempo, se necessário.
> - Você não pode excluir uma marca que está sendo usada em máquinas marcadas. Para excluir a marcação, você deve primeiro remover a restrição da marca.

Depois de aplicar a restrição da marca, você pode removê-la do grupo de entrega mais tarde se assim desejar. Para isso, vá para a página **Manage Autoscale > Autoscaling Tagged Machines** e desmarque **Enable Autoscale for machines with tag**.

> **Aviso:**
>
> - Se você remover a marca das máquinas aplicáveis sem desmarcar **Enable Autoscale for machines with tag**, poderá receber um aviso ao abrir o assistente **Manage Autoscale**. Remover a marcação das máquinas pode acabar deixando o AutoScale sem nenhuma

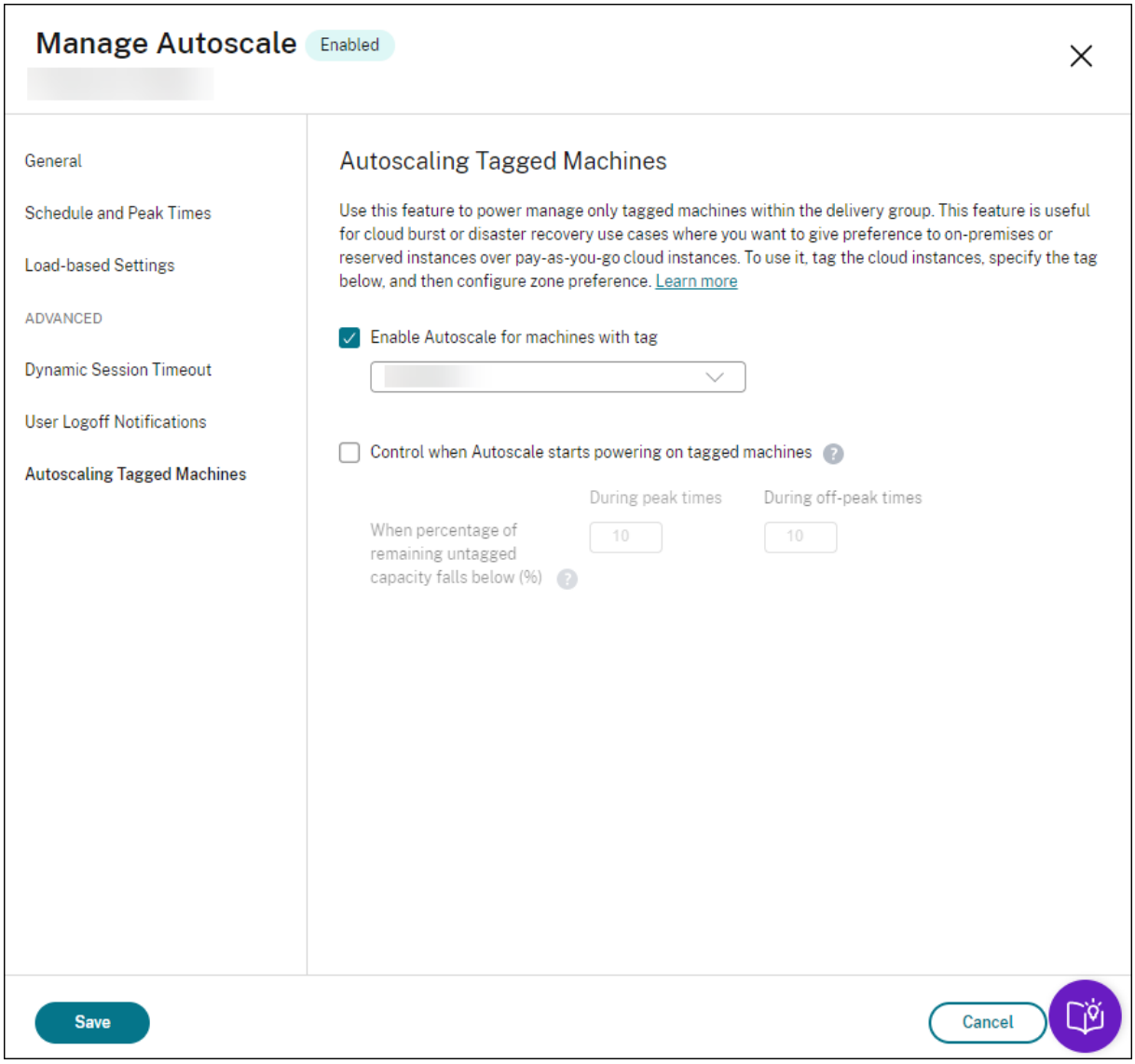
> máquina para gerenciar porque a marca que você especificou no AutoScale se torna inválida. Para resolver o aviso, acesse a página **Autoscaling Tagged Machines**, remova a marca inválida e clique em **Apply** para salvar as alterações.

Controle quando o AutoScale liga os recursos

Você também pode controlar quando o AutoScale começa a ligar as máquinas marcadas baseado no uso das máquinas não marcadas. Isso ajuda a otimizar ainda mais o consumo de suas cargas de trabalho marcadas ou da nuvem pública.

Para isso, conclua as seguintes etapas:

1. Na página **Autoscaling Tagged Machines**, selecione **Control when Autoscale starts powering on tagged machines**.
2. Insira a porcentagem de uso de máquinas não marcadas que você deseja alcançar nos horários de pico e fora de pico e clique em **Apply**. 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 com 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 com SO de sessão única não marcadas. Quando apenas uma fica sem uma sessão, o AutoScale começa a ligar uma máquina marcada.
- Para grupos de entrega com SO multissessão: o valor é definido como uma porcentagem da capacidade total (em termos de índice de carga) das máquinas não marcadas disponíveis.

> Exemplo: você tem 10 máquinas com SO multissessão não marcadas. Quando estão 90% carregadas, o AutoScale começa a ligar uma máquina etiquetada.

Usar o PowerShell para aplicar o AutoScale a determinadas máquinas marcadas

Para usar o SDK do PowerShell diretamente, conclua as seguintes etapas:

1. **Crie uma marca.** Use o comando New-Brokertag do PowerShell para criar uma marca.
   - Por exemplo: `$managed = New-BrokerTag Managed`. Nesse caso, a marca é chamada de "Managed". Para obter mais informações sobre o comando New-Brokertag do PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Aplique a marca às máquinas**. Use o comando Get-Brokermachine do PowerShell para aplicar a marca às máquinas em um catálogo que você deseja aplicar o AutoScale para gerenciar a energia.
   - Por exemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. Nesse caso, o catálogo é chamado de "cloud".
   - Para obter mais informações sobre o comando Get-Brokermachine do PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Nota:**
   >
   > Você pode adicionar novas máquinas ao catálogo depois de aplicar a marca. A marca *NÃO* é aplicada automaticamente a essas novas máquinas.

3. **Adicione máquinas marcadas ao grupo de entrega que você deseja que a energia seja gerenciada pelo AutoScale.** Use o comando Get-BrokerDesktopGroup do PowerShell para adicionar uma restrição de marca ao grupo de entrega que contém as máquinas (em outras palavras, "restringir inicializações a máquinas com a marca X").
   - Por exemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. Nesse caso, o UID do grupo de entrega é 1.
   - Para obter mais informações sobre o comando Get-BrokerDesktopGroup do PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Depois de aplicar a restrição da marca, você pode removê-la do grupo de entrega mais tarde se assim desejar. Para isso, use o comando Get-BrokerDesktopGroup do PowerShell.

Exemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscal $null`. Nesse caso, o UID do grupo de entrega é 1.

> **Nota:**
>
> As máquinas não marcadas são reiniciadas automaticamente depois que os usuários as desligam. Esse comportamento garante que fiquem disponíveis para lidar com cargas de trabalho mais cedo. Isso pode ser ativado ou desativado em um grupo por área de trabalho usando a propriedade `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para obter mais informações, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

Exemplos de cenário

Suponhamos 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 marca** Uma marca 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 do catálogo 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 programado.
- **Configuração de AutoScale**
  - O buffer de capacidade está definido para 10%.
  - A energia do AutoScale gerencia apenas máquinas com a marca "Cloud". Nesse caso, a energia do AutoScale gerencia as máquinas na nuvem de M6 a M10.
- **Configuração do aplicativo ou da área de trabalho publicada**. As preferências de zona são configuradas para as áreas de trabalho publicadas (por exemplo), em que a Zona Z1 é preferida à Zona Z2 para uma solicitação de inicialização do usuário.

  - A zona Z1 é configurada como a zona preferida (zona inicial) para as áreas de trabalho publicadas.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões do usuário aumentam.
3. As sessões de usuário aumentam ainda mais até que todas as máquinas locais disponíveis sejam consumidas.
4. Mais sessões de usuário começam.
5. A sessão do usuário diminui devido ao encerramento da sessão.
6. A sessão do usuário diminui ainda mais até que a carga da sessão seja manipulada apenas por máquinas locais.

Veja abaixo os detalhes sobre como o AutoScale funciona no cenário acima.

- Sem carga do usuário (estado inicial)
  - As máquinas locais M1 a M5 são todas ligadas.
  - Uma máquina na nuvem (por exemplo, M6) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Nesse 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 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 por meio da preferência de zona configurada e têm balanceamento de carga realizado 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.
- Os usuários aumentam a carga, consumindo todos os recursos locais
  - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 por meio da preferência de zona configurada e têm balanceamento de carga realizado entre essas máquinas locais.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atinge 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 estoura a preferência de zona e é direcionada para ser hospedada na máquina M6 na nuvem.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atinge 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 total de reserva 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) atinge 10.000.
  - O valor do índice de carga da máquina ligada M6 aumenta ainda mais, mas a capacidade total de reserva 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 está pronta, as sessões são direcionadas para serem hospedadas nas máquinas M6 e M7 e têm balanceamento de carga realizado entre essas máquinas.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atinge 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 total de reserva 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 o tempo limite das sessões ociosas expira, a capacidade liberada nas máquinas M1 a M7 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade total de reserva aumenta para um nível acima de 10.000 em termos de índice de carga, o AutoScale coloca uma das máquinas na nuvem (M6 a M7) no estado de esvaziamento. 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 aumente novamente ou outras máquinas na nuvem fiquem menos carregadas.

- A carga da sessão do usuário diminui ainda mais até que uma ou mais máquinas na nuvem não sejam mais necessárias

  - Depois que todas as sessões na máquina M7 forem encerradas e o atraso de desligamento especificado expirar, 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 na nuvem seja necessária

  - Mesmo que não haja sessões de usuário na máquina M6, o AutoScale não a desliga porque ela está reservada como capacidade de reserva.
  - O AutoScale mantém a máquina M6 na nuvem restante ligada devido ao buffer de capacidade configurado. Essa máquina está esperando para servir uma área de trabalho para um usuário que entre.
  - As sessões não são direcionadas para serem hospedadas na máquina M6, desde que as máquinas locais tenham capacidade disponível.

Provisionar máquinas dinamicamente

November 28, 2022

O AutoScale oferece a capacidade de criar máquinas e excluí-las dinamicamente. Você pode aproveitar o recurso usando um script do PowerShell. O script ajuda a aumentar ou diminuir dinamicamente o número de máquinas no grupo de entrega com base nas condições de carga atuais.

O script oferece os seguintes benefícios (e mais):

- **Redução dos custos de armazenamento**. O AutoScale ajuda a reduzir os custos de computação, mas o script fornece uma solução mais econômica e rentável para o provisionamento de máquinas.
- **Manipulação eficaz das mudanças de carga** O script ajuda a lidar com as alterações de carga aumentando ou diminuindo automaticamente o número de máquinas com base na carga atual do grupo de entrega.

Baixar o script

O script do 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 que deve 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 para o mesmo grupo de entrega de várias localizações simultaneamente.

O script funciona no nível de grupo de entrega. Ele mede a carga (em termos de índice de carga) e, em seguida, determina se as máquinas devem ser criadas ou excluídas.

As máquinas criadas por meio desse script são marcadas exclusivamente (por meio 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 criar máquinas no AutoScale para lidar com cargas extras. Quando esse limite é excedido, as máquinas são criadas em lotes para garantir que a carga atual diminua até esse limite ou abaixo.
- **Carga percentual mínima de um grupo de entrega**. Especifica o nível mínimo no qual excluir máquinas criadas por meio desse script que não têm sessões ativas. Quando esse limite é excedido, as máquinas criadas por meio desse script que não têm sessões ativas são excluídas.

Esse script tem como objetivo monitorar um grupo de entrega e criar ou excluir máquinas quando o critério do gatilho for disparado. Ele é executado baseado nas execuções específicas. Isso significa que você precisa executar o script regularmente para que ele possa funcionar 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	Cadeia de caracteres	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. Por exemplo: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3'-XdProfileName profile`.
XdProfileName	Cadeia de caracteres	X	Nome do perfil a ser usado para autenticação em servidores remotos. Para obter detalhes sobre a autenticação em servidores remotos usando esse 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 as cargas extras.

Parâmetro	Tipo	Valor padrão	Descrição
LowWatermark	Inteiro	15	Carga percentual mínima (em termos de índice de carga) na qual excluir máquinas criadas por meio do script que não têm sessões ativas.
MachineCatalogName	Cadeia de caracteres	X	Nome do catálogo de máquinas onde as máquinas devem ser criadas.
MaximumCreatedMachines	Inteiro	-1	Quantidade máxima 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 esse parâmetro.
ScriptTag	Cadeia de caracteres	AutoscaledScripted	A marca que se aplica às máquinas criadas por meio do script.
EventLogSource	Cadeia de caracteres	X	Nome da origem que aparece no Visualizador de Eventos do Windows.

> **Nota:**
>
> Um “X”indica que nenhum valor padrão é especificado para o parâmetro.

Por padrão, o script requer todos os parâmetros (exceto o parâmetro `ScriptTag`) na primeira vez em que é executado. Nas execuções subsequentes, somente 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 a primeira vez que executar o script. Por exemplo, o script *não* funciona se você usar o seguinte comando do PowerShell para especificar

dois grupos de entrega a 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 em que as máquinas estão sendo criadas.
- O SDK do PowerShell remoto está instalado nessa máquina. Para obter mais informações sobre o Remote PowerShell SDK, consulte SDKs e APIs.
- Outros pré-requisitos:
  - Um grupo de entrega para monitorar
  - Um catálogo de máquinas criado por meio do MCS (Machine Creation Services) que tem um esquema de provisionamento associado (modelo)
  - Um pool de identidade associado ao esquema de provisionamento
  - A origem do log de eventos a ser criada para que o script possa gravar informações no log de eventos do Windows
  - Um cliente seguro que permita que você faça a autenticação em servidores remotos

Permissões, recomendações e avisos

Ao executar o script, tenha em mente o seguinte:

- Para se 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 API de autenticação.

- 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 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>`. Em seguida, você pode 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 solucione os problemas efetuando verificações do 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 na 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, conclua estas etapas:

1. Faça login no Citrix Cloud e navegue até **Identity and Access Management > API Access**.
2. Digite o nome do seu cliente seguro e clique em **Create Client**.

Para autenticar-se em servidores remotos, use o comando `Set-XDCredentials` do PowerShell. 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 do PowerShell com o Agendador de Tarefas do Windows. Isso permite que o script seja executado automaticamente em determinados intervalos ou quando determinadas condições são atendidas. Para executar esse script com o Agendador de Tarefas do Windows, selecione **Não iniciar uma nova instância** na guia **Criar tarefa > Configurações**. Isso impede que o Agendador de Tarefas do Windows execute uma nova instância se o script 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, em seguida, encerrada.

```
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName devtest -XdProfileName profile -MachineCatalogName autoscaled -ScriptTag "devtest"
[devtest]: Assuming default values for watermarks [15 : 80].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName engtest -XdProfileName profile -MachineCatalogName autoscaled2 -ScriptTag "engtest"
[engtest]: Assuming default values for watermarks [15 : 80].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Provisioning more machines. Current Usage [99.99] >= High Watermark [80].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Began provisioning of [1] machines to [engtest]. Monitoring task [ca2b0cad-9c50-4e20-8f1d-9ff81307b201].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Provisioning task [ca2b0cad-9c50-4e20-8f1d-9ff81307b201] is complete. [1] created. [0] failed to create.

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Added [1] machines to [engtest].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Removing extraneous machines: Current Usage [0] <= Low Watermark [15].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Removing [1] machines from [engtest]. Monitoring task [28c6c242-af81-4693-a2a8-0587f09689b4]

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Machine deletion task [28c6c242-af81-4693-a2a8-0587f09689b4] is [Finished].

PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
```

Lista de verificação para a solução de problemas do script

O script grava informações (por exemplo, erros e ações) no Log de Eventos do Windows. As informações ajudam a solucionar os problemas que você tenha ao executar o script. A seguinte lista se mostrou útil para a verificação de problemas e possíveis soluções:

- 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 está executando 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 da máquina (ou seja, se a sua imagem ainda existe e se 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.

Notificações de logoff do usuário (anteriormente forçar logoff de usuário)

June 6, 2023

> **Importante:**
>
> Esse recurso está disponível somente na interface do usuário do AutoScale para grupos de entrega baseados em aplicativos multissessão.

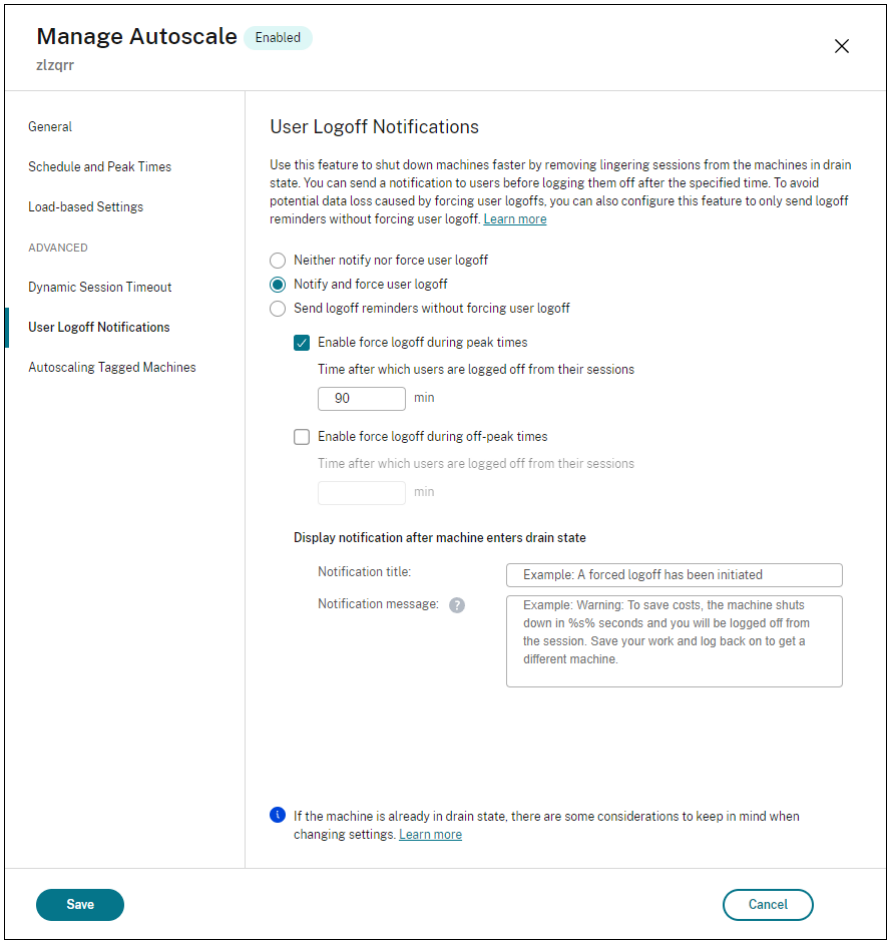
Para obter maior economia de custos, o AutoScale permite forçar o logoff em sessões prolongadas. Ele faz isso permitindo que você envie uma notificação personalizada aos usuários e especifique um período de tolerância após o qual o logoff das sessões é feito à força. Isso é feito apenas para máquinas no estado de esvaziamento e não para todas as máquinas ligadas. Para evitar a possível perda de dados causada por logoffs de usuário forçados, você pode configurar esse recurso para apenas enviar lembretes de logoff, sem forçar o logoff do usuário.

Você tem as seguintes opções:

- **Notify and force user logoff**
- **Send logoff reminders without forcing user logoff**
- **Neither notify nor force user logoff**

Notify and force user logoff

Se selecionada, o AutoScale faz o logoff dos usuários de suas sessões após os tempos especificados abaixo.



Enable force logoff during peak times. Se selecionada, o AutoScale faz o logoff desses usuários de suas sessões durante os horários de pico, quando o tempo especificado termina.

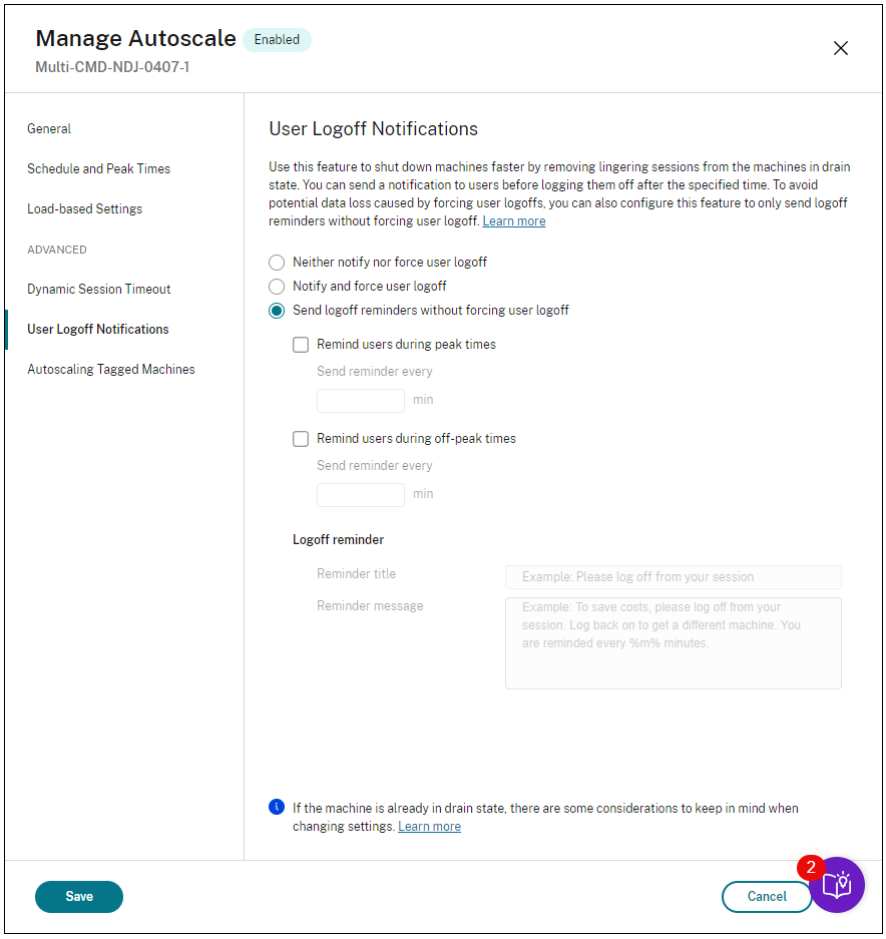
Enable force logoff during off-peak times. Se selecionada, o AutoScale faz o logoff desses usuários de suas sessões fora dos horários de pico, quando o tempo especificado termina.

Display notification after machine enters drain state. Permite enviar notificações aos usuários após a máquina entrar no estado de esvaziamento.

- **Notification title**. Permite especificar um título para a notificação a ser enviada aos usuários. Exemplo: `A forced logoff has been initiated`.
- **Notification message**. Permite especificar o conteúdo da notificação a ser enviada aos usuários. Você pode usar %s% ou %m% como variáveis para indicar a hora especificada 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.`

Send logoff reminders without forcing user logoff

Se selecionada, os usuários receberão um lembrete para fazer logoff da máquina depois que ela entrar no estado de esvaziamento. Esse lembrete pode ser configurado para ser enviado no intervalo especificado abaixo.



Remind users during peak times. Se selecionada, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de pico a cada X minutos (X indica o tempo especificado).

Remind users during off-peak times. Se selecionada, os usuários recebem um lembrete para fazer logoff de suas sessões fora dos horários de pico a cada X minutos (X indica o tempo especificado).

Logoff reminder. Permite configurar o lembrete enviado aos usuários após a máquina entrar no estado de esvaziamento.

- **Reminder title**. Permite especificar um título para o lembrete a ser enviado aos usuários. Exemplo: `Please log off from your session`.
- **Reminder message**. Permite especificar a mensagem a ser enviada aos usuários. Exemplo: `Please log off from your session and log back on to save costs`.

Neither notify nor force user logoff

Se selecionada, o AutoScale não força os usuários a se desconectarem das máquinas em estado de esvaziamento nem notifica os usuários a mudarem manualmente para uma máquina diferente.

Considerações

Se a máquina já estiver no estado de esvaziamento, considere o seguinte ao alterar as configurações:

- Se você alterar a configuração de **Send logoff reminders without forcing user logoff** para **Notify and force user logoff**, a nova configuração entra em vigor imediatamente.
- Se você alterar a configuração de **Notify and force user logoff** para **Send logoff reminders without forcing user logoff**, a nova configuração não entra em vigor até a próxima vez que a máquina entrar no estado de esvaziamento. O usuário continua a ser forçado a fazer logoff.

Analisar a eficiência das configurações do AutoScale

December 20, 2023

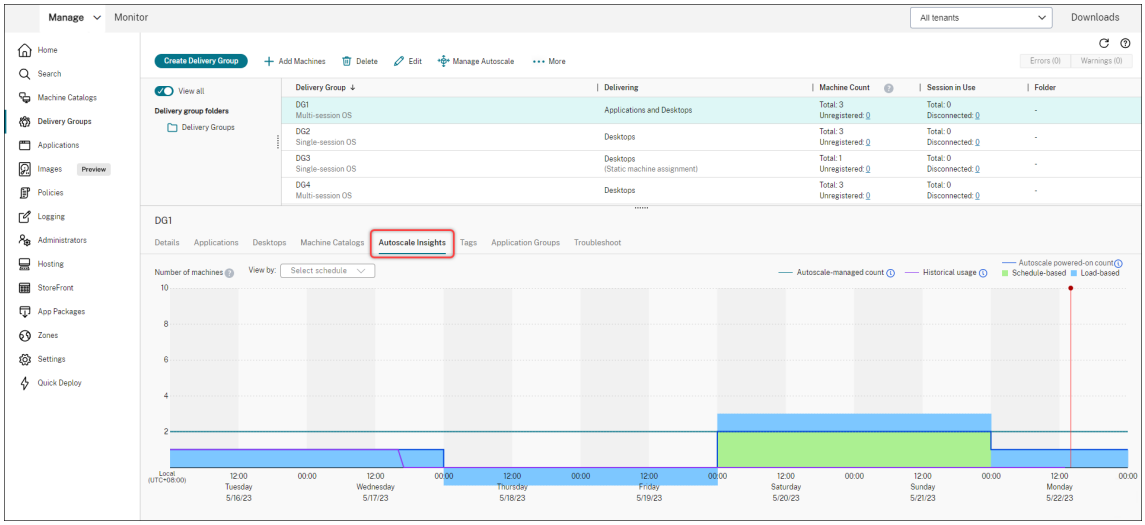
Você pode analisar a eficácia das configurações do AutoScale com base no uso da máquina na semana anterior. Por meio da análise, você pode obter esses insights sobre a eficiência das configurações do AutoScale:

- Identificar desperdício financeiro resultante do provisionamento excessivo.
- Determinar se a experiência do usuário é afetada negativamente devido ao provisionamento insuficiente.
- Certificar-se de que a capacidade provisionada esteja alinhada adequadamente com o uso da máquina.

Para atingir esse objetivo, siga estas etapas:

1. Selecione um grupo de entrega habilitado para AutoScale.
2. No painel inferior, clique na guia **Autoscale Insights**.

   O gráfico a seguir é exibido, 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.

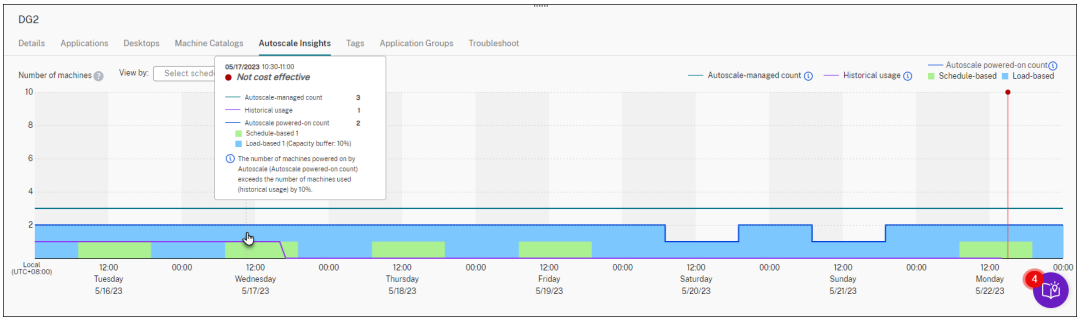
A tabela a seguir fornece descrições das métricas mostradas no gráfico.

Métrica	Descrição
Autoscale-managed count	Número total de máquinas gerenciadas pelo AutoScale. Autoscale-managed count = Número total de máquinas no grupo de entrega — Número de máquinas no modo de manutenção —Número de máquinas não marcadas para AutoScale (se o recurso de marcação de AutoScale estiver ativado).
Autoscale powered-on count	Número total de máquinas ativadas pelo AutoScale. Autoscale powered-on count = Contagem de máquinas com base em cronograma + Contagem de máquinas com base em carga.
Historical usage	Número de máquinas que foram entregues aos usuários.
Schedule-based	Número de máquinas que são ativadas com base nas configurações baseadas em cronograma do AutoScale (**Observação:** as configurações baseadas em cronograma não se aplicam a grupos de entrega do tipo de OS de sessão única estático).

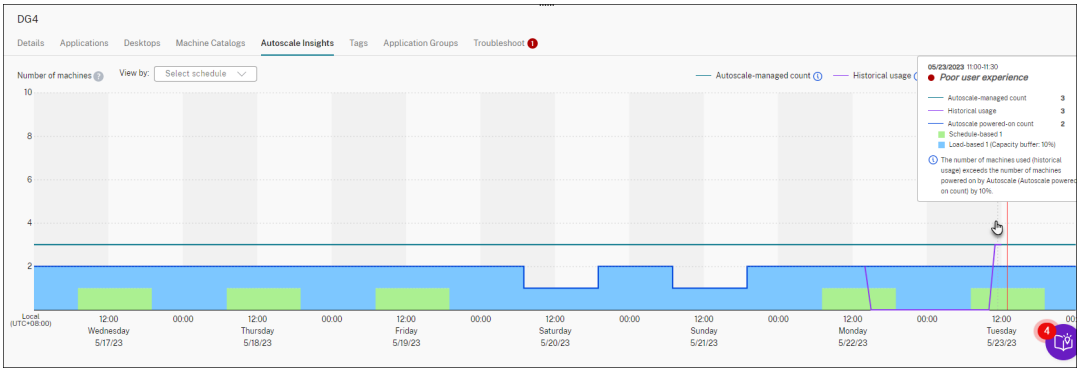
Métrica	Descrição
Load-based	Número de máquinas que são ligadas com base nas configurações baseadas na carga da AutoScale.

3. Para verificar a eficiência das configurações do AutoScale em um horário específico, passe o mouse sobre o slot no gráfico. Uma caixa de informações é exibida, mostrando os resultados de comparação e as contagens detalhadas das máquinas:

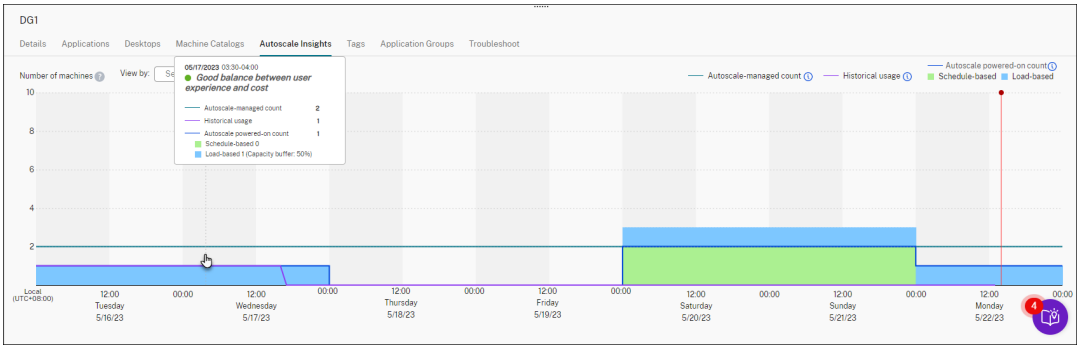
   - **Not cost effective**. O uso histórico é inferior a 90% das configurações do AutoScale (contagem ativada do AutoScale). Como resultado, pode haver desperdício de capacidade.



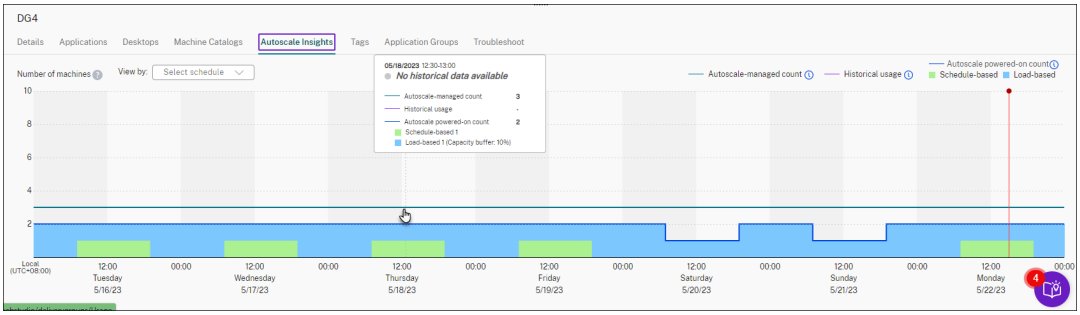
   - **Poor user experience**. O uso histórico é superior a 110% das configurações de AutoScale (contagem ativada do AutoScale). Como resultado, os usuários podem enfrentar tempos de espera mais longos para que as máquinas sejam ligadas.



   - **Good balance between user experience and cost**. A diferença entre o uso histórico e as configurações do AutoScale (contagem ativada do AutoScale) é inferior a 10%. As configurações do AutoScale estão alinhadas com o uso histórico.



- **No historical data available**. Não há dados históricos disponíveis. As possíveis causas incluem a ativação do AutoScale para o grupo de entrega há menos de uma semana.



4. Para destacar um intervalo de datas com base em uma programação do AutoScale, selecione a programação no campo **View by**.
5. Com base na sua análise, ajuste as configurações do AutoScale. Para obter mais informações, consulte Configurações baseadas em agendamento e carga.

Comandos do Broker PowerShell SDK

November 21, 2023

Você pode configurar o AutoScale para grupos de entrega usando o Broker PowerShell SDK. Para configurar o AutoScale usando comandos do PowerShell, você deve usar o Remote PowerShell SDK versão 7.21.0.12 ou posterior. Para obter mais informações sobre o Remote PowerShell SDK, consulte SDKs e APIs.

Set-BrokerDesktopGroup

Desativa ou ativa um BrokerDesktopGroup existente ou altera suas configurações. Para obter mais informações sobre esse 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.

Ativar AutoScale

- Suponha que você queira ativar o AutoScale para o grupo de entrega cujo nome é “MyDesktop” . Use o comando do 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 a 20% para horários de pico e 10% para horários fora de pico para um grupo de entrega cujo nome é “MyDesktop”. Use o comando do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
    ```

Configurar o parâmetro **when disconnected timeout**

- Suponha que você queira definir o tempo limite em **when disconnected timeout** como 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 do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
    ```

Configurar o parâmetro **when logged off timeout**

- Suponha que você queira definir o tempo limite em **when logged off timeout** como 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 do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30
    ```

Configurar o parâmetro **power-off delay**

- Suponha que você queira definir o atraso de desligamento como 15 minutos para um grupo de entrega cujo nome é “MyDesktop”. Use o comando do 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 30 minutos decorridos para um grupo de entrega cujo nome é "MyDesktop". Use o comando do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh 30.`

Configurar o parâmetro **machine instance cost**

- Suponha que você queira definir o custo da instância de máquina por hora como 0,2 dólar para um grupo de entrega cujo nome é "MyDesktop". Use o comando do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2`

## 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 de UID é 3. O novo esquema abrange fim de semana, segunda-feira e terça-feira. O horário das 8h00 às 18h30 é definido como horário 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 `Set-BrokerDesktopGroup` do PowerShell. 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 tempo limite de sessão dinâmica

Os seguintes cmdlets do SDK do Broker PowerShell foram estendidos para tempo limite de sessão dinâmica, oferecendo suporte a vários 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. Essa propriedade tem um valor padrão de 0, que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 permite o seu comportamento para o grupo de entrega somente durante o horário de pico.
- **DisconnectOffPeakIdleSessionAfterSeconds** –Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante os horários fora de pico. O valor padrão dessa propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário fora do pico. Um valor maior que 0 ativa o seu comportamento associado para o grupo de entrega somente fora do horário de pico.
- **LogoffPeakDisconnectedSessionAfterSeconds** –Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de pico. O valor padrão dessa propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 ativa o seu comportamento associado para o grupo de entrega somente durante o horário de pico.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** –Representa o tempo, em segundos, após o qual uma sessão desconectada é encerrada durante o horário fora de pico. O valor padrão dessa propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário fora do pico. Um valor maior que 0 ativa o seu comportamento associado para o grupo de entrega somente fora do horário de pico.

#### Exemplo

Suponha que você queira definir o tempo limite da sessão ociosa para 3.600 segundos durante os horários de pico para um grupo de entrega cujo nome é “MyDesktop”. Use o comando do PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte
  3600
  ```

Isso desconecta as sessões que ficaram ociosas por mais de 1 hora no horário fora do pico para o grupo de áreas de trabalho cujo nome é “MyDesktop”.


  ```

# Cloud Health Check

December 13, 2022

> **Nota:**
>
> O Cloud Health Check está integrado ao Citrix DaaS. A integração está disponível como a ação Run Health Check na interface de gerenciamento Full Configuration. Para obter mais informações, consulte Solucionar problemas de registro do VDA e início de sessão.

O Cloud Health Check permite executar verificações que avaliam a integridade e a disponibilidade do site e de seus componentes. Você pode executar verificações de integridade para Virtual Delivery Agents (VDAs), servidores StoreFront e Profile Management. As verificações de integridade do VDA identificam possíveis causas para problemas comuns de registro VDA e inicializações de sessão.

Se houver problemas durante as verificações, o Cloud Health Check fornece um relatório detalhado e as ações para corrigi-los. Sempre que o Cloud Health Check é iniciado, ele verifica a versão mais recente dos scripts na CDN (Content Delivery Network) e baixa automaticamente os scripts se não estiverem presentes 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 sempre 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:**
>
> Não é possível 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 esse arquivo para solucionar problemas.

Veja uma introdução ao Cloud Health Check.

Veja quando usar o Cloud Health Check.

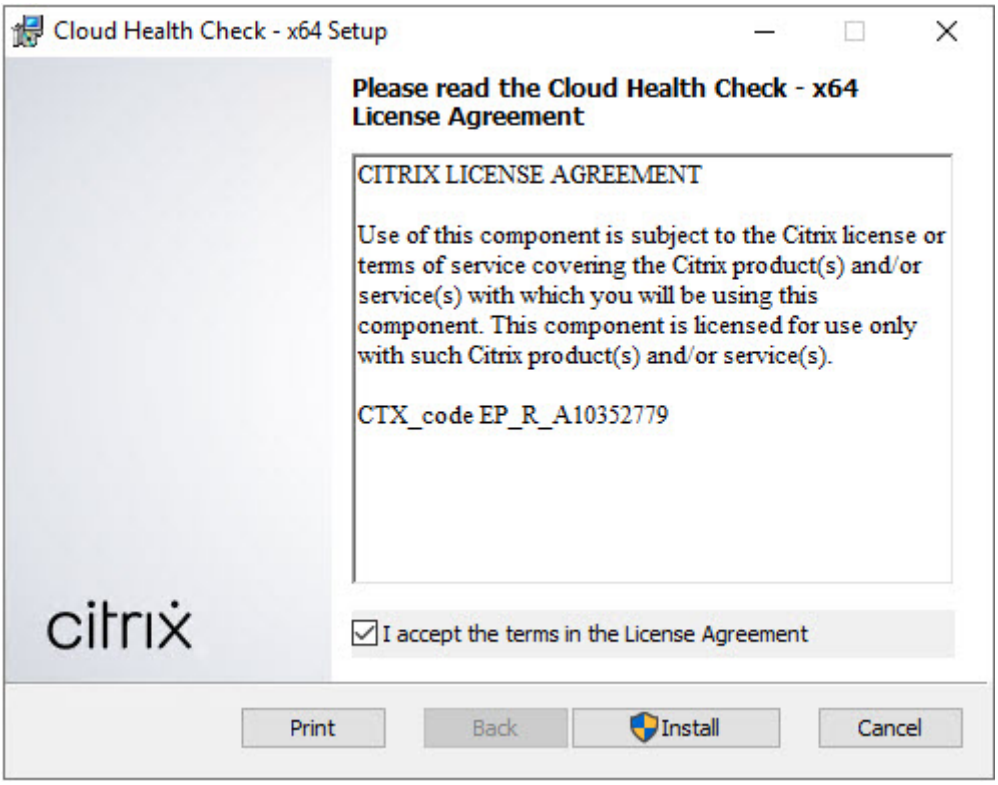
## Instalação

Para preparar seu ambiente para a instalação do Cloud Health Check, você deve ter uma máquina Windows ingressada no domínio.

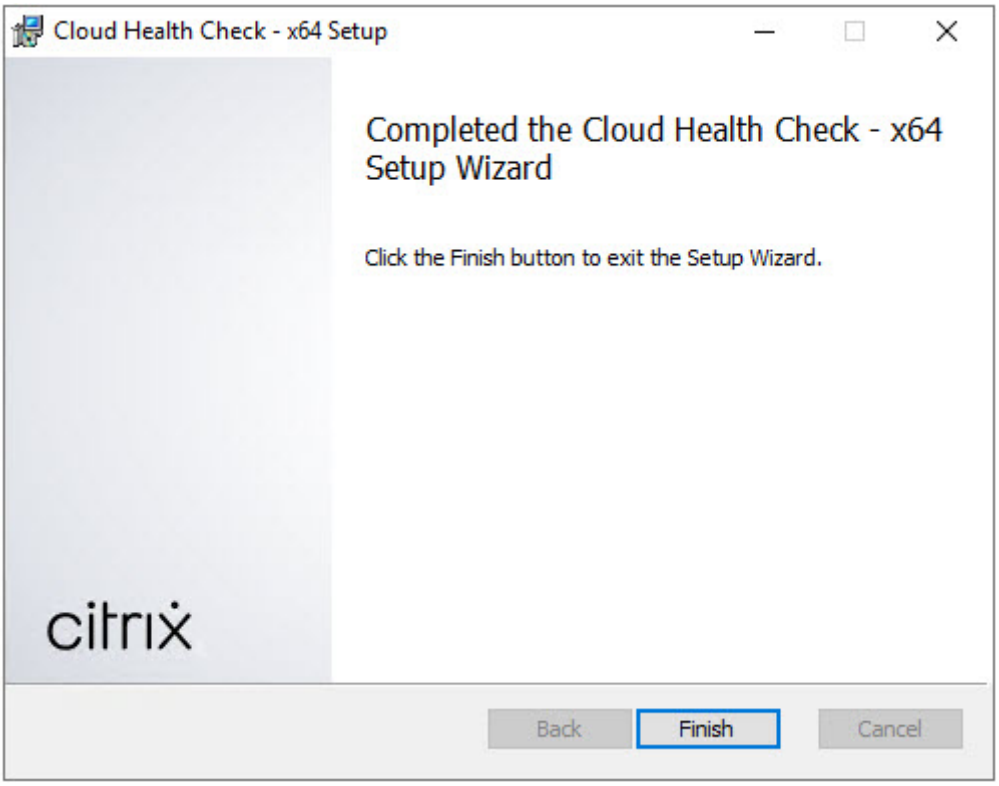
> **Nota:**
>
> Não é possível instalar ou executar o Cloud Health Check no Cloud Connector.

1. Na máquina ingressada no domínio, baixe o instalador do Cloud Health Check.
2. Clique duas vezes no arquivo CloudHealthCheckInstaller_x64.msi.
3. Clique na caixa de seleção para aceitar os termos.
4. Clique em Install.




5. Após a conclusão da instalação, clique em **Finish**.




### Permissões e requisitos

Permissões:

- Para executar verificações de integridade:
  - Você deve ser membro do grupo de usuários do domínio.
  - Você deve ser um administrador com direitos completos ou ter uma função personalizada com permissões somente leitura e executar **Run Environment Tests** para o site.
  - Defina a política de execução de script como pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Observação:** outras permissões de execução de scripts também podem funcionar.
- Use **Run as administrator** ao iniciar o Cloud Health Check.

Para cada máquina VDA ou StoreFront em que você executa verificações de integridade:

- O sistema operacional deve ser de 64 bits.
- 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 Infraestrutura de Gerenciamento do Windows (WMI) deve estar habilitado na máquina.

## Sobre verificações de integridade

Os dados da verificação de integridade são armazenados em pastas em `C:\ProgramData\Citrix\TelemetryService\`.

### Verificações de integridade VDA

Para registro no VDA, o Cloud Health Check verifica:

- Instalação do software VDA
- Associação ao domínio da máquina VDA
- Disponibilidade da porta de comunicação VDA
- Status do serviço VDA
- Configuração de firewall do Windows
- Comunicação com o Controller
- Sincronização de tempo com o Controller
- Status de registro VDA

Para a inicialização de sessões em VDAs, o Cloud Health Check verifica:

- Disponibilidade da porta de comunicação de início de sessão
- Status dos serviços de início de sessão
- Iniciar sessão Configuração de firewall do Windows
- Licenças de acesso para cliente do VDA Remote Desktop Services
- Caminho de início do aplicativo VDA
- Configurações de registro de início de sessão
- Status do Citrix Universal Injection Driver (CTXUVI)

Para Profile Management em VDAs, o Cloud Health Check verifica:

- Detecção do Hypervisor
- Detecção do Provisioning
- Citrix Virtual Apps and Desktops
- Configuração pessoal do vDisk
- Armazenamento do usuário
- Detecção de status do Profile Management Service
- Teste de hooking de Winlogon.exe

Para executar verificações no Profile Management, você deve instalar e ativar o Profile Management no VDA. Para obter mais informações sobre verificações de configuração do Profile Management, consulte o artigo do Knowledge Center CTX132805.

#### Verificações de integridade do StoreFront

As verificações do StoreFront verificam se:

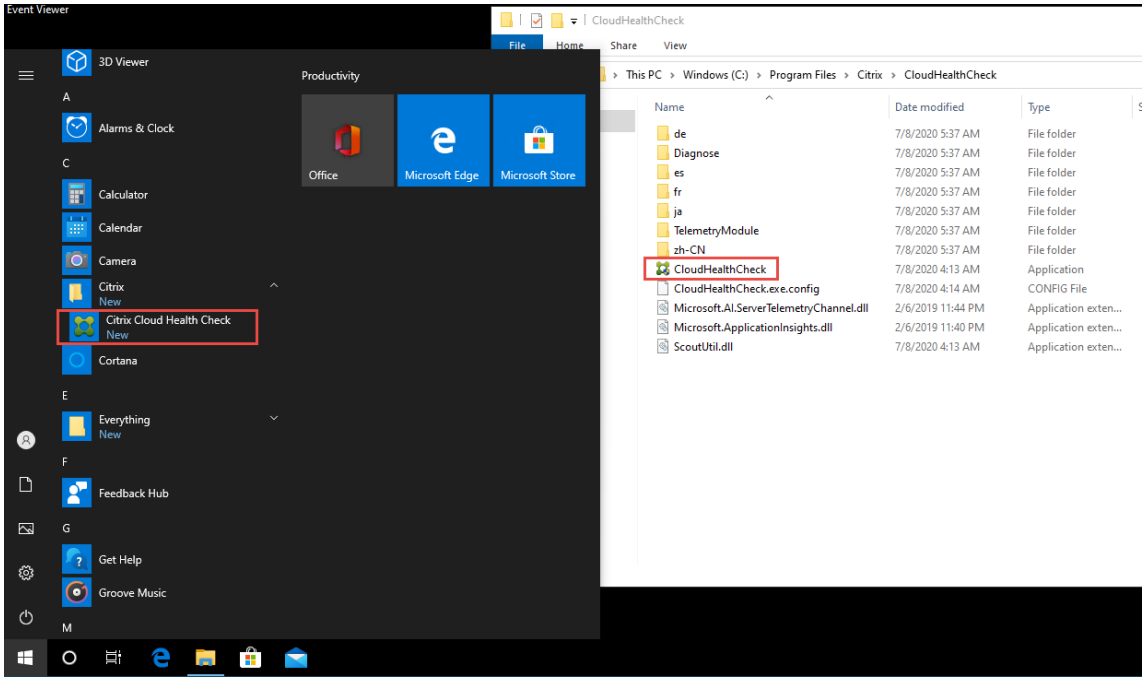
- O serviço Citrix Default Domain está em execução
- O serviço Citrix Credential Wallet está em execução
- A conexão do servidor StoreFront com o Active Directory é pela porta 88
- A conexão do servidor StoreFront com o Active Directory é pela porta 389
- A conexão do servidor StoreFront com o Active Directory é pela porta 464
- O URL de base tem um FQDN válido
- O endereço IP correto da URL de base pode ser obtido
- O pool de aplicativos do IIS está usando .NET 4.0
- O certificado está vinculado à porta SSL para o URL do host
- A cadeia de certificados está completa
- Os certificados expiraram
- Um certificado expira dentro de 30 dias

### Executar o Cloud Health Check

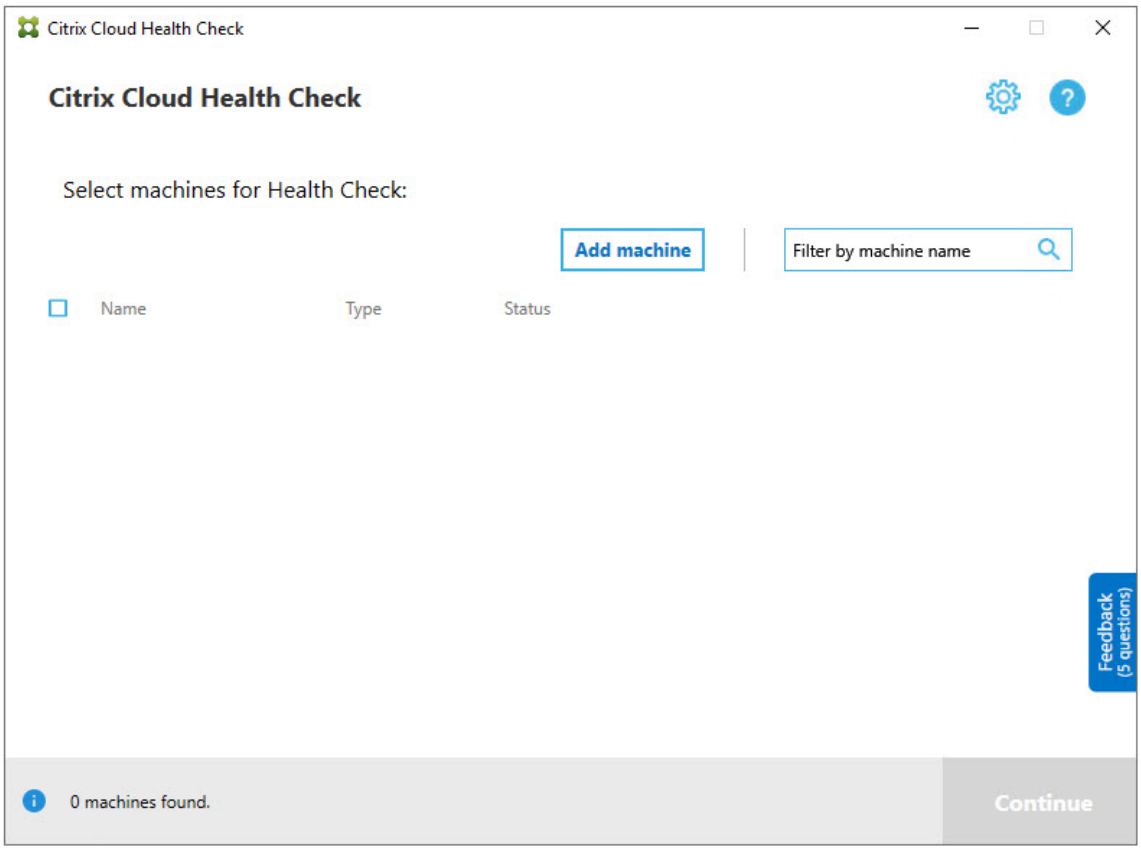
Para executar o Citrix Cloud Health Check:

1. Selecione **Citrix > Citrix Cloud Health Check** no menu Iniciar da máquina ou execute `CloudHealthCheck.exe` em `C:\Program Files\Citrix\CloudHealthCheck`.



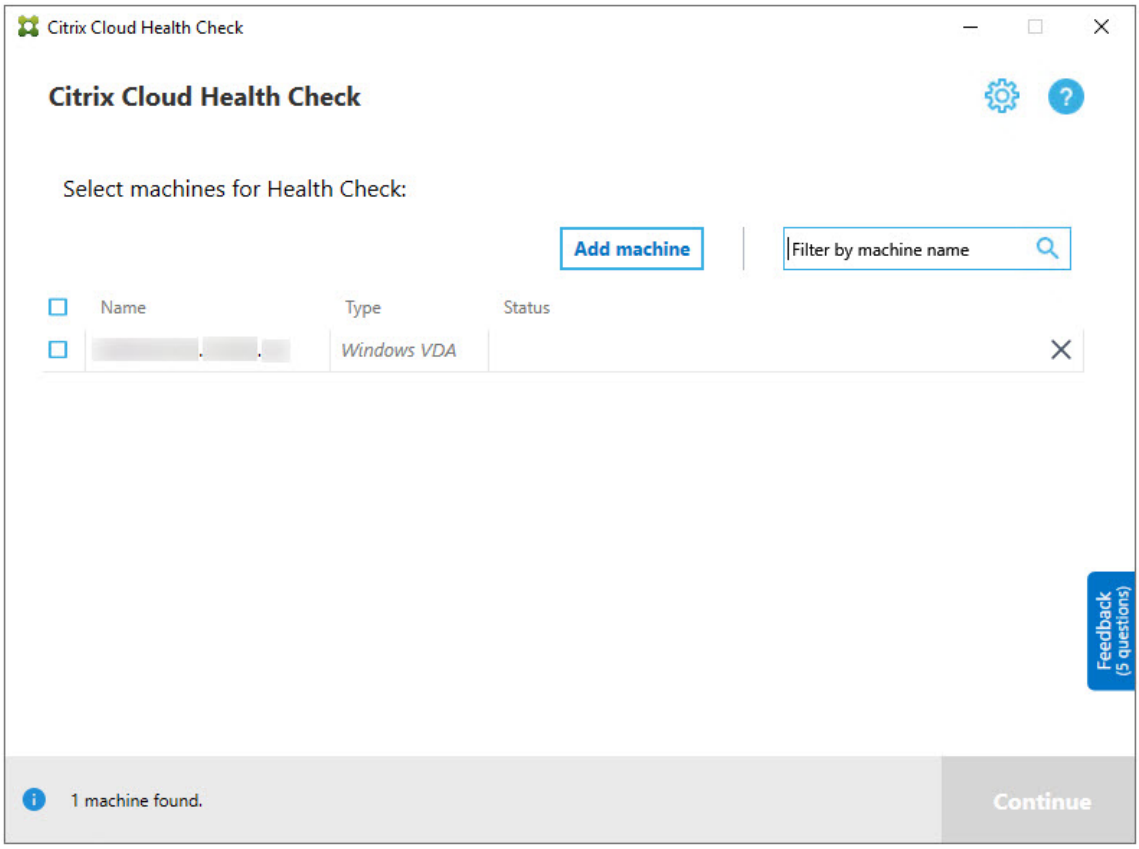

2. Na tela principal do Cloud Health Check screen, clique em **Add machine**.




3. Digite o FQDN da máquina que você deseja adicionar. **Nota:** Embora a inserção de um alias DNS em vez de um FQDN possa parecer válida, as verificações de integridade podem falhar.

4. Clique em **Continue**.
5. Repita para adicionar outras máquinas, conforme necessário.




6. Para remover uma máquina adicionada manualmente, clique no **X** na extremidade direita 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 estão listadas na parte superior da lista.

### Importar máquinas VDA

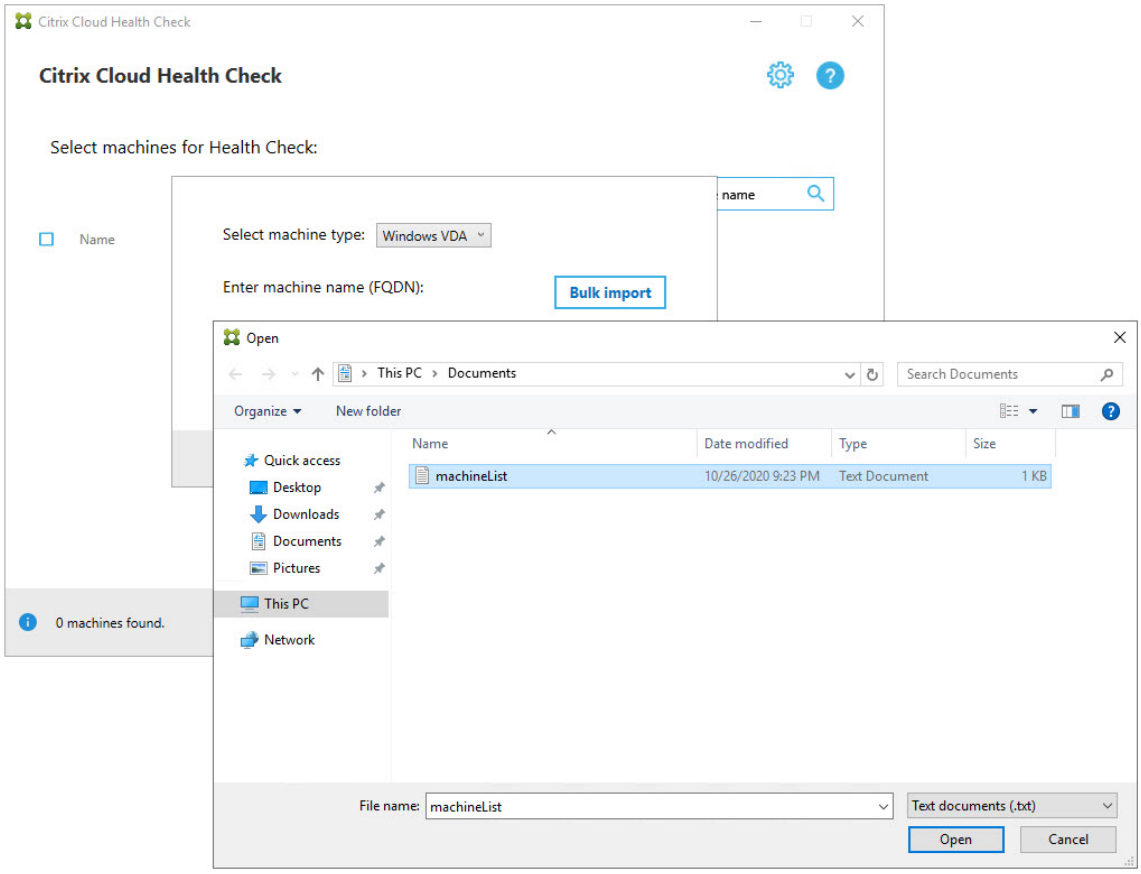
Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

1. No Connector, gere o arquivo de lista de máquinas com o seguinte comando do PowerShell. No Connector, você deve inserir 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 em que você deseja executar o Cloud Health Check.

2. Na página Cloud Health Check, clique em **Add Machine**.
3. Selecione o tipo de máquina Windows VDA.
4. Clique em **Import VDA machines**.
5. Selecione o arquivo machineList.txt.
6. Clique em **Open**.



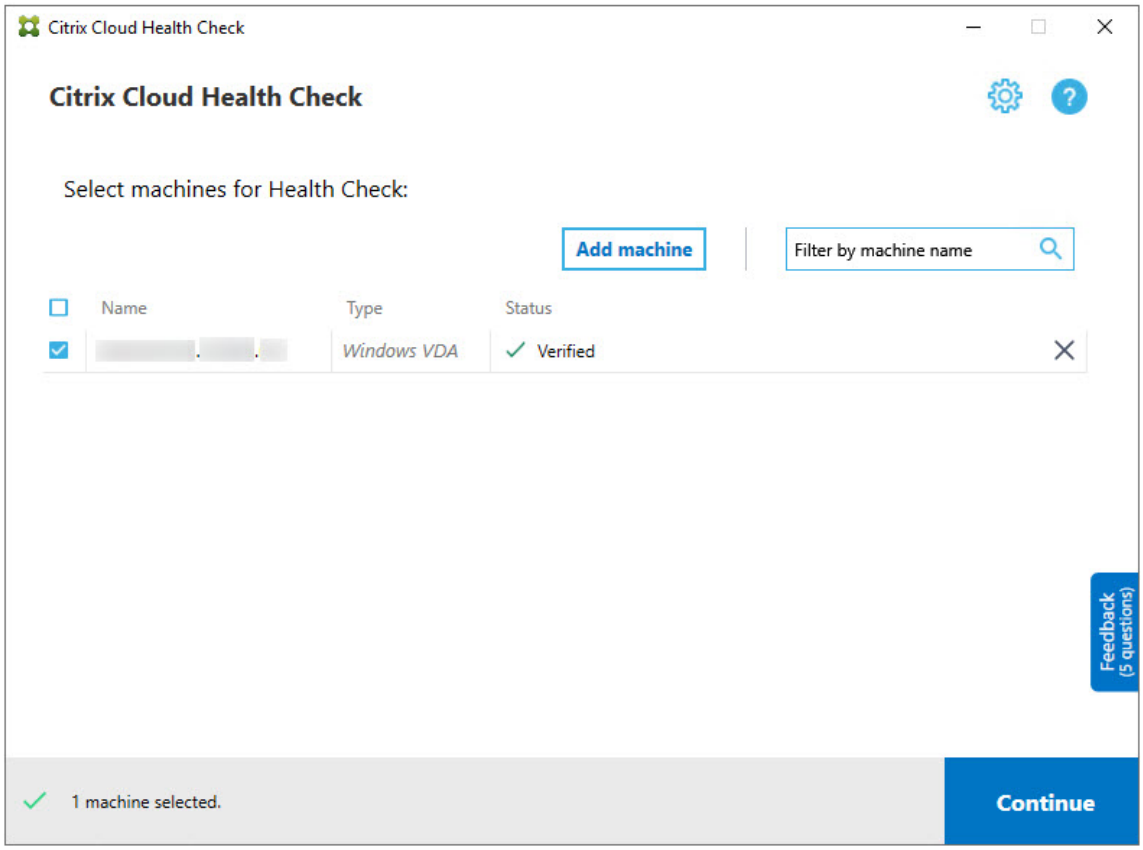
As máquinas VDA importadas estão listadas na página Cloud Health Check.

7. Marque a caixa de seleção ao lado de cada máquina em que você deseja executar verificações de integridade.

   O Cloud Health Check inicia automaticamente testes de verificação em cada máquina selecionada, certificando-se de que ele atende aos critérios listados nos testes de verificação. Se a verificação falhar, uma mensagem aparece na coluna **Status** e a caixa de seleção dessa máquina fica desmarcada. Em seguida, você pode:

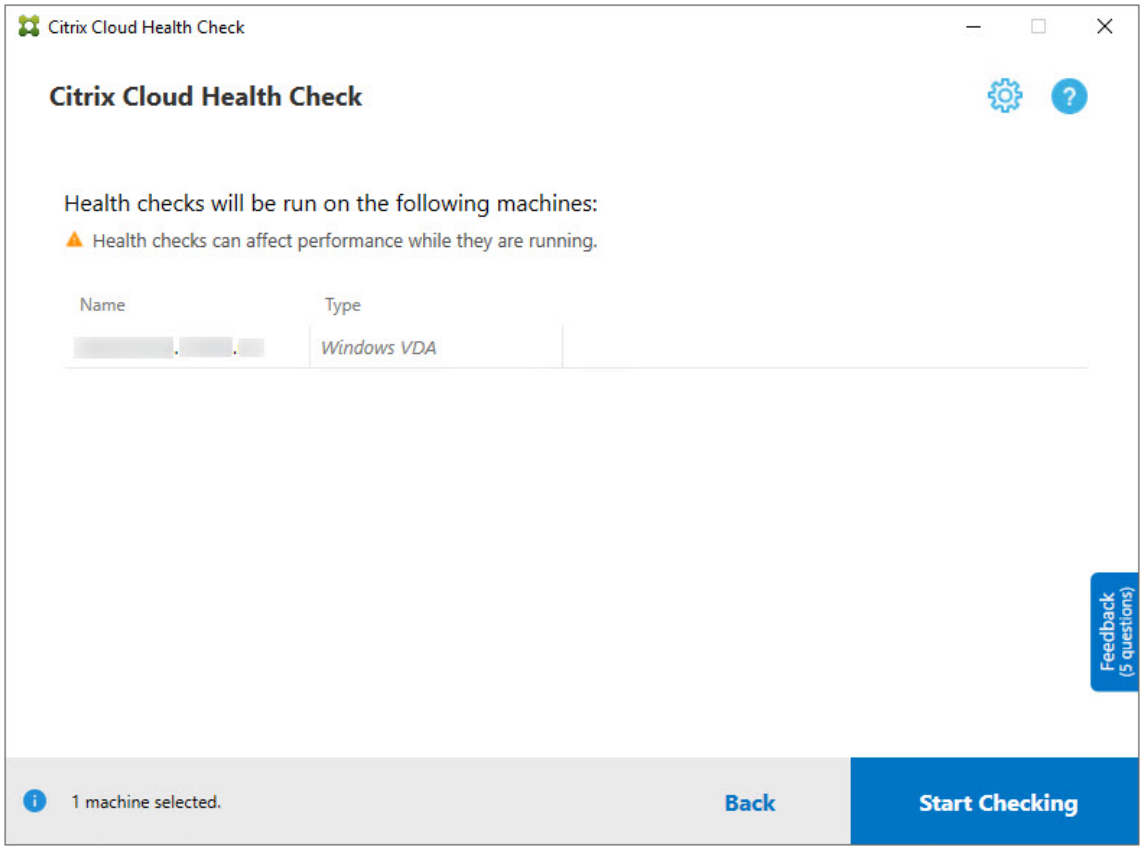
   - Resolver o problema e marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina deixando sua caixa de seleção desmarcada. As verificações de integridade não são executadas para essa máquina.

8. Quando os testes de verificação forem concluídos, clique em **Continue**.



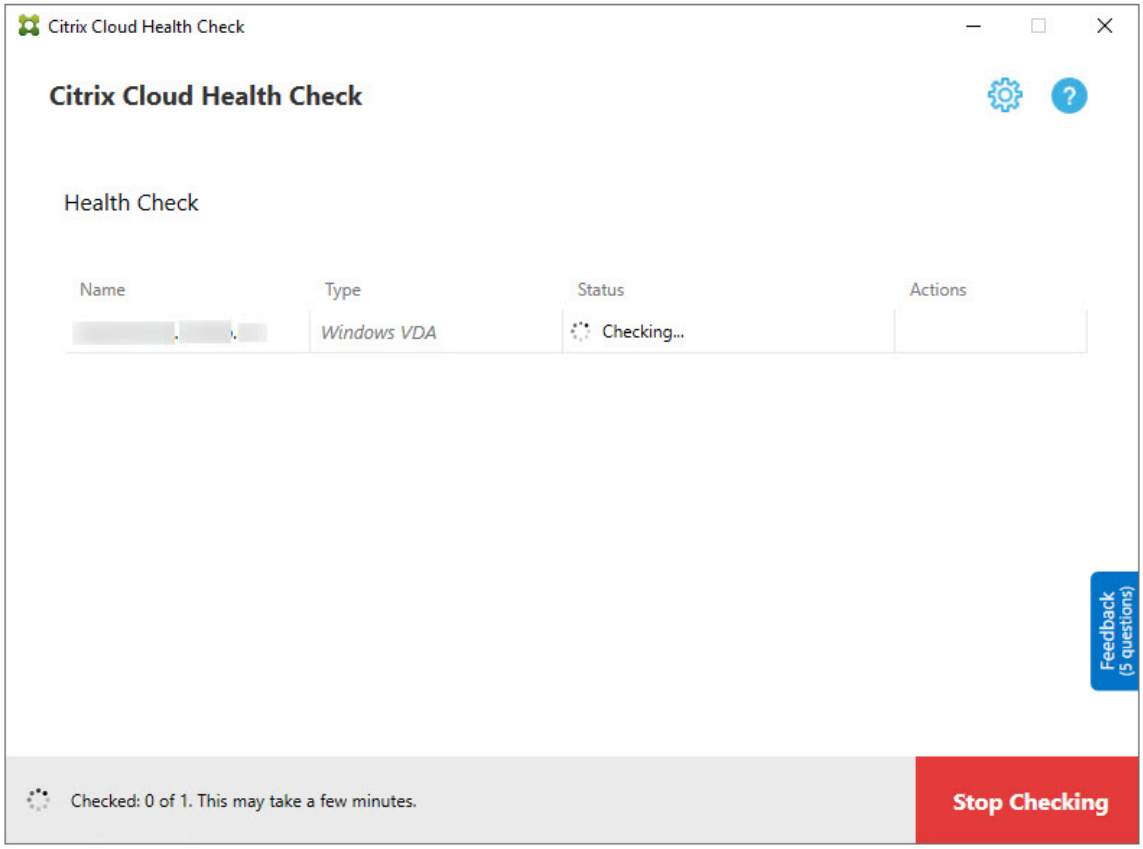
9. Execute as verificações de integridade nas máquinas selecionadas. O resumo lista as máquinas em que os testes são executados (as máquinas que você selecionou que passaram nos testes de verificação).

10. Clique em **Start Checking**.

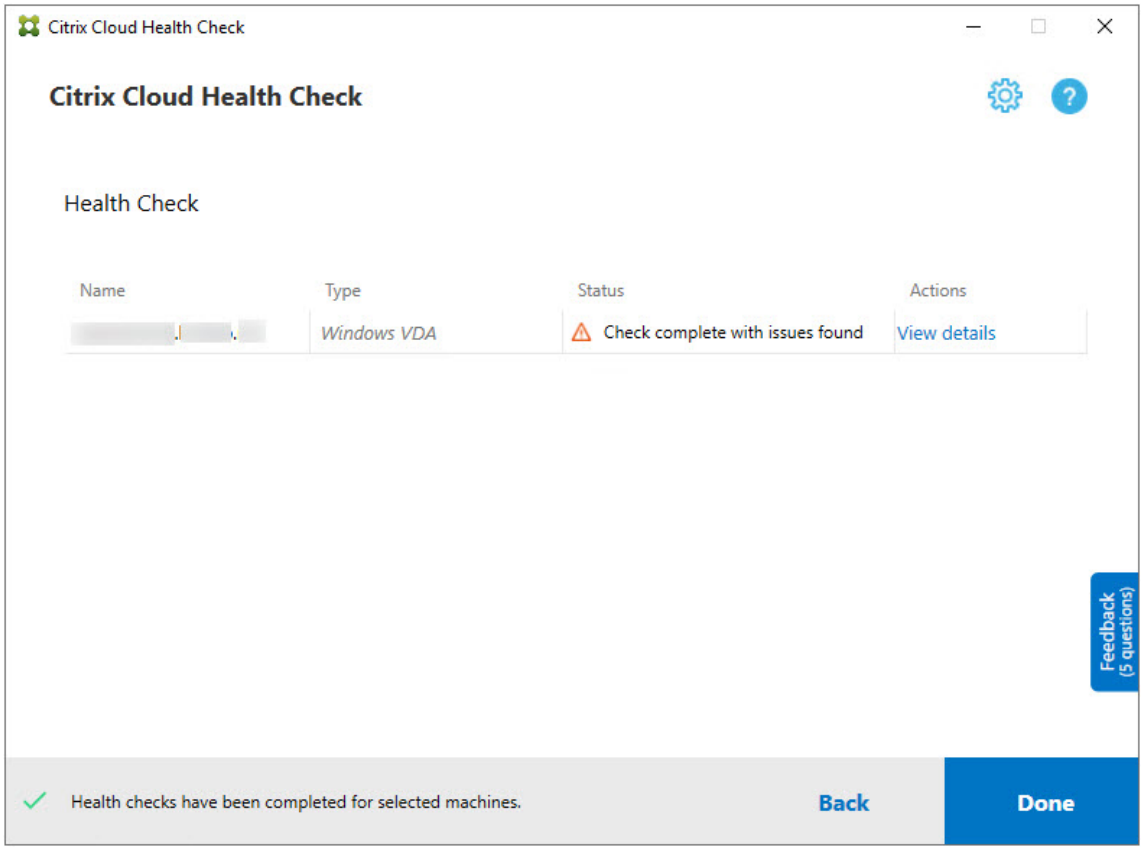


Durante e após a verificação, a coluna **Status** indica o estado de verificação atual de uma máquina.

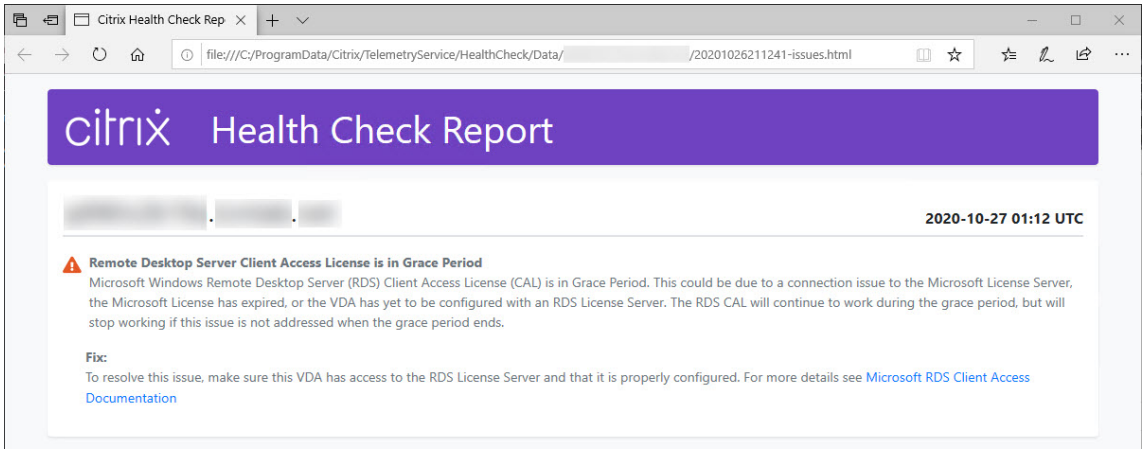
11. Para interromper todas as verificações em andamento, clique em **Stop Checking** no canto inferior direito da página. Você não pode cancelar a verificação de integridade de uma única máquina; você só pode cancelar a verificação para todas as máquinas selecionadas.



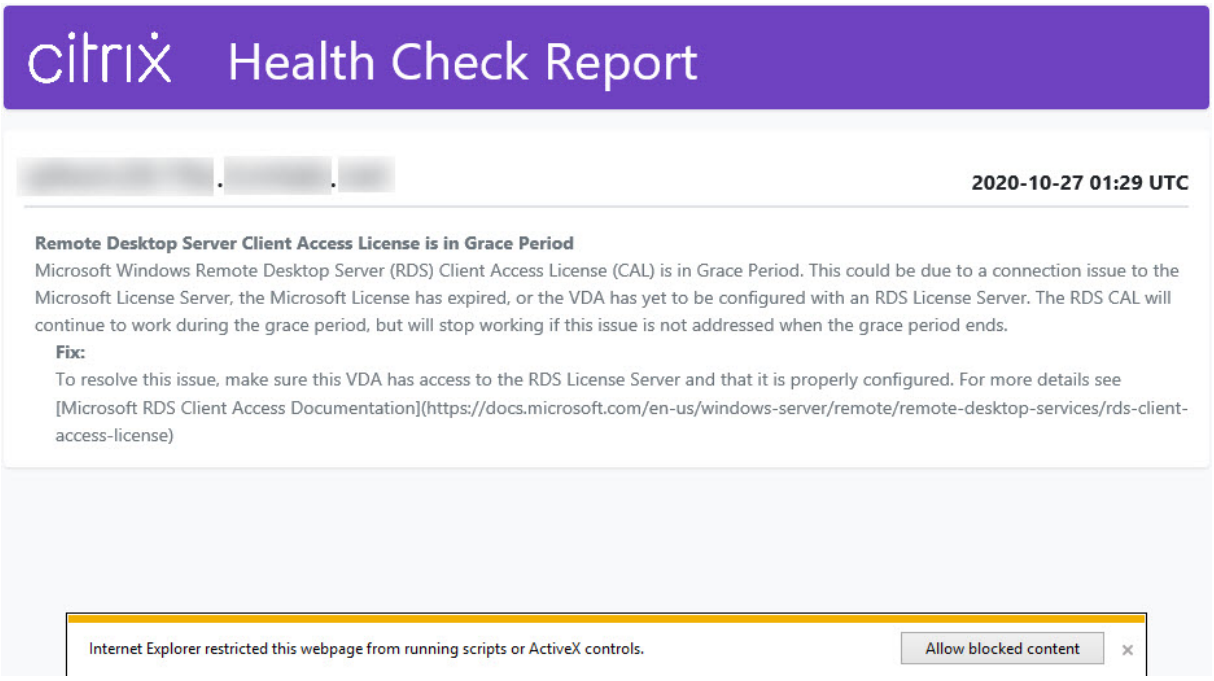
12. Quando as verificações forem concluídas para todas as máquinas selecionadas, o botão **Stop Checking** no canto inferior direito muda para **Done**.



- Se uma verificação falhar, você poderá clicar em **Retry** na coluna **Action**.
- Se uma verificação for concluída sem problemas encontrados, a coluna **Action** estará vazia.
- Se uma verificação encontrar problemas, clique em **View Details** para exibir os resultados.



Se você usar o Internet Explorer para exibir o relatório, deve clicar em **Permitir conteúdo bloqueado** para exibir o hiperlink.



Depois que a verificação for concluída para todas as máquinas selecionadas, clicar em **Back** fará você perder os resultados da verificação.

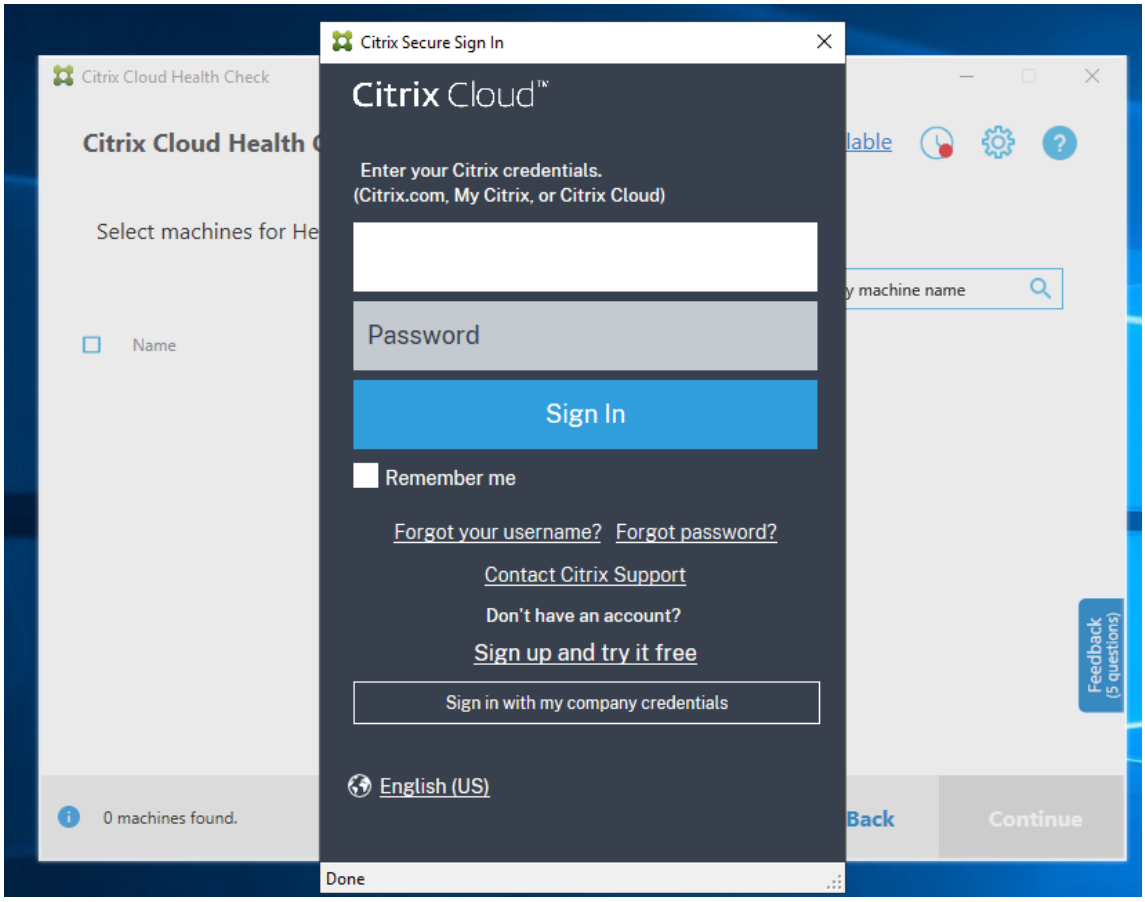
Quando as verificações forem concluídas, clique em **Done** para retornar à tela principal do Cloud Health Check.

Recuperar máquinas VDA

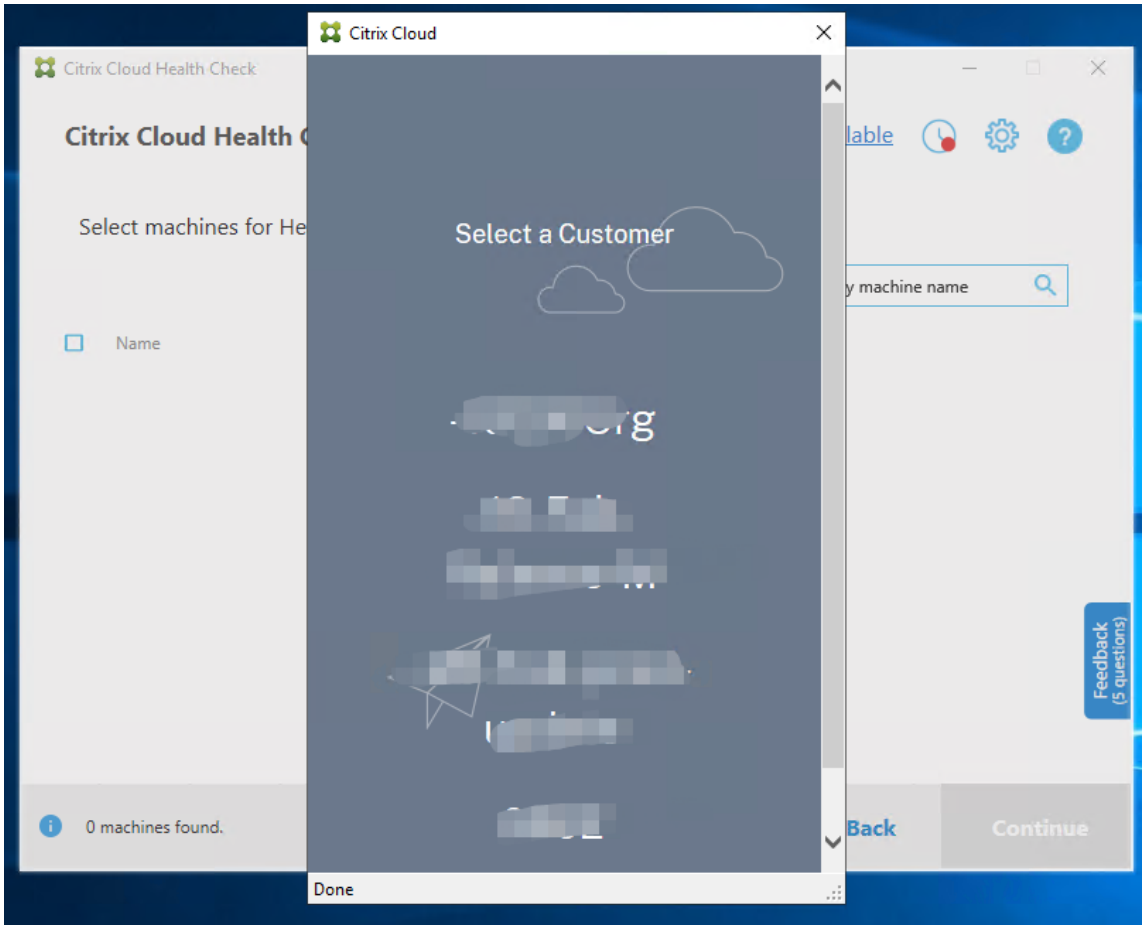
O Cloud Health Check pode detectar e recuperar automaticamente VDAs de suas implantações do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service).

Para recuperar seus VDAs:

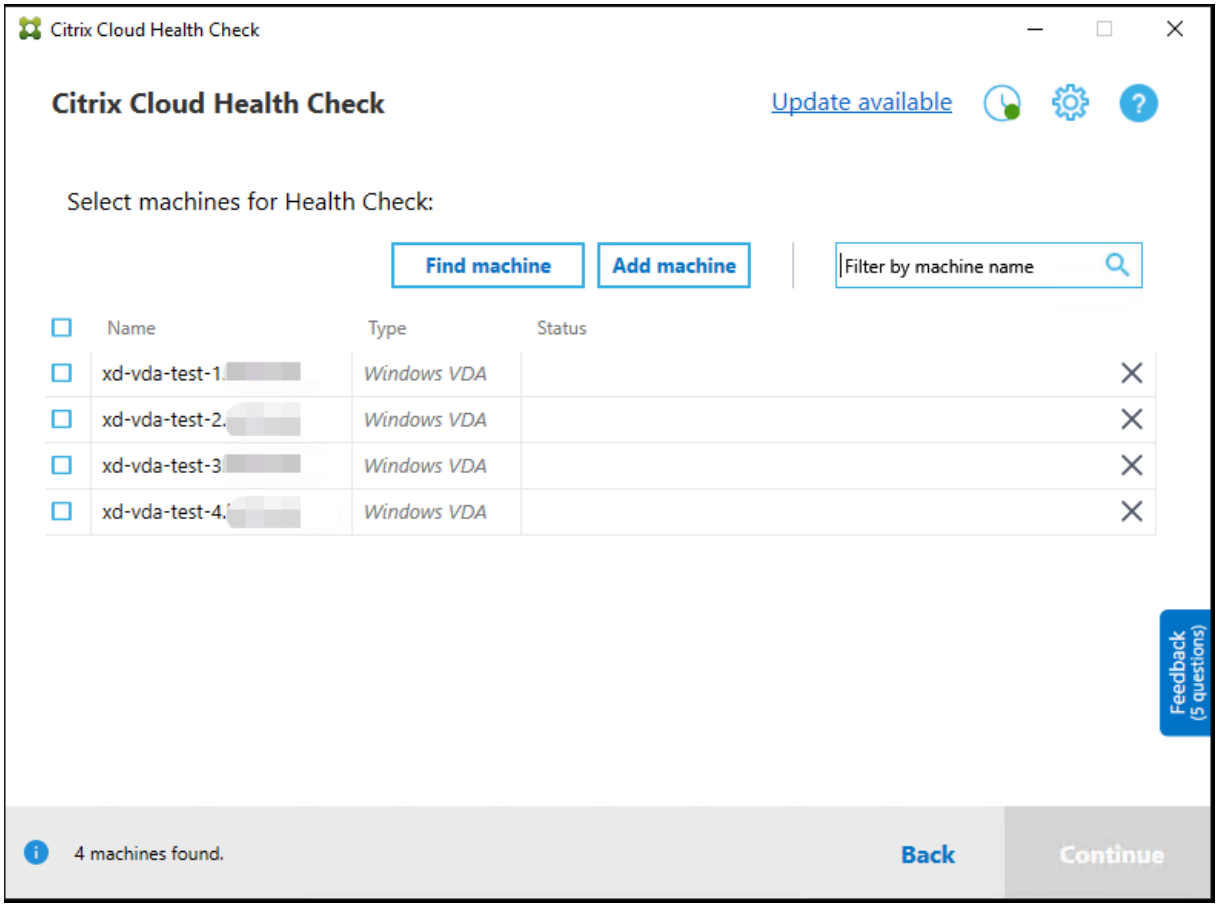
1. Prepare uma nova máquina que esteja ingressada na mesma floresta do domínio da máquina em que o Cloud Health Check é executado.
2. Abra o Cloud Health Check e clique em **Find machine** para entrar no Citrix Cloud.



3. Selecione o cliente com o site da nuvem que você deseja recuperar.

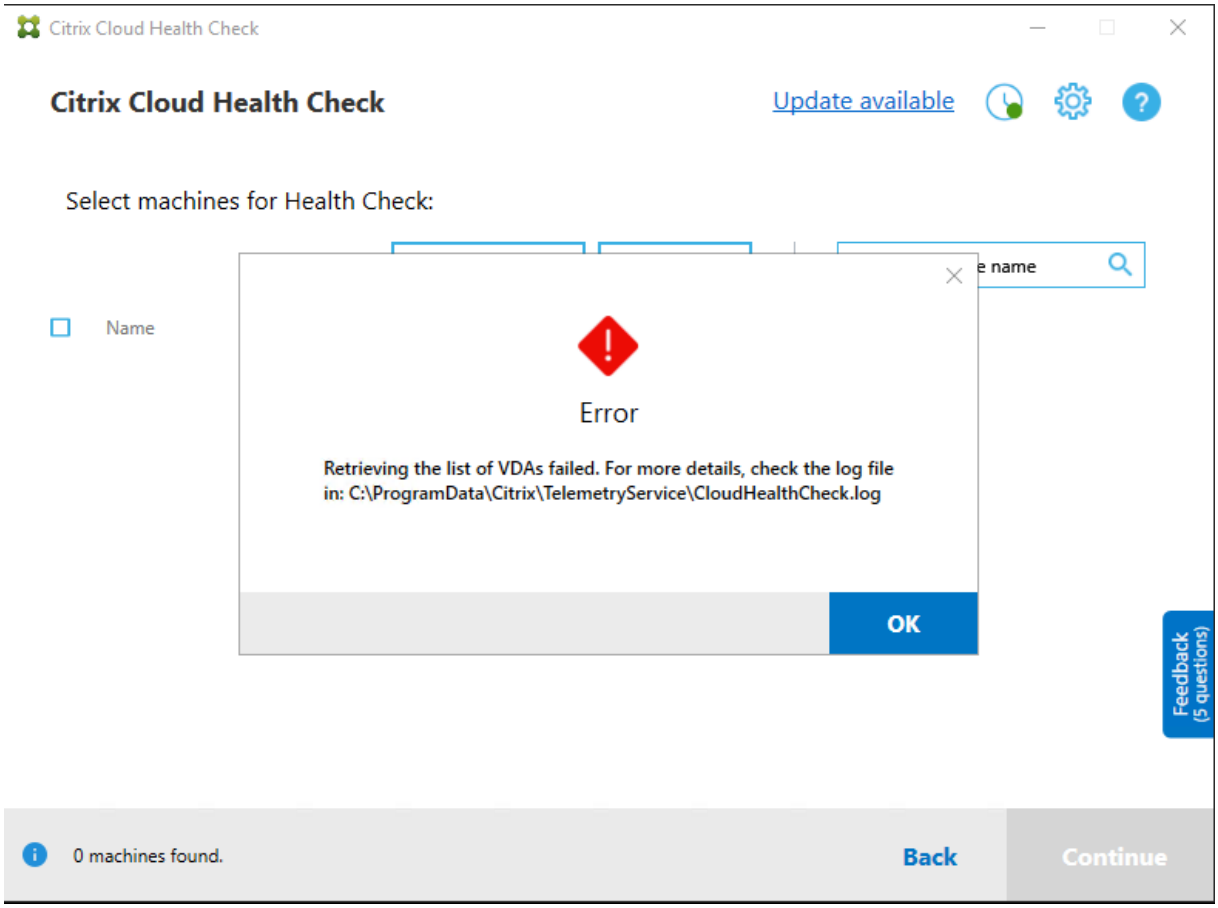


A lista VDA é exibida no Cloud Health Check. A lista também é salva em um arquivo local localizado em `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.



Sua lista de máquinas carrega o cache local quando você abre o Cloud Health Check novamente. Se você fez alguma atualização em sua implantação, clique em **Find machine** para atualizar a lista de máquinas.

> **Nota:**
>
> - O Cloud Health Check encontra máquinas somente na mesma floresta do domínio da máquina que executa o Cloud Health Check.
> - As sessões do Citrix Cloud expiram em uma hora. Após uma hora, você deve clicar em **Find machine** novamente para obter a lista VDA mais recente.
> - Uma mensagem de erro aparece se a recuperação da lista VDA 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

Executar o Cloud Health Check na linha de comando

O Cloud Health Check pode ser executado na linha de comando para ajudar os clientes a realizarem 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, somente uma máquina pode ser verificada por vez. Somente uma instância do `CloudHealthCheck.exe` pode ser executada ao mesmo

> tempo na máquina de destino. Se você quiser verificar várias máquinas, as máquinas devem ser verificadas uma a uma, agrupando os cmdlets em um loop nos scripts cmdlet/PowerShell. Instâncias de IU abertas do Cloud Health Check também devem ser fechadas.

Cmdlets

Os cmdlets de linha de comando suportados são:

- `MachineFQDN` - Esse cmdlet é **obrigatório**. Esse é o nome de domínio totalmente qualificado da máquina de destino.
- `MachineType` - Esse cmdlet é opcional. O valor do cmdlet pode ser o VDA do Windows (valor padrão) ou o StoreFront.
- `ReportName` - Esse cmdlet é opcional. O valor do cmdlet deve ser um nome de arquivo válido no Windows. O valor padrão é `HealthCheckReport`.
- `SkipAdminCheck` - Esse cmdlet é opcional. Pode ser adicionado para ignorar as verificações que exigem permissões de administrador.
- `UpdateScripts` - Esse cmdlet é opcional. Pode ser adicionado para atualizar os scripts de verificação do servidor CDN.
- `DisableCeip` - Esse cmdlet é opcional se o CEIP estiver habilitado na interface do usuário; adicione-o para desabilitar o CEIP.
- `Help` - Mostrar 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 de parâmetros não diferenciam maiúsculas de minúsculas

Por padrão, a saída do console não é mostrada na janela do console da linha de comando. Você pode exibir manualmente a saída anexando `|more` ao cmdlet.

Exemplo: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

O padrão da linha de comando precisa de permissões de administrador para ser executado. Adicione o parâmetro `-SkipAdminCheck` para substituir 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 do cmdlet.

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 cmdlet `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 em que o Cloud Health Check está instalado. Os relatórios de verificação de integridade estão localizados em `HealthCheckDataFolder` em `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Os relatórios só são criados quando existem problemas na máquina de destino.

> **Nota:**
>
> Os arquivos de relatório são substituídos se o nome do relatório especificado existir.

Alertas e informações básicas são armazenados no relatório .json.

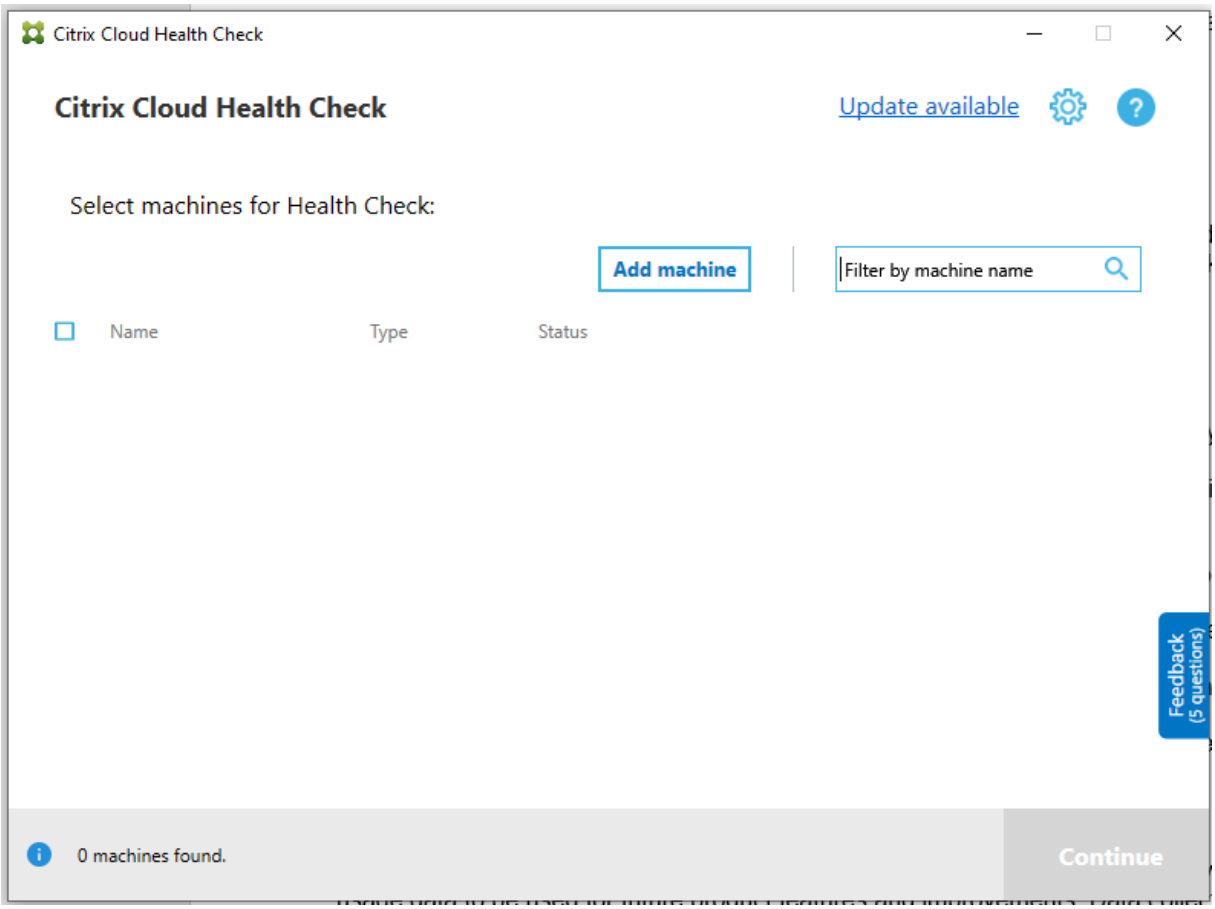

```
JSON
  version : 1
  id : 9547e4ae-022c-4d36-b3a6-77ee61aa72cd
  siteId : 00000000-0000-0000-0000-000000000000
  generatedTime : 2020-09-08T06:53:25Z
  machineReports
    0
      startTime : 2020-09-08T02:53:13.000Z
      endTime : 2020-09-08T02:53:23.000Z
      fqdn : machine.domain.local
      machineType : VDA
      alerts
        0
          issueKey : citrix.vda.network.registration-port-unreachable
          issueUuid : a3547960-fdad-4594-96bd-ebf9c0af7f4a
          fixRecommendation : To resolve this issue, see [CTX227516](https://support.citrix.com/article/CTX227516)
          severity : error
          issueName : Invalid Windows Firewall configuration
          issueDescription : 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)<br>
          tags : null
          checkNames
            0 : VDA Health Check
          HtmlFix : Fix:
        1
        2
        3
        4
      HtmlReportName : Health Check Report
```


Os códigos de relatório são:

- **issueKey**: uma descrição em texto simples do problema.
- **issueUuid**: uma cadeia de caracteres de identificação exclusiva do problema.
- **fixRecommendation**: a recomendação para correção do problema.
- **severity**: indica se o problema deve ser corrigido. Um erro pode indicar que o componente (VDA ou StoreFront) não funcionou corretamente; um aviso indica que o componente funciona, mas pode ter alguns possíveis problemas.
- **issueName**: o título do problema.
- **issueDescription**: uma descrição detalhada do problema.

Atualizar o Cloud Health Check

Se houver uma nova versão do Cloud Health Check disponível, um link Update available será exibido no canto superior direito da janela do Cloud Health Check. Clique no link para acessar o Citrix Downloads e obter a nova versão.

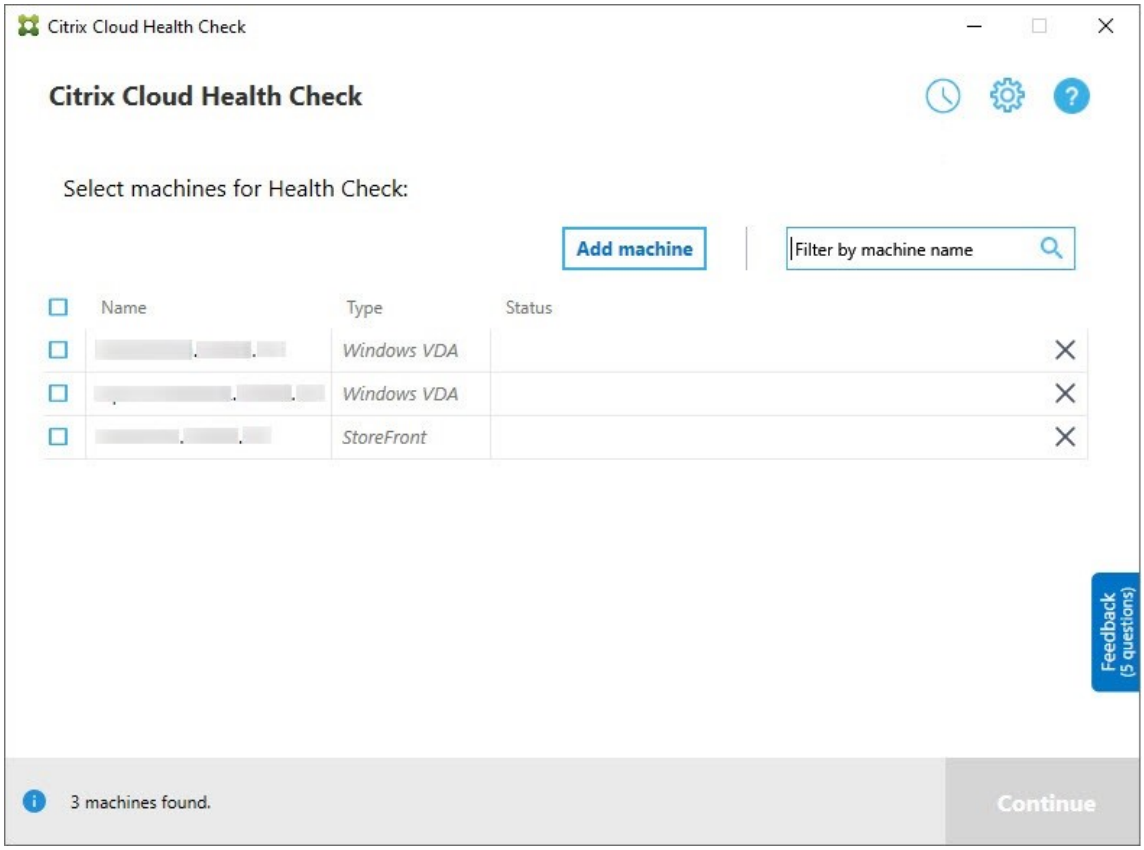


Agendador do Cloud Health Check

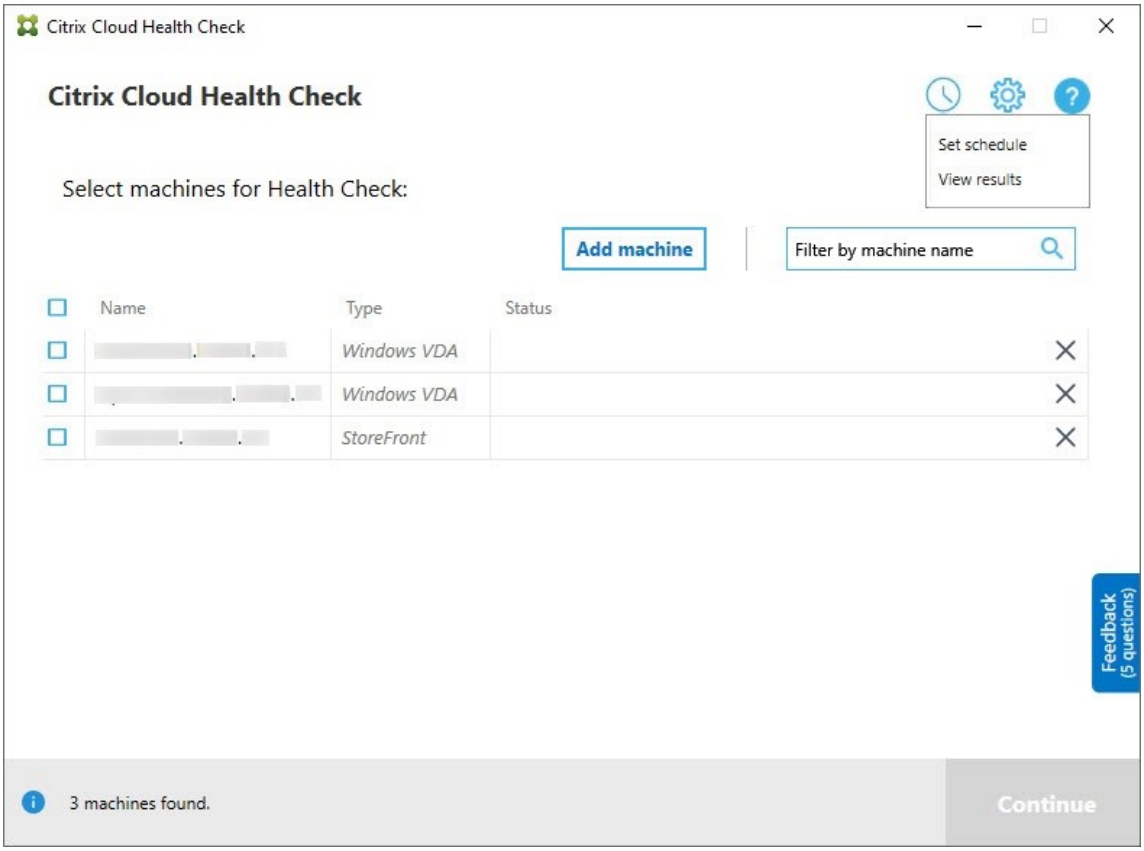
Use o agendador do Cloud Health Check para realizar verificações periódicas de integridade.

Configurar o agendamento

1. Clique em **Add machine** na janela principal do Cloud Health Check para adicionar máquinas nas quais deseja executar verificações periódicas.



2. Clique no ícone de relógio e, em seguida, clique em **Set schedule**.

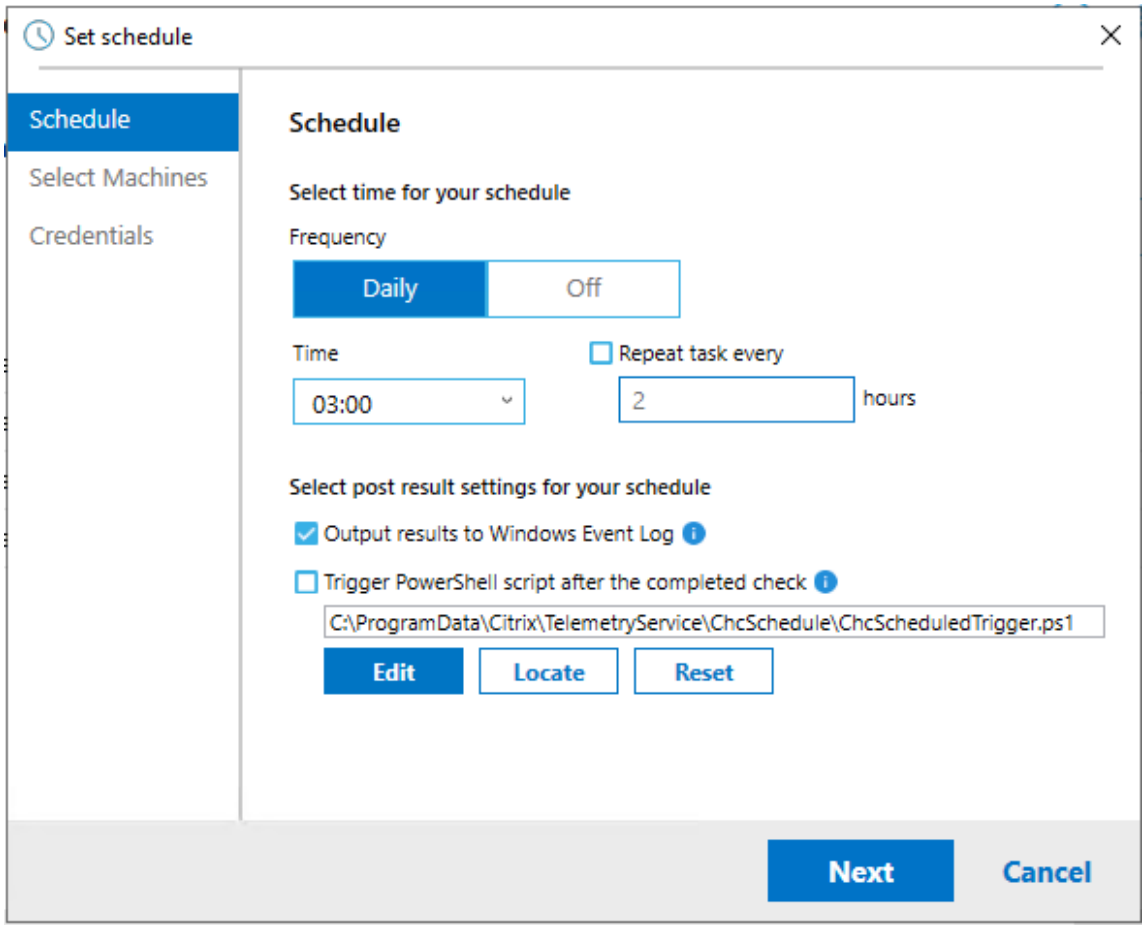


3. Selecione um horário para sua programação e clique em **Next**. A tarefa pode ser definida para ser repetida marcando a caixa de seleção **Repeat task every**.
4. Escolha a saída dos resultados para o Log de Eventos do Windows. A tarefa pode ser configurada para gravar os resultados no Log de Eventos do Windows.
5. Escolha disparar um script do PowerShell personalizado após a conclusão da verificação agendada e clique em **Next**.
   - Clique em **Edit** para editar o conteúdo do script no Windows PowerShell ISE, se necessário.
   - Clique em **Locate** para abrir o local do arquivo e usar um editor diferente para abrir o arquivo e editar o script.
   - Clique em **Reset** para redefinir o script para a configuração original.

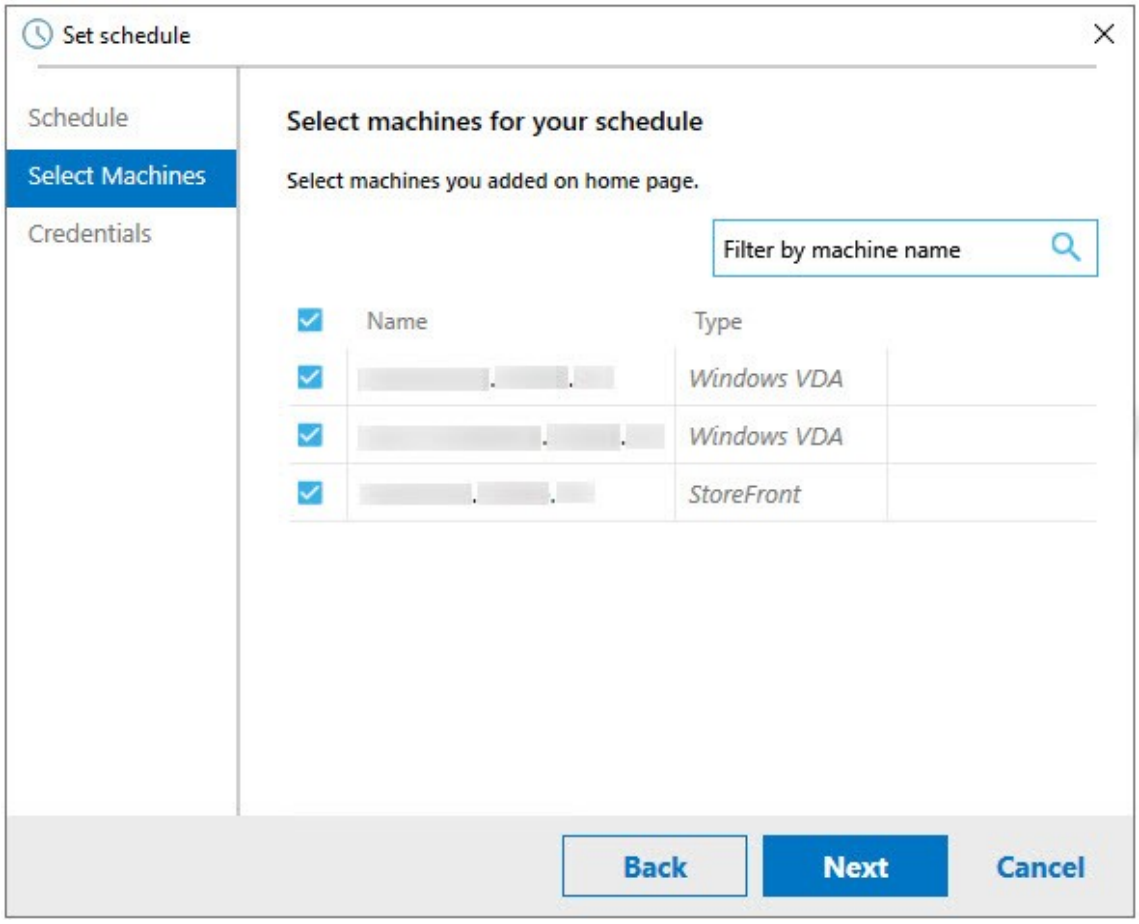
     > **Nota:**
     >
     > – Você não pode alterar o nome do script e o caminho do script.
     > – Você pode implementar ações personalizadas usando o script ChcShceduledTrigger.ps1, como enviar um e-mail depois que o relatório de verificação agendada estiver pronto. Adicione o seguinte código ao final 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 a tarefa agendada executa.

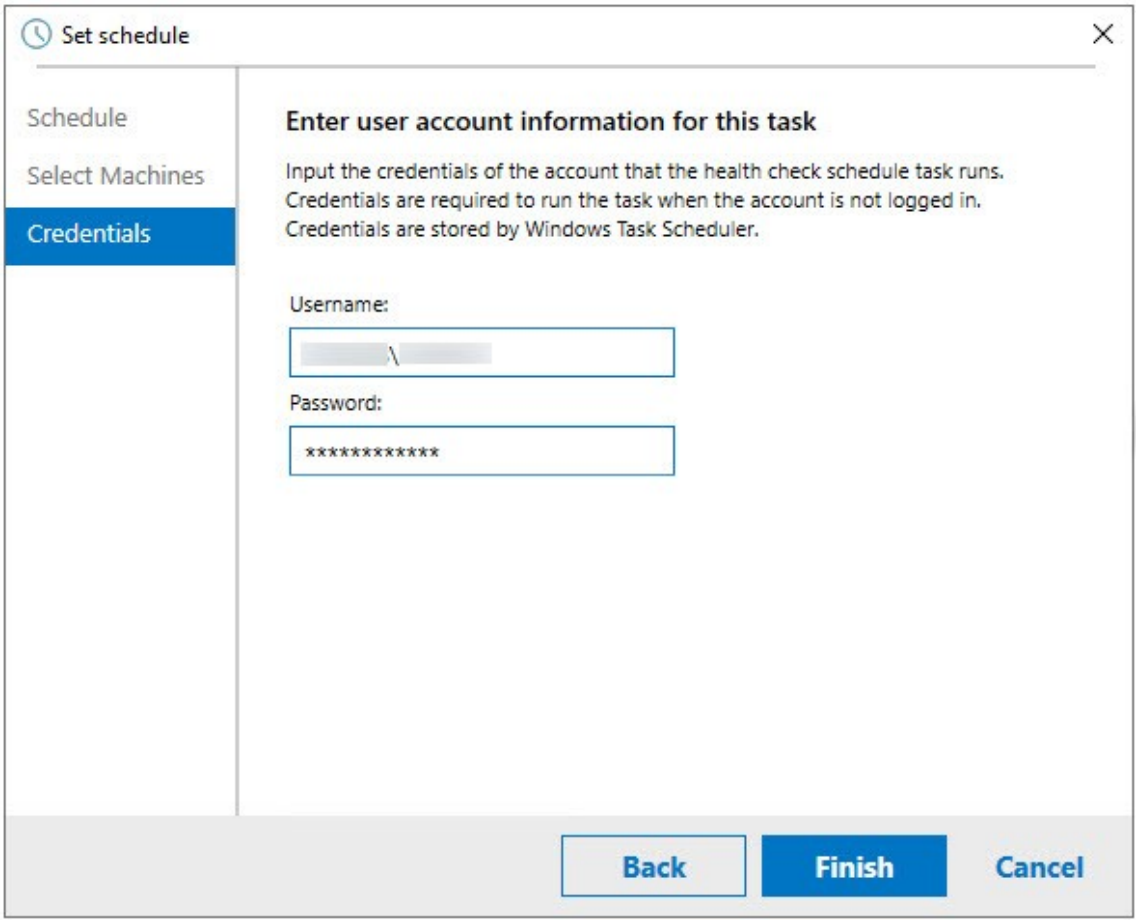
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



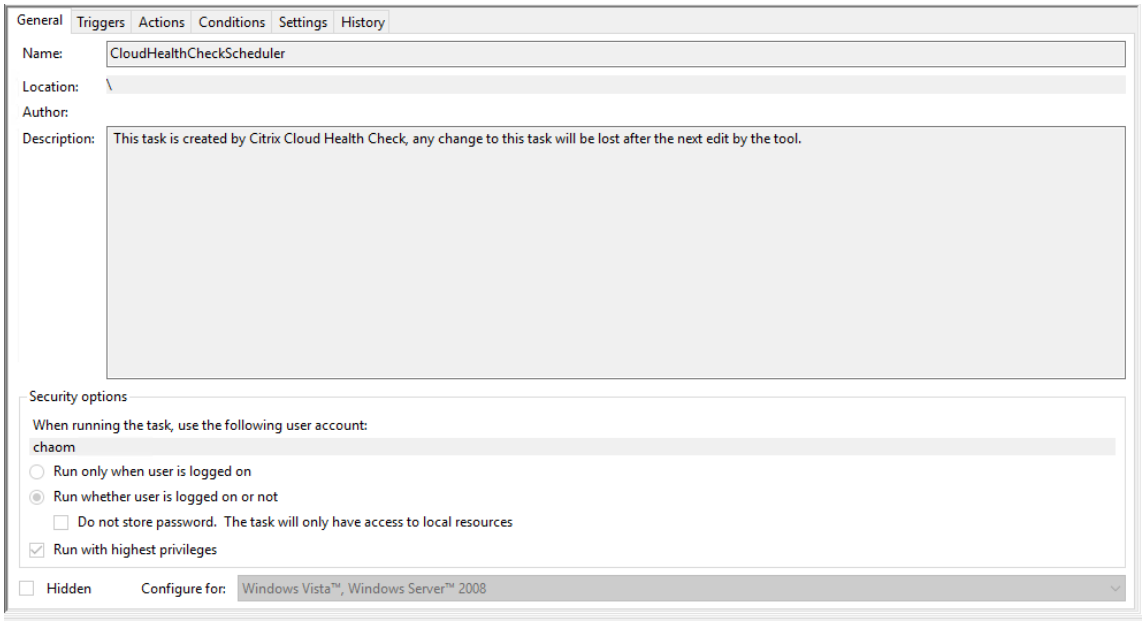
6. Selecione as máquinas para sua programação e clique em **Next**.



7. Insira as credenciais da conta em que a tarefa é executada e clique em **Finish**.

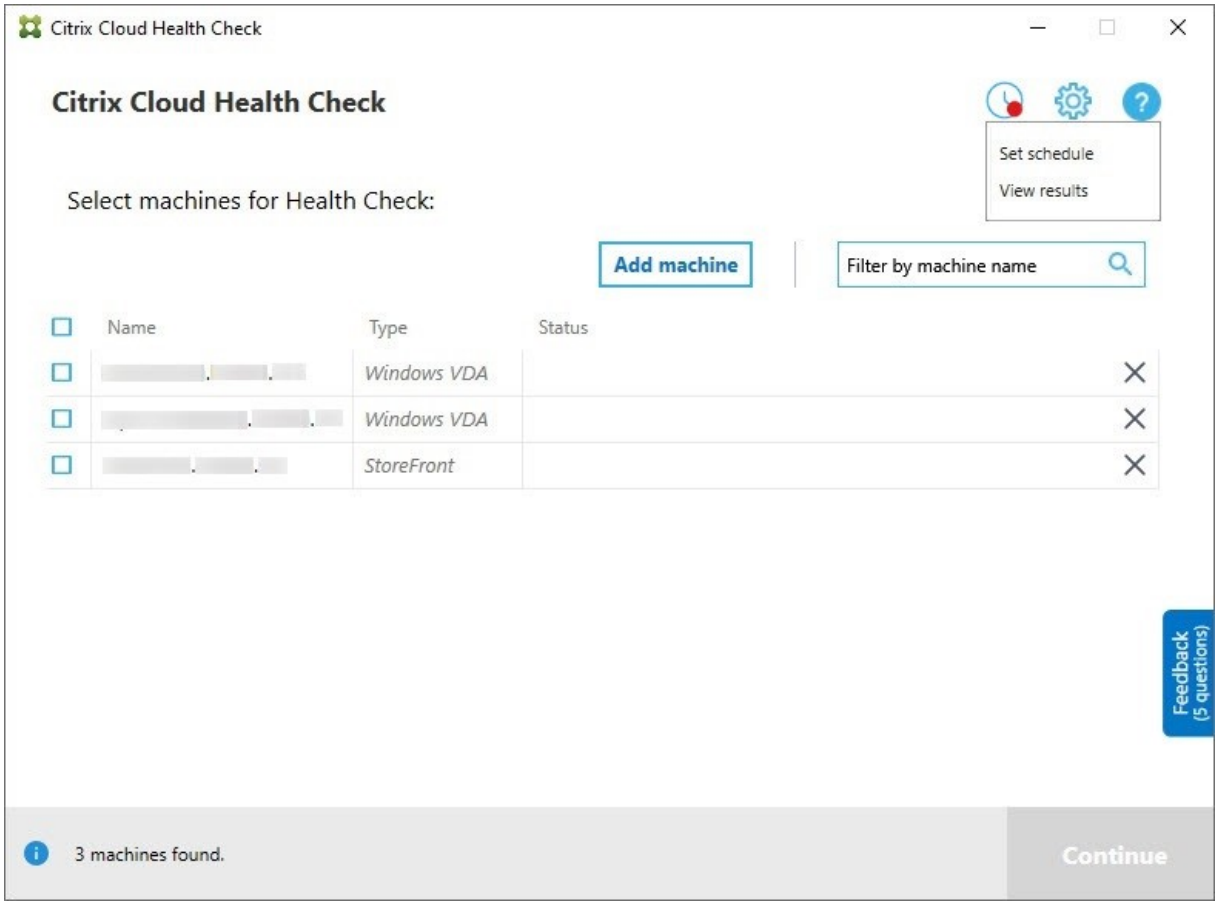


8. Uma tarefa CloudHealthCheckScheduler é criada no Agendador de Tarefas do Windows.

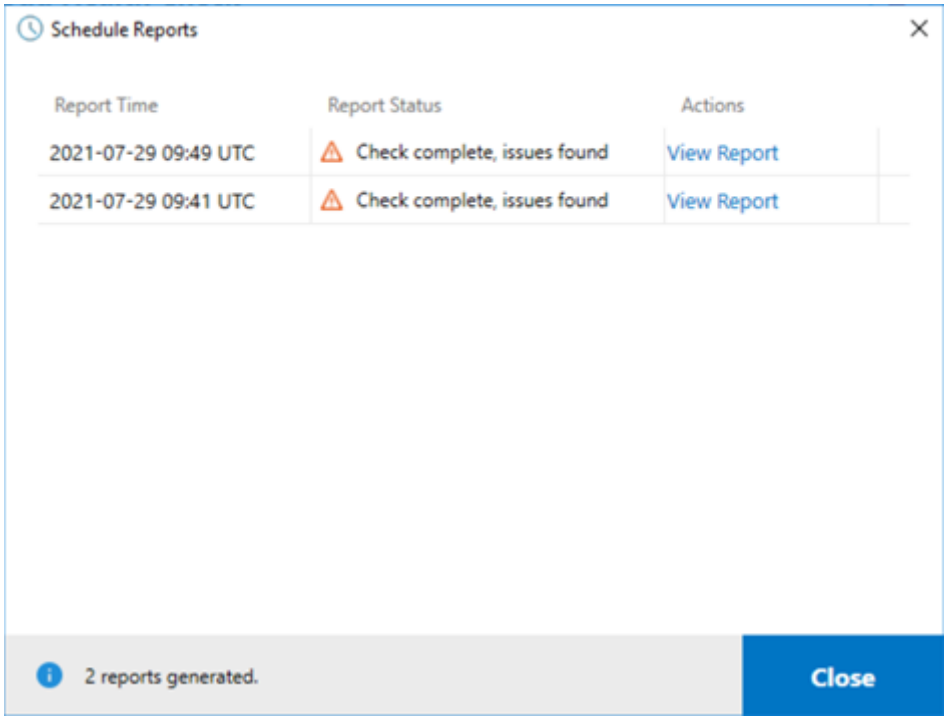


Ver os resultados da programação

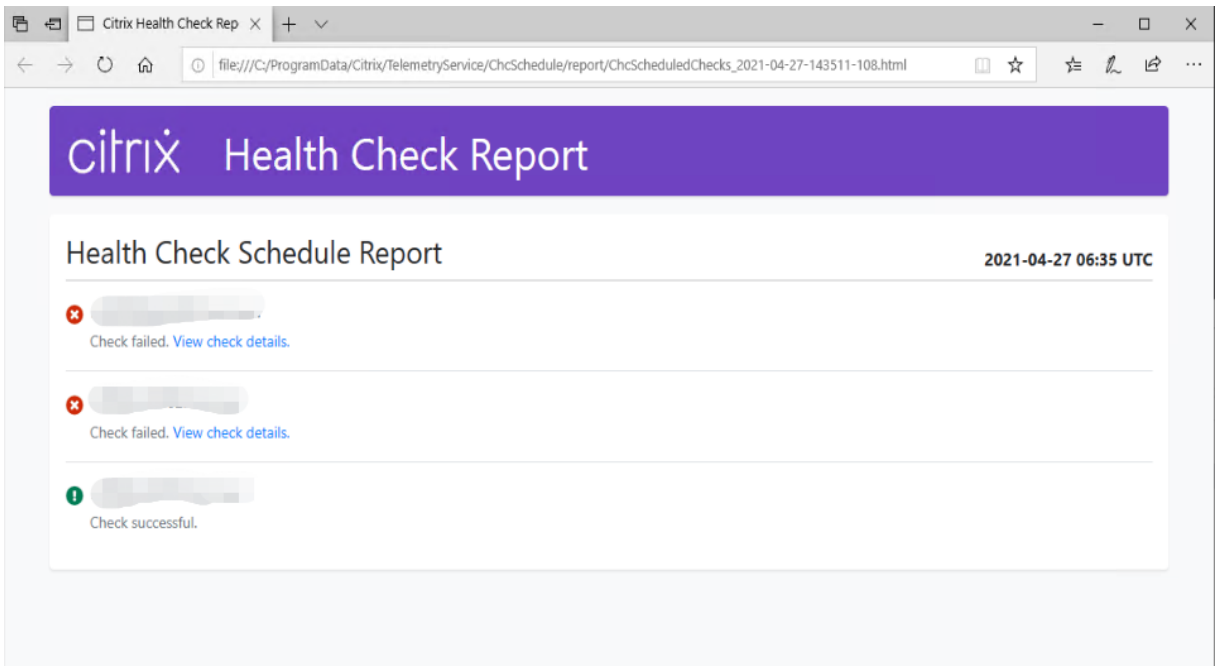
O ícone do relógio com um ponto vermelho indica que os problemas foram encontrados na última verificação. Para visualizar os resultados, clique no ícone do relógio e, em seguida, clique em **View results**.



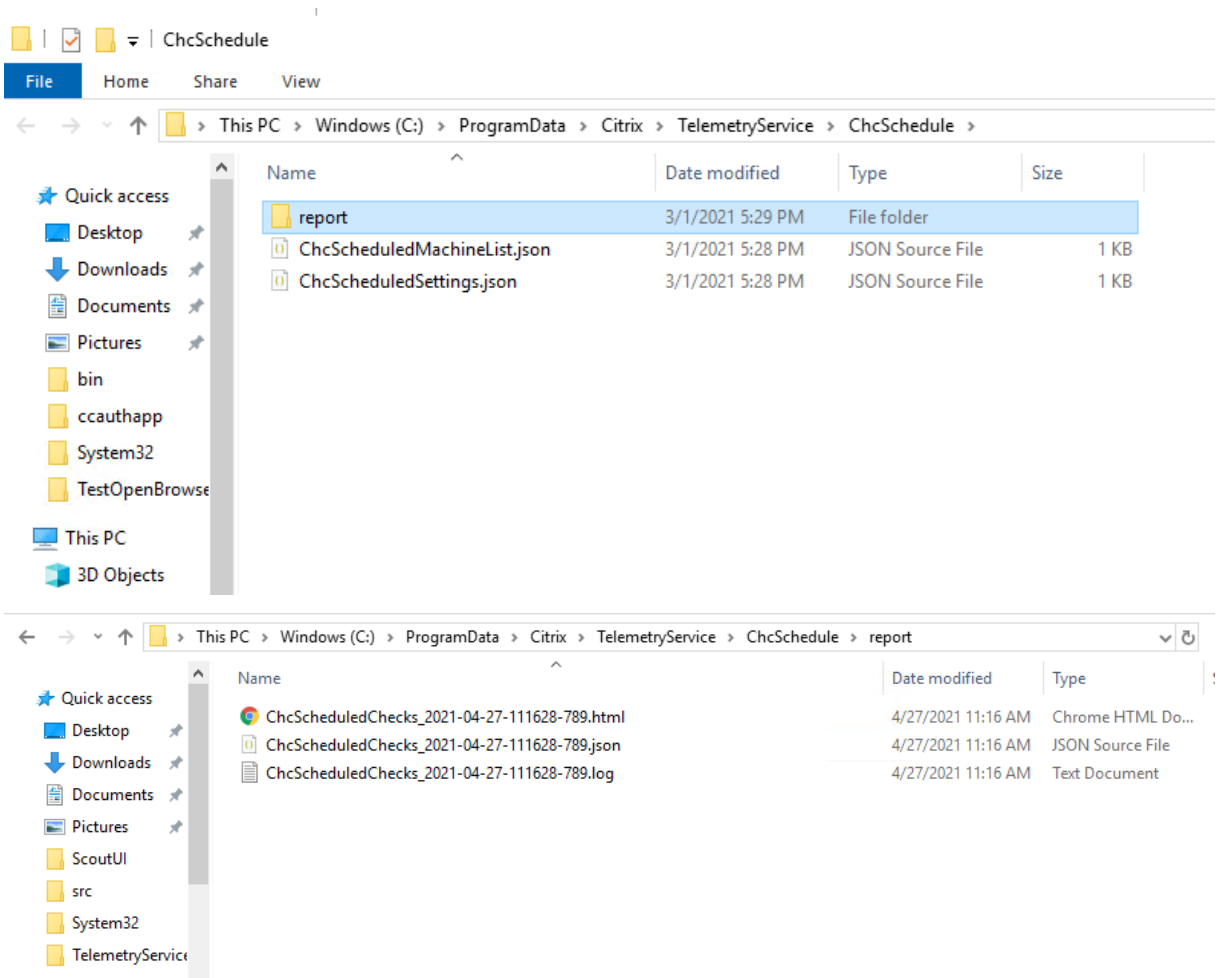
A página Schedule Reports mostra os resultados de todas as tarefas de verificação de integridade agendadas. Clique em **View Report** para verificar o relatório de cada programação.



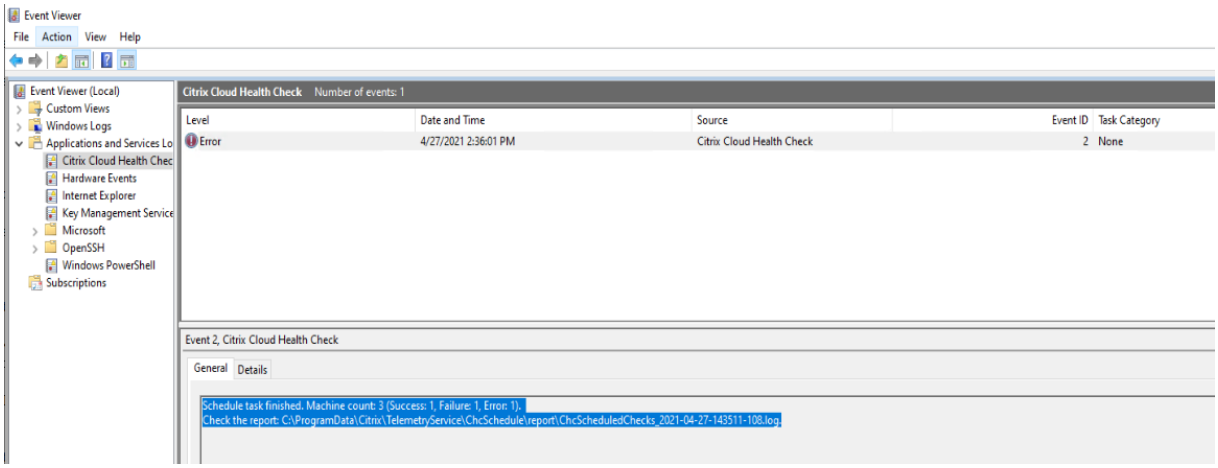
O relatório html lista o relatório geral de cada agendamento. Veja abaixo um exemplo de relatório:



Todos os resultados da verificação de integridade são armazenados em uma pasta chamada Chc-Schedule. O Cloud Health Check cria três arquivos durante cada execução de verificação. Até 500 logs de iteração são mantidos.

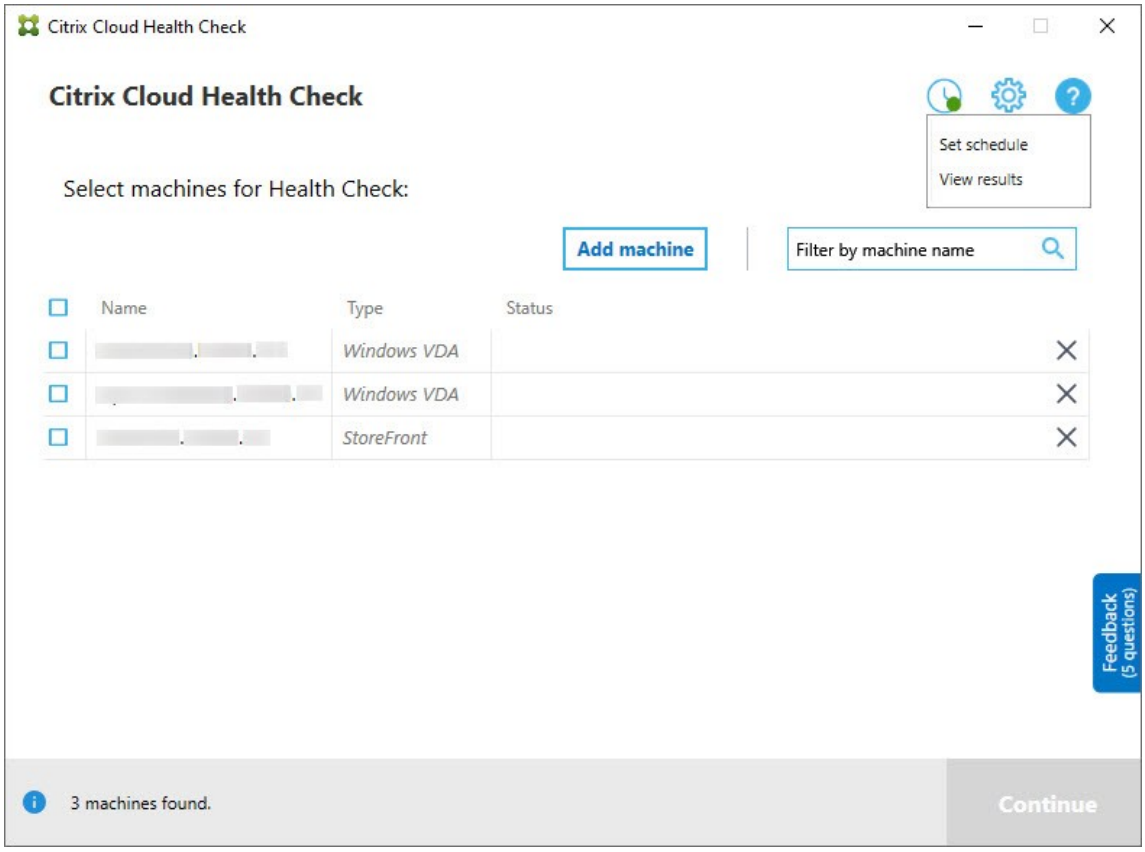


Se a caixa de seleção **Output results to Windows Event Log** estiver marcada, o resultado da verificação também será enviado para o Log de Eventos do Windows.

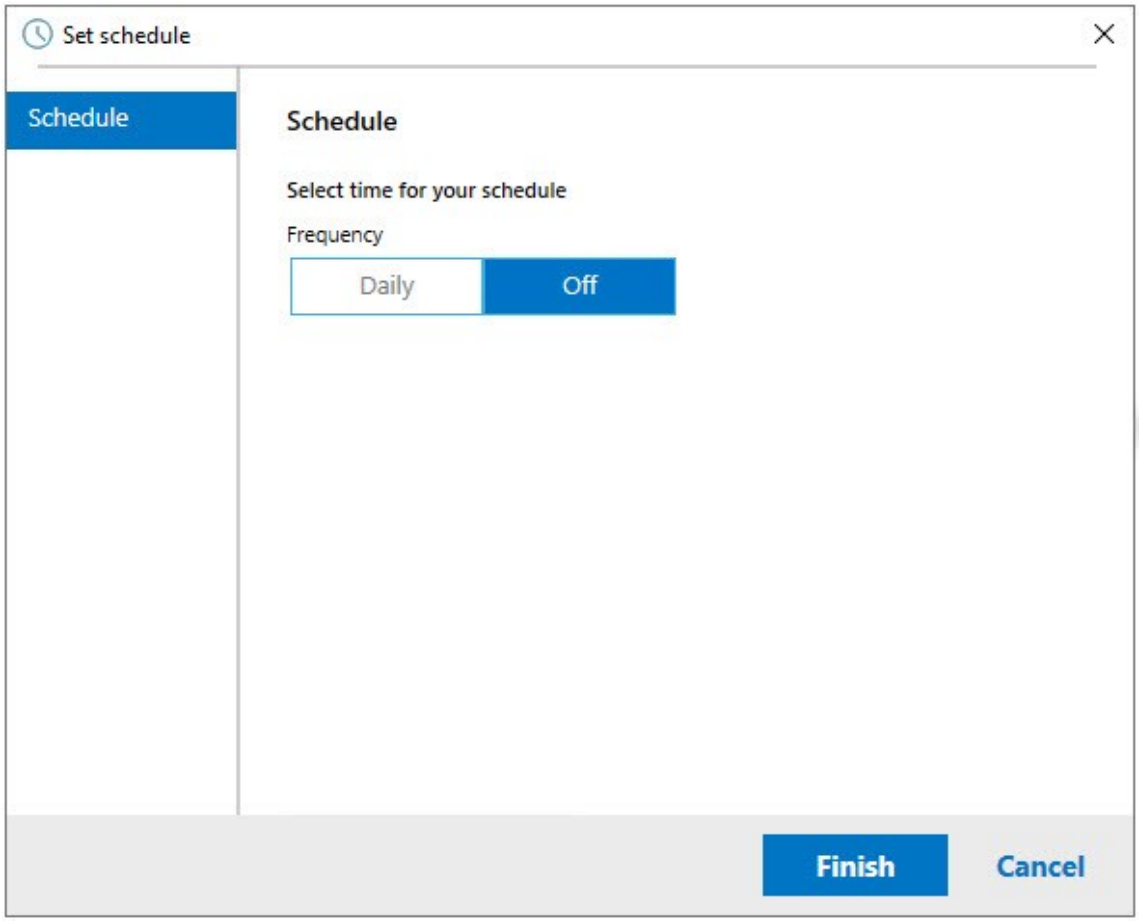


Desativar agendamentos

1. Clique no ícone de relógio e, em seguida, clique em **Set schedule**.



2. Clique em **Off** e clique em **Finish** para desativar 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 só pode agendar uma tarefa por vez em uma máquina ingressada no domínio. Se você definir a programação várias vezes, somente a última terá efeito.

Testes de verificação

Antes de iniciar uma verificação de integridade, 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 em uma máquina, o Cloud Health Check exibirá uma mensagem com sugestões de ações corretivas.

- **Cloud Health Check cannot reach this machine** - Certifique-se de que:
  - A máquina está ligada.

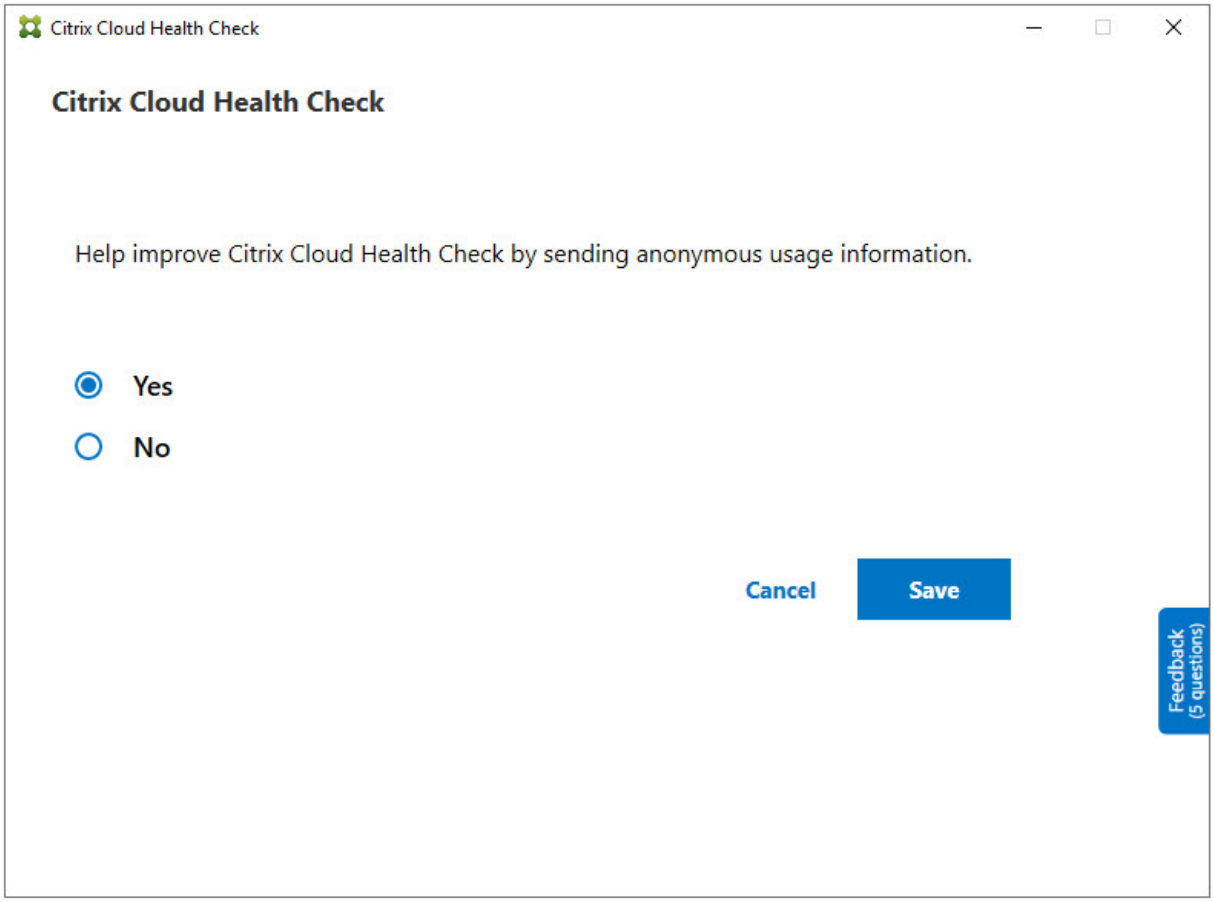
  - A conexão de rede está funcionando corretamente. (Isso pode incluir verificar se o firewall está configurado corretamente.)
  - O compartilhamento de arquivos e impressoras está ativado. Consulte a documentação da Microsoft para obter instruções.

- **Enable PSRemoting and WinRM** - Você pode habilitar a comunicação remota do PowerShell 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.
- **Cloud Health Check requires PowerShell 3.0 or later** - Instale o PowerShell 3.0 ou posterior na máquina e, em seguida, ative a comunicação remota do PowerShell.
- **WMI is not running on the machine** - Certifique-se de que o acesso ao Windows Management Instrumentation (WMI) está habilitado.
- **WMI connections blocked** - Ative o WMI no serviço Firewall do Windows.

Coleta de dados de uso

Quando você usa o Cloud Health Check, a Citrix usa o Google Analytics para coletar dados de uso anônimos que serão usados para futuros recursos e melhorias do produto. A coleta de dados está ativada por padrão.

Para alterar a coleta e o upload de dados de uso, clique na engrenagem **Settings** na interface do usuário do Cloud Health Check. Você pode escolher se deseja enviar as informações selecionando **Yes** ou **No** e, em seguida, clicando em **Save**.



Correção automática

A correção automática permite que o Cloud Health Check detecte e corrija automaticamente determinados problemas alterando as configurações ou reiniciando os serviços.

A correção automática verifica os seguintes itens do registro do VDA, com as correções recomendadas:

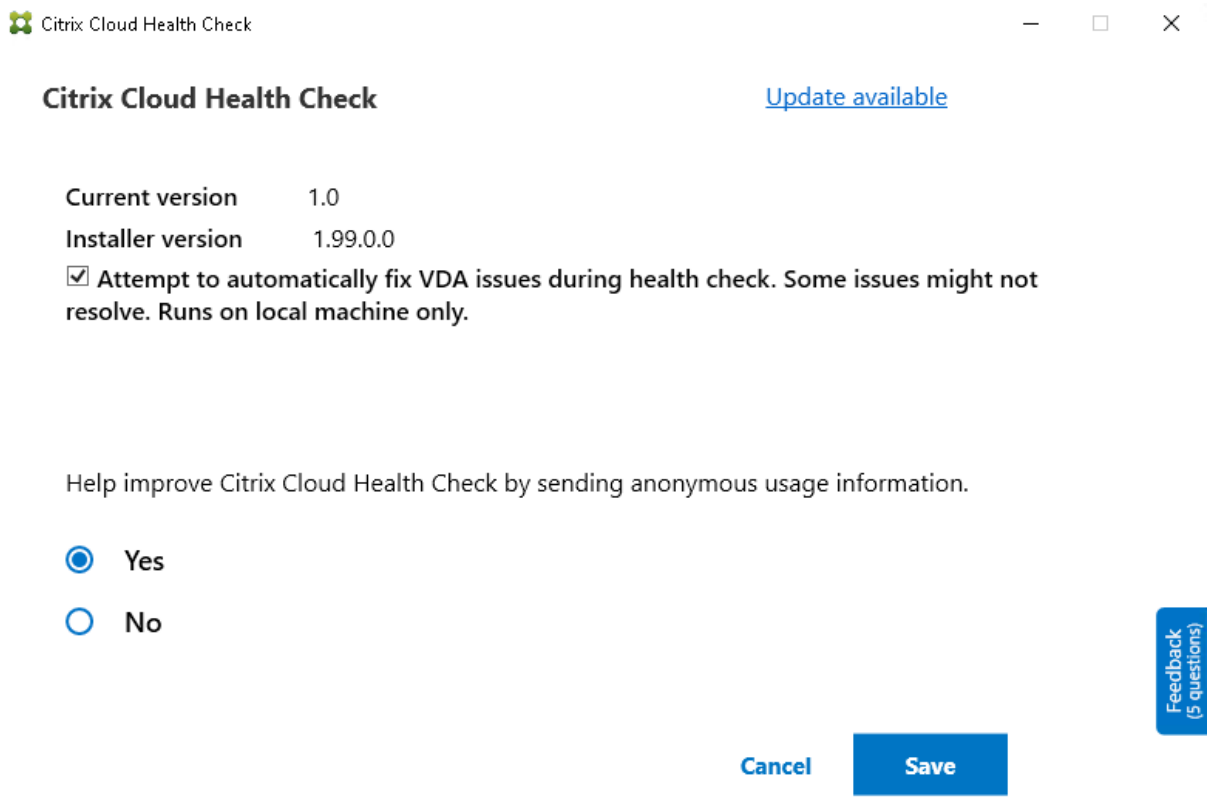
- Associação ao domínio da máquina VDA
  - Correção: Teste o canal de segurança de conexão com um modelo “repair”para corrigir
- Status dos serviços VDA
  - Correção: Reinicie o serviço BrokerAgent
- Comunicação com o Controller
  - Correção: Reinicie o serviço BrokerAgent
- Sincronização de tempo com o Controller

  - Correção: Execute o comando W32tm

Para inicializações de sessão, a correção automática verifica o seguinte item, com a correção recomendada:

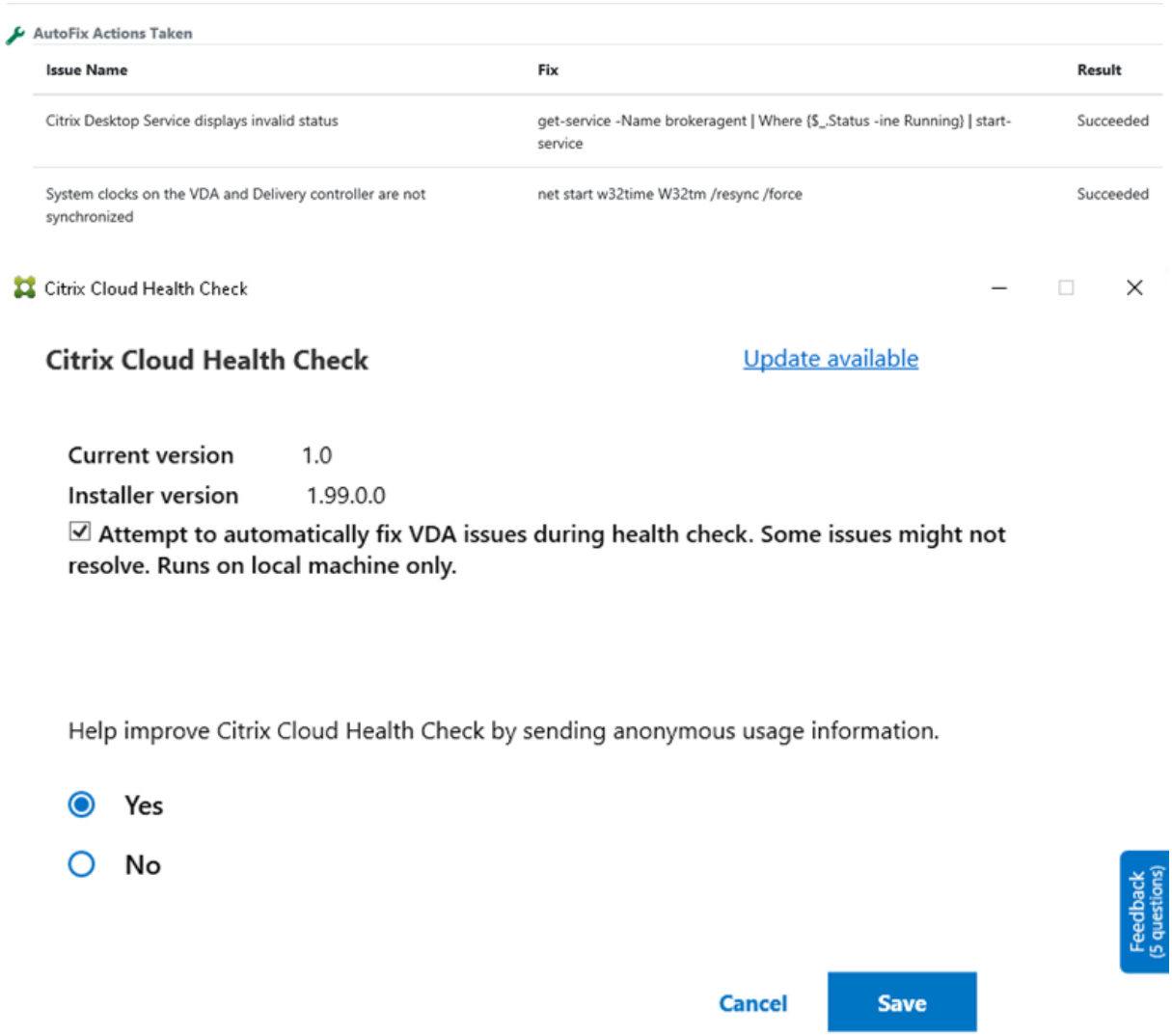
- Status do serviço de início de sessão
  - Correção: Reinicie o serviço BrokerAgent

Esse recurso é ativado por padrão. Para desativá-lo, clique no ícone de engrenagem no canto superior direito da janela principal do Cloud Health Check e desmarque **Attempt to automatically fix VDA issues during health check**.



Relatório de resultados

Depois de executar a correção automática, há uma seção no relatório de resultados da verificação que mostra todos os detalhes:



Solução de problemas

Se o Cloud Health Check apresentar falha na execução ou ocorrer alguma exceção, verifique o log do Cloud Health Check em `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

O log do Cloud Health Check de cada máquina de destino está em `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Para ativar 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.

Feedback

Para deixar comentários sobre o Cloud Health Check, responda à pesquisa da Citrix.

Log de configuração

December 6, 2023

> **Nota:**
>
> Os registros do log de configuração aparecem somente em inglês, independentemente do idioma selecionado para a sua conta do Citrix Cloud. As datas e horas associadas a esses registros estão no formato MM/DD/AA, expressas em Tempo Universal Coordenado (UTC).

O log de configuração é um recurso que captura as alterações de configuração de implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops) e atividades administrativas em um banco de dados de log no Citrix Cloud. Você pode usar o conteúdo no log para:

- Diagnosticar e solucionar problemas após fazer alterações de configuração. O log fornece uma trilha de localização.
- Auxiliar no gerenciamento de mudanças e rastrear as configurações.
- Informar atividades administrativas.

Neste Citrix DaaS, o log de configuração está sempre ativado. Você não pode desativá-lo.

Na interface de gerenciamento Full Configuration, você pode exibir 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. Nesse console, você não pode editar ou excluir o conteúdo do log. Você pode usar o Remote PowerShell SDK para agendar a exclusão periódica de dados do log.

Permissões necessárias (consulte Administração delegada):

- Full Administrators no Citrix Cloud, além de Cloud Administrators e Read Only Administrators no Citrix DaaS, podem visualizar logs de configuração no console **Manage**.
- Full Administrators e Cloud Administrators também podem baixar um relatório CSV da atividade de log, usando o PowerShell.

O que é registrado no log

As seguintes operações são registradas em log:

- Alterações de configuração e atividades administrativas iniciadas nas guias **Manage** e **Monitor**

- Scripts do PowerShell
- Solicitações de API REST

> **Nota:**
>
> Você não pode ver entradas de log de operações internas da plataforma Citrix Cloud, como configuração e gerenciamento de banco de dados.

Exemplos de alterações de configuração em log 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 do administrador
- Recursos e conexões do host
- Políticas da Citrix por meio do console **Manage**

Exemplos de alterações administrativas em log incluem:

- Gerenciamento de energia de uma máquina virtual ou área de trabalho do usuário
- Gerenciar ou monitorar funções enviando uma mensagem para um usuário

As seguintes operações não são registradas em log. (Muitas delas não estão disponíveis para administradores de clientes.)

- Operações automáticas, como a ativação do gerenciamento em pool de máquinas virtuais.
- Ações de políticas implementadas por meio do Console de gerenciamento de política de grupo (GPMC). Use as ferramentas da Microsoft para exibir os logs dessas ações.
- Alterações feitas por meio do registro ou de fontes que não a interface de gerenciamento Full Configuration, Monitor ou PowerShell.

Exibir conteúdo do log de configuração

Para exibir o conteúdo do log de configuração, siga estas etapas:

1. Faça login no Citrix Cloud. Selecione **My Services > DaaS** no menu superior esquerdo.
2. Em **Manage > Full Configuration**, selecione **Logging > Events** no painel esquerdo.

Por padrão, a exibição no painel central lista o conteúdo do log cronologicamente (entradas mais recentes primeiro), separado por data. Você pode:

- Ordenar a exibição pelo cabeçalho da coluna.
- Filtrar a exibição especificando um intervalo de dias ou um período de tempo personalizado, ou inserindo texto na caixa de pesquisa. Para retornar à exibição padrão depois de usar a pesquisa, apague o texto na caixa Search.

Características de exibição:

- As operações de alto nível criadas durante o gerenciamento e o monitoramento são listadas no painel central superior. Uma operação de alto nível resulta em uma ou mais chamadas de serviço e PowerShell SDK, que são operações de baixo nível. Quando você seleciona uma operação de alto nível no painel central superior, o painel inferior exibe as operações de nível baixo.
- Se você criar uma operação de baixo nível no PowerShell sem especificar uma operação de alto nível pai, o log de configuração cria 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 o registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Quando você exibe logs com base em intervalos de tempo, os registros incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se você solicitar os logs dos últimos cinco dias e um log com uma hora de início nos últimos cinco dias não tiver hora de término, ele será incluído.
- Lembre-se: você não pode ver entradas de log de operações internas da plataforma Citrix Cloud, como configuração e gerenciamento de banco de dados.

Exibir tarefas relacionadas às operações do catálogo de máquinas

Para exibir tarefas relacionadas às operações do catálogo de máquinas, navegue até **Manage > Full Configuration > Logging > Tasks**. A guia **Tasks** exibe apenas as tarefas relacionadas aos catálogos criados por meio do Machine Creation Services (MCS) ou Provisioning Services (PVS). Especificamente, as tarefas associadas às seguintes operações do catálogo de máquinas são exibidas:

- Criar catálogos
- Clonar catálogos
- Adicionar máquinas
- Remover máquinas
- Atualizar um catálogo (atualizar imagens ou máquinas)
- Reverter atualizações da máquina

> **Dica:**
>
> A guia **Tasks** exibe somente as tarefas relacionadas às alterações do esquema de provisionamento (criação ou modificação de um esquema de provisionamento).

Uma tarefa pode estar no seguinte estado:

- Completed
- Not started
- Running
- Canceled

- Failed
- Unknown

Para cancelar uma tarefa em execução, selecione-a e clique em **Cancel**. O cancelamento leva algum tempo para ser concluído.

Exemplos de tarefas em log 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
- Provisionamento de VMs para um determinado catálogo
- Remoção de VMs de um determinado catálogo
- Criação de um determinado catálogo

Por padrão, a exibição no painel central lista as tarefas registradas cronologicamente (as entradas mais recentes primeiro), separadas por data. Você pode classificar a exibição pelo cabeçalho da coluna. Para limpar tarefas concluídas, clique em **Clear Completed Tasks** na guia **Tasks**.

Exibir logs de API

Para visualizar os logs da API REST, navegue até **Manage > Full Configuration > Logging > APIs**. A guia **APIs** exibe as solicitações da API REST feitas durante um determinado período de tempo.

Esteja ciente das seguintes considerações:

- Os logs da API REST são apagados depois que você sai do console. (Eles também são apagados se você atualizar a janela do navegador.)
- Todas as operações no console que resultam em chamadas da API têm suas solicitações de API correspondentes exibidas na guia **APIs**.
- A exibição lista as solicitações de API cronologicamente (as entradas mais recentes primeiro), separadas por data. O número máximo de solicitações de API na tela é 1.000.

Associar metadados aos 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 do PowerShell `Set-LogHighLevelOperationMetadata` para associar um registro de log ao `MetadataMap`.
`Set-LogHighLevelOperationMetadata` usa os seguintes parâmetros:

- **Id**:ID da operação de alto nível.
- **InputObject**:as operações de alto nível às quais você adiciona os metadados. Essa é uma alternativa ao parâmetro `Id` em que um objeto de operação de alto nível ou uma lista de objetos é passada para o comando do PowerShell.
- **Name**:nome da propriedade dos metadados a serem adicionados. A propriedade deve ser exclusiva para a operação de alto nível especificada. A propriedade não pode conter nenhum dos seguintes caracteres:
  `()\/;:#.*?=<>|[]"'`
- **Value**:valor da propriedade.
- **Map**:dicionário de pares (nome, valor) para as propriedades. Essa 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 do 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 do PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

Recuperar usando os metadados

Execute os seguintes comandos do PowerShell para usar os metadados associados para recuperar os registros de log:

- Pesquise por chave e valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Pesquise por valor e qualquer chave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Pesquise por chave e qualquer valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```


Remover os metadados

Execute o comando do PowerShell `Remove-LogHighLevelOperationMetadata` para remover os metadados associados.
`Remove-LogHighLevelOperationMetadata` usa os seguintes parâmetros:

- **Id**:ID da operação de alto nível.
- **InputObject**:as operações de alto nível às quais você adiciona os metadados. Essa é uma alternativa ao parâmetro `Id`' em que um objeto de operação de alto nível ou uma lista de objetos é passada para o comando do PowerShell.
- **Name**:nome da propriedade dos metadados a serem removidos. Defina como $null para remover todos os metadados do objeto especificado.
- **Map**:dicionário de pares (nome, valor) para as propriedades. Isso pode ser uma tabela de hash (criada com @{"name1"= "val1"; "name2"= "val2"}) ou um dicionário de cadeias de caracteres (criado com o novo objeto "System.Collections.Generic.Dictionary[String, String]"). As propriedades cujos nomes correspondem às chaves no mapa são removidas.

Gerar relatórios

Para gerar um relatório CSV ou HTML contendo dados do log de configuração, use os cmdlets do PowerShell para o ConfigLogging Service no SDK do PowerShell remoto do Citrix Virtual Apps and Desktops. Para obter detalhes, consulte:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

Agendar a exclusão periódica de dados

Use o Remote PowerShell SDK para especificar por quanto tempo os dados são retidos no banco de dados do log de configuração. (Esse recurso não está disponível na interface de gerenciamento Full Configuration.) No Citrix DaaS, você deve ter acesso completo.

No cmdlet `Set-LogSite`, o parâmetro `-LoggingDBPurgeDurationDays` especifica por quantos dias os dados são retidos no banco de dados do log de configuração antes de serem excluídos automaticamente.

- Por padrão, o valor desse parâmetro é 0. Um valor zero significa que os dados no banco de dados do 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 do que o período de retenção são excluídos.

Use `Get-LogSite` para exibir o valor atual do parâmetro.

Diferenças do Citrix Virtual Apps and Desktops no local

Se você estiver familiarizado com o log de configuração no produto Virtual Apps and Desktops local, a versão do Citrix Cloud tem 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 do log de configuração, porque o banco de dados é gerenciado na plataforma Citrix Cloud.
- As exibições do log de configuração não incluem operações e atividades que são executadas na plataforma Citrix Cloud.
- O PowerShell é a sua única opção para criar um relatório CSV ou HTML das operações registradas no log. No produto local, os relatórios podem ser gerados a partir do Citrix Studio ou do PowerShell.
- Não é possível excluir o conteúdo do log de configuração.

Administração delegada

November 9, 2023

Visão geral

Com a administração delegada no Citrix Cloud, você pode configurar as permissões de acesso de que todos os seus administradores precisam, de acordo com suas funções na organização.

Por padrão, os administradores têm acesso completo. 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 gerais de gerenciamento de um administrador no Citrix Cloud.
- Configure o acesso personalizado para serviços assinados. No Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), 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 do 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 o acesso personalizado: administradores, funções e escopos.

- **Administradores:** um administrador representa uma pessoa identificada pelo login do Citrix Cloud, que normalmente é um endereço de e-mail. Cada administrador está associado a um ou mais pares de função e escopo.
- **Funções:** uma função representa um cargo de trabalho e tem permissões associadas a ela. Essas permissões permitem determinadas tarefas que são exclusivas do Citrix DaaS. Por exemplo, a função Administrador do grupo de entrega tem permissão para criar um grupo de entrega e remover uma área de trabalho 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 personalizadas internas. Você não pode alterar as permissões dentro dessas funções internas nem excluir essas funções.

  Você pode criar suas próprias funções de acesso personalizadas 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 tem.

  Uma função é sempre atrelada a um escopo.
- **Escopos:** um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma que seja relevante para a sua organização. Os objetos podem estar em mais de um escopo.

  Há um escopo interno: All, que contém todos os objetos. Os administradores do Citrix Cloud e do Help Desk estão sempre atrelados com o escopo All. Esse escopo não pode ser alterado para esses administradores.

  Quando você convida (adiciona) um administrador para esse serviço, uma função é sempre atrelada a um escopo (por padrão, o escopo All).

  Você cria e exclui escopos na interface **Manage > Full Configuration**. Você atribui pares de função/escopo no console do Citrix Cloud.

  O escopo não é mostrado para administradores com acesso completo. Por definição, esses administradores podem acessar todos os objetos de serviços de assinantes e do Citrix Cloud gerenciados pelo cliente.

Escopos e funções internas

O Citrix DaaS tem as seguintes funções internas.

- **Cloud Administrator:** pode executar todas as tarefas que podem ser iniciadas no Citrix DaaS.

  Pode ver as guias **Manage** e **Monitor** no console. Essa função é sempre combinada com o escopo All. Você não pode alterar o escopo.

  Não se confunda com o nome dessa função. Um Cloud Administrator com acesso personalizado não pode executar tarefas no nível do Citrix Cloud (as tarefas do Citrix Cloud exigem acesso total).

- **Read Only Administrator:** pode ver todos os objetos nos escopos especificados (além das informações globais), mas não pode alterar nada. Por exemplo, um Read Only Administrator com um escopo de Londres pode ver todos os objetos globais e todos os 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 (supondo que os escopos Londres e Nova York não se sobrepõem).

  Pode ver a guia **Manage** no console. Não pode ver a guia **Monitor**. Você pode alterar o escopo.

- **Help Desk Administrator:** pode exibir grupos de entrega e gerenciar sessões, máquinas e computadores associados a esses grupos. Pode ver informações do catálogo de máquinas e do host para os grupos de entrega que estão sendo monitorados. Também pode executar operações de gerenciamento de sessão e gerenciamento de energia da máquina para as máquinas nesses grupos de entrega.

  Pode ver a guia **Monitor** no console. Não pode ver a guia **Manage**. Essa função é sempre combinada com o escopo All. Você não pode alterar o escopo.

- **Machine Catalog Administrator:** pode criar e gerenciar catálogos de máquina e provisionar as máquinas neles. Pode gerenciar imagens básicas e instalar softwares, mas não pode atribuir aplicativos ou áreas de trabalho aos usuários.

  Pode ver a guia **Manage** no console. Não pode ver a guia **Monitor**. Você pode alterar o escopo.

- **Delivery Group Administrator:** pode entregar aplicativos, áreas de trabalho e máquinas. Também pode gerenciar as sessões associadas. Pode gerenciar configurações de aplicativos e áreas de trabalho, como configurações de gerenciamento de energia e políticas.

  Pode ver a guia **Manage** no console. Não pode ver a guia **Monitor**. Você pode alterar o escopo.

- **Host Administrator:** pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, computadores, aplicativos ou áreas de trabalho aos usuários.

  Pode ver a guia **Manage** no console. Não pode ver a guia **Monitor**. Você pode alterar o escopo.

- **Session Administrator:** pode visualizar grupos de entrega sendo monitorados e gerenciar suas sessões e máquinas associadas.

  Pode ver a guia **Monitor** no console. Não pode ver a guia **Manage**. Você não pode alterar o escopo.

- **Full Administrator:** pode executar todas as tarefas e operações. Um administrador completo é sempre combinado com **All scope**.

  Pode ver as guias **Manage** e **Monitor** no console. Essa função é sempre combinada com **All scope**. Você não pode alterar o escopo.

- **Full Monitor Administrator:** tem acesso total a todas as exibições e comandos na guia **Monitor**.

  Pode ver a guia **Monitor** no console. Não pode ver a guia **Manage**. Você não pode alterar o escopo.

- **Probe Agent Administrator:** tem acesso às APIs do Probe Agent.

  Pode ver a guia **Monitor** no console. Não pode ver a guia **Manage**. Tem acesso somente leitura à página **Applications**, mas não pode acessar nenhuma outra exibição.

A tabela a seguir resume quais guias do console são visíveis para cada função de acesso personalizado no Citrix DaaS e se a função pode ser usada com escopos personalizados.

Função de administrador de acesso personalizado	Pode ver a guia **Manage** no console?	Pode ver a guia **Monitor** no console?	A função pode ser usada com escopos personalizados?
Cloud Administrator	Sim	Sim	Não
Read Only Administrator	Sim	Não	Sim
Help Desk Administrator	Não	Sim	Não
Machine Catalog Administrator	Sim	Não	Sim
Delivery Group Administrator	Sim	Não	Sim
Host Administrator	Sim	Não	Sim
Session Administrator	Não	Sim	Não
Full Administrator	Sim	Sim	Não
Full Monitor Administrator	Não	Sim	Não

Função de administrador de acesso personalizado	Pode ver a guia **Manage** no console?	Pode ver a guia **Monitor** no console?	A função pode ser usada com escopos personalizados?
Probe Agent Administrator	Não	Sim	Não

> **Nota:**
>
> Funções de administrador de acesso personalizado (exceto Cloud Administrator e Help Desk Administrator) não estão disponíveis para Citrix Virtual Apps and Desktops Standard for Azure, Virtual Apps Essentials e Virtual Desktops Essentials.

Para exibir as permissões associadas a uma função:

1. Faça logon no Citrix Cloud. Selecione **My Services > DaaS** no menu superior esquerdo.
2. Em **Manage > Full Configuration**, selecione **Administrators** no painel esquerdo.
3. Selecione a guia **Roles**.
4. Selecione uma função no painel central superior. A guia **Role definition**, no painel inferior, lista as categorias e as permissões. Selecione uma categoria para ver as permissões específicas. A guia **Administrators** lista os administradores que receberam a função selecionada.

   Problema conhecido: uma entrada Full Administrator não exibe o conjunto correto de permissões para um administrador do Citrix DaaS de acesso completo.

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 alguns administradores fazem tudo. Não há delegação de acesso personalizado. Nesse caso, cada administrador tem acesso completo, que sempre tem o escopo All.
- Em implantações maiores com mais máquinas, computadores, aplicativos e áreas de trabalho, é necessária mais delegação. Vários administradores podem ter responsabilidades funcionais (funções) mais específicas. Por exemplo, dois têm acesso completo e os outros são administradores de help desk. Além disso, um administrador pode gerenciar apenas determinados grupos de objetos (escopos), como catálogos de máquinas em um departamento em particular. Nesse caso, crie novos escopos, além de administradores com a função de acesso personalizada e os escopos apropriados.

Resumo do gerenciamento do administrador

A configuração de administradores para o Citrix DaaS segue esta sequência:

1. Se você quiser que o administrador tenha uma função diferente de Full administrator (que abrange todos os serviços de assinante no Citrix Cloud) ou uma função interna, crie uma função personalizada.
2. Se você quiser que o administrador tenha um escopo diferente de All (e um escopo diferente seja permitido para a função desejada e ainda não tenha sido criado), crie escopos.
3. No Citrix Cloud, convide um administrador. Se você quiser que o novo administrador tenha algo diferente do que o acesso completo padrão oferece, especifique uma função de acesso personalizado e um par de escopo.

Posteriormente, 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 do Citrix Cloud. Um subconjunto dessas informações é repetido aqui.

> **Importante:**
>
> Não confunda como “custom”e “custom access”são usados.
>
> - Ao criar administradores e atribuir funções para o Citrix DaaS no console do Citrix Cloud, o termo “custom access”inclui as funções internas e quaisquer funções personalizadas adicionais que foram criadas na interface **Manage > Full Configuration** do serviço.
> - Na interface **Manage > Full Configuration** do serviço, “custom”simplesmente diferencia essa função de uma função interna.

O fluxo de trabalho geral para adicionar administradores é o seguinte:

1. Faça logon no Citrix Cloud e selecione **Identity and Access Management** no menu superior esquerdo.
2. Na página **Identity and Access Management**, selecione **Administrators**. A guia **Administrators** lista todos os administradores atuais da conta.
3. Na guia **Administrators**, selecione seu tipo de identidade, insira o endereço de e-mail do administrador e clique em **Invite**.

- Selecione **Full access** se quiser que o administrador tenha acesso completo. Dessa forma, o administrador pode acessar todas as funções de administrador do cliente no Citrix Cloud e em todos os serviços de assinante.

- Selecione **Custom access** se quiser que o administrador tenha acesso limitado. Em seguida, você pode selecionar uma função de acesso personalizado e um par de escopo. Dessa forma, o administrador tem as permissões desejadas ao fazer login no Citrix Cloud.

1. Clique em **Send Invite**. O Citrix Cloud envia um convite para o endereço de e-mail e adiciona o administrador à lista depois que o administrador conclui a integração.

Ao receber o e-mail, o administrador clica no link **Sign in** para aceitar o convite.

Para obter mais informações sobre como adicionar administradores, consulte Gerenciar administradores do Citrix Cloud.

Como alternativa, vá para **Manage > Full Configuration > Administrators > Administrators** e clique em **Add Administrator**. Você é levado diretamente para **Identity and Access Management > Administrators**, que é aberto em uma nova guia do navegador. Quando acabar de adicionar os administradores nessa guia, feche-a e retorne ao console para continuar com as suas outras tarefas de configuração.

Criar e gerenciar funções

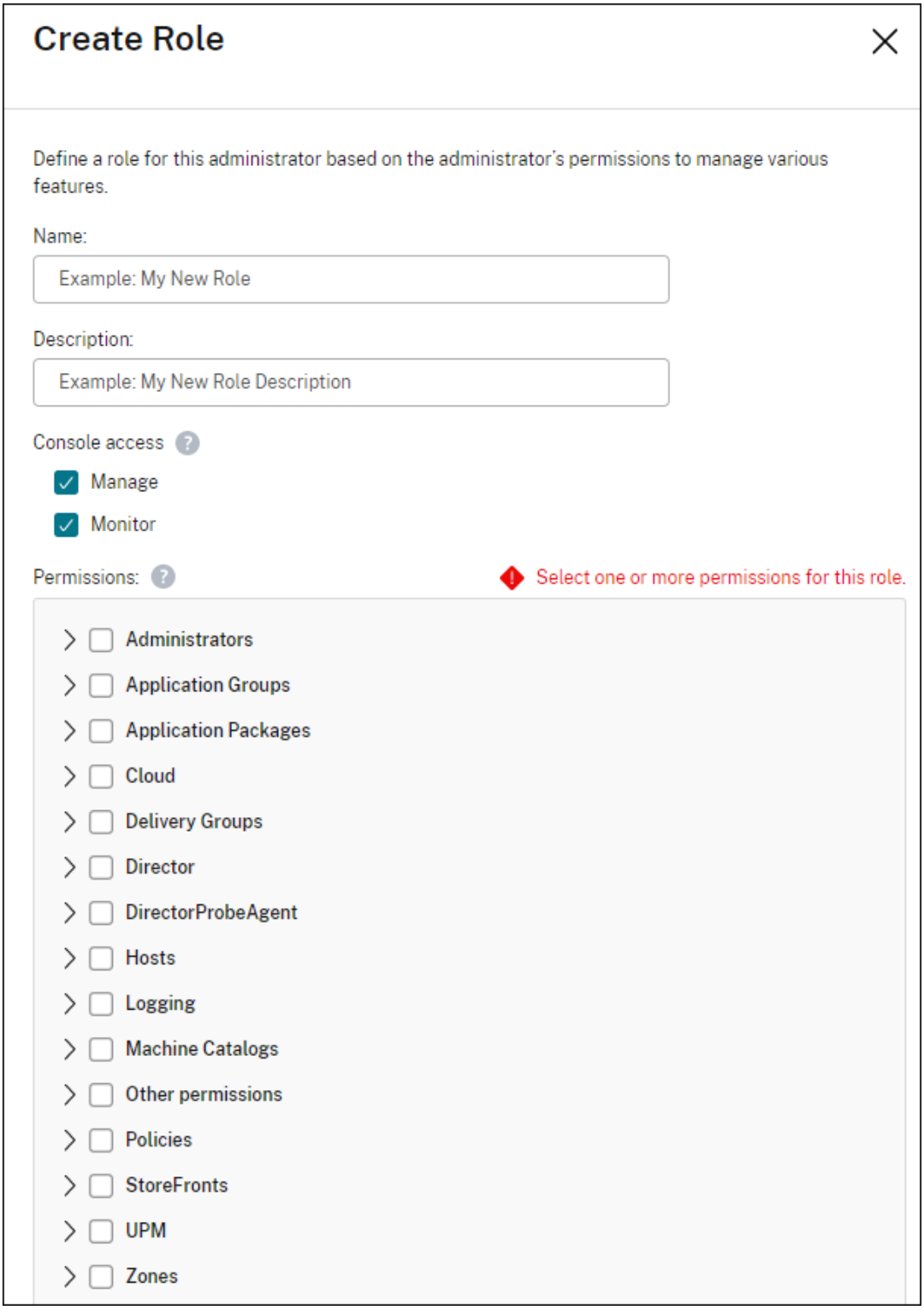
Quando os administradores criam ou editam uma função, eles podem ativar apenas as permissões que eles próprios têm. Esse controle impede que os administradores criem uma função com mais permissões do que as que têm no momento e a atribuam a si mesmos (ou editem uma função à qual já estão atribuídos).

O nome das funções personalizadas pode 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, barra vertical, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas e apóstrofo.

A descrição das funções pode conter até 256 caracteres Unicode.

1. Faça logon no Citrix Cloud, caso ainda não tenha feito. Selecione **My Services > DaaS** no menu superior esquerdo.
2. Em **Manage > Full Configuration**, selecione **Administrators** no painel esquerdo.
3. Selecione a guia **Roles**.
4. Siga as instruções para a tarefa que você deseja concluir:
    - **Exibir detalhes da função:** selecione a função no painel central. A parte inferior do painel central lista os tipos de objetos e as permissões associadas para a função. Clique na guia **Administrators** no painel inferior para exibir uma lista de administradores que atualmente têm a função.

- **Criar uma função personalizada:** selecione **Create Role** na barra de ações. Defina as configurações da seguinte forma:
  - Insira um nome e uma descrição.
  - Configure o acesso ao console. Determine quais consoles ficam visíveis para os administradores. Você pode continuar sem selecionar nenhum console. Nesse caso, os administradores com a função não podem acessar **Manage** e **Monitor**, mas podem acessar, exibir ou gerenciar objetos por meio de SDKs e APIs.
  - Selecione os tipos de objetos e as permissões. Para conceder permissão de acesso completo a um tipo de objeto, marque a sua caixa de seleção. Para conceder permissão em um nível granular, expanda o tipo de objeto e selecione **Read Only** ou objetos individuais em **Manage** dentro do tipo.



- **Copiar uma função:** selecione a função no painel central e, em seguida, selecione **Copy Role** na barra de ações. Altere o nome, a descrição, os tipos de objetos e as permissões, conforme necessário. Quando terminar, selecione **Save**.

- **Editar uma função personalizada:** selecione a função no painel central e selecione **Edit Role** na barra de ações. Altere o nome, a descrição, os tipos de objetos e as permissões, conforme necessário. Você não pode editar uma função interna. Quando terminar, selecione **Save**.
- **Excluir uma função personalizada:** selecione a função no painel central e selecione **Delete Role** na barra de ações. Quando solicitado, confirme a exclusão. Você não pode excluir uma função interna. 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 All para seus objetos relevantes. Por exemplo, um Delivery Group Administrator pode gerenciar todos os grupos de entrega. Para algumas funções de administrador, você pode criar um escopo que permita que essa função de administrador acesse um subconjunto dos objetos relevantes. Por exemplo, você pode querer que um Machine Catalog Administrator tenha acesso apenas aos catálogos que contêm um determinado tipo de máquinas, em vez de todos os catálogos.

- Full Access Administrators ou Cloud Administrators com acesso personalizado podem criar escopos para as funções de Read Only Administrator, Machine Catalog Administrator, Delivery Group Administrator e Host Administrator roles.
- Os escopos não podem ser criados para Full Access Administrators nem para Cloud Administrators ou Help Desk Administrators Esses administradores sempre têm o escopo All.

Regras para criar e gerenciar escopos:

- 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, barra vertical, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas e apóstrofo.
- A descrição dos escopos pode conter até 256 caracteres Unicode.
- Quando você copia ou edita um escopo, lembre-se de que a remoção de objetos do escopo pode tornar esses objetos inacessíveis a um administrador. Se o escopo editado estiver casado com uma ou mais funções, certifique-se de que as atualizações do seu escopo não tornem nenhum par de função/escopo inutilizável.

Para criar e gerenciar escopos:

1. Faça logon no Citrix Cloud. Selecione **My Services > DaaS** no menu superior esquerdo.
2. Em **Manage > Full Configuration**, selecione **Administrators** no painel esquerdo.
3. Selecione a guia **Scopes**.

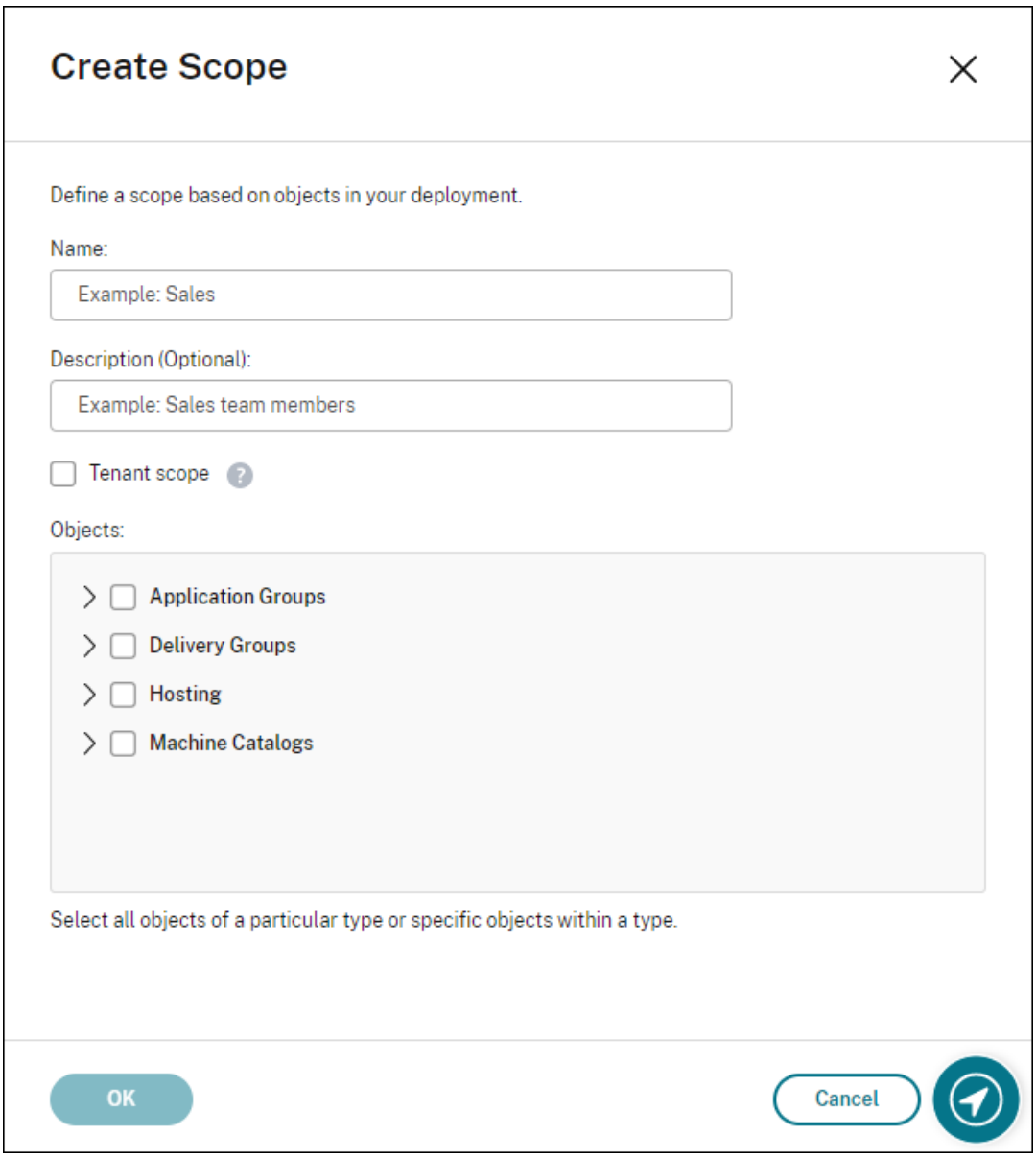
4. Siga as instruções para a tarefa que você deseja concluir:

   - **Exibir detalhes do escopo:** selecione o escopo. A parte inferior do painel lista os objetos e os administradores que têm esse escopo.
   - **Criar um escopo:** selecione **Create Scope** na barra de ações. Insira um nome e uma descrição. Os objetos são listados por tipo, como grupo de entrega e catálogo de máquinas.
     - Para incluir todos os objetos de um tipo específico (por exemplo, todos os grupos de entrega), marque a caixa de seleção do tipo de objeto.
     - Para incluir objetos individuais em um tipo, expanda o tipo e marque as caixas de seleção dos 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 gerenciamento deles no DaaS. Você pode selecionar uma pasta para selecionar todos os seus objetos ou expandir uma pasta para selecionar objetos específicos.

     - Para criar um cliente locatário, marque a caixa de seleção **Tenant scope**. 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 Gerenciamento de locatários.

   Quando terminar, selecione **OK**.



- **Copiar um escopo:** selecione o escopo no painel central e selecione **Copy Scope** na barra de ações. Mude o nome, a descrição. Altere os tipos de objetos e objetos, conforme necessário. Quando terminar, selecione **Save**.
- **Editar um escopo:** selecione o escopo no painel central e selecione **Edit Scope** na barra de ações. Altere o nome, a descrição, os tipos de objetos e os objetos, conforme necessário. Quando terminar, selecione **Save**.
- **Excluir um escopo:** selecione o escopo no painel central e selecione **Delete Scope** 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 esse escopo é atribuído a um administrador. Primeiro, remova a atribuição do par função/escopo para todos os administradores que o usam. Em seguida, exclua o escopo no console **Manage**.

Depois de criar um escopo, ele aparece na lista **Custom access** no console do Citrix Cloud. Você pode então selecioná-lo quando atribuir uma função a um administrador.

Por exemplo, digamos que você crie um escopo chamado CAD e selecione os catálogos que contêm máquinas adequadas para aplicativos CAD. Quando você retorna ao console do Citrix Cloud e seleciona **Edit scopes** para uma função, a lista de escopos disponíveis exibe o escopo CAD que você criou anteriormente.

O Cloud Administrator e o Help Desk Administrator sempre terão o escopo All, portanto, o escopo CAD não se aplica a eles.

Gerenciamento de locatários

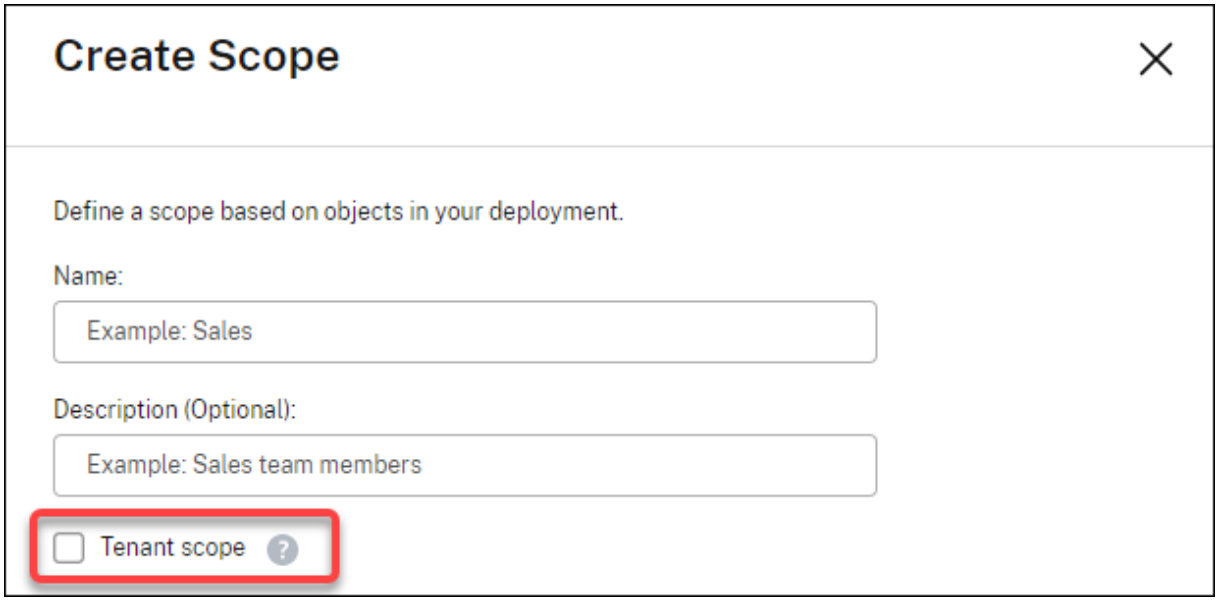
Usando a interface de gerenciamento Full Configuration, você pode criar locatários mutuamente exclusivos em um único Citrix DaaS. Você faz isso criando escopos de locatário em **Administrators > Scopes** e associando objetos de configuração relacionados, como catálogos de máquinas e grupos de entrega, a esses locatários. Como resultado, os administradores com acesso a um locatário podem gerenciar somente os objetos associados ao locatário.

Esse recurso é útil, por exemplo, se sua organização:

- Tem diferentes silos de negócios (divisões independentes ou equipes de gerenciamento de TI separadas) ou
- Tem vários sites locais e deseja manter a mesma configuração em uma única instância do Citrix DaaS.

A interface permite filtrar os clientes locatários pelo nome. Por padrão, a interface exibe informações sobre todos os clientes locatários. Para exibir informações sobre um locatário específico, selecione-o na lista no canto superior direito.

Criar um cliente locatário Para criar um cliente locatário, selecione **Tenant scope** ao criar um escopo. Ao selecionar a opção, você cria um tipo de escopo exclusivo que se aplica a objetos em cenários em que 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.



A guia **Scopes** exibe todos os itens de escopo. A única diferença entre os escopos regulares e os escopos de locatário está na coluna **Type**. Um campo de coluna em branco indica um escopo regular. Você pode clicar na coluna **Type** para classificar os itens do escopo, se necessário.

Para ver os recursos (objetos) anexados a um escopo, selecione **Administrators** no painel esquerdo. Na guia **Scopes**, selecione o escopo e, em seguida, selecione **Edit Scope** na barra de ações.

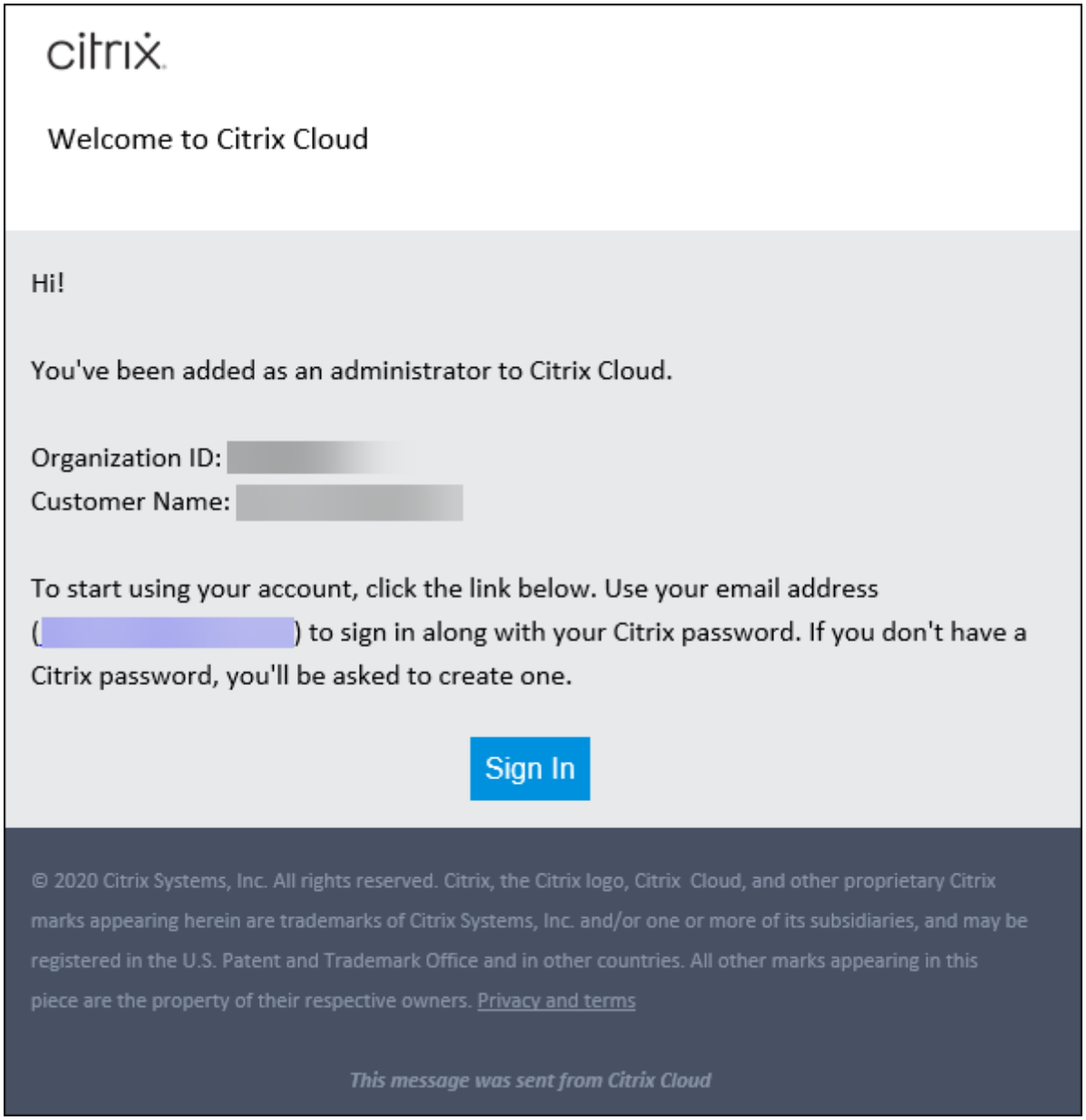
> **Dica:**
>
> A propriedade do locatário é atribuída no nível de escopo. Catálogos de máquinas, grupos de entrega, aplicativos e conexões herdam a propriedade do locatário do escopo aplicável.

Ao usar um escopo de locatário, esteja ciente das seguintes considerações:

- A propriedade do 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 do locatário. Por exemplo, ao selecionar um grupo de entrega, você deve selecionar a hospedagem associada e o catálogo de máquinas. Caso contrário, o grupo de entrega não poderá herdar a propriedade do locatário.
- Depois de criar um escopo de locatário, você pode editar as atribuições de locatário modificando os objetos. Quando uma atribuição de locatário é alterada, ela continua sujeita à restrição de que deve ser atribuída aos mesmos locatários ou a um subconjunto desses locatários. No entanto, os objetos de nível inferior não são reavaliados quando as atribuições do locatário mudam. Certifique-se de que os objetos estejam devidamente restritos quando alterar as atribuições do 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 associados a esse catálogo de máquinas.) Em seguida,

você pode alterar o catálogo de máquinas para que seja associado somente a `TenantA`. Como resultado, o grupo de entrega associado ao `TenantB` se torna inválido.

Configurar o acesso personalizado para administradores Depois de criar os escopos do locatário, configure o acesso personalizado para os respectivos administradores. Para obter mais informações, consulte Configurar o acesso personalizado para um administrador. O Citrix Cloud envia um convite para os administradores do cliente que você especificou e os adiciona à lista. Ao receber o e-mail, eles clicam no link **Sign in** para aceitar o convite. Quando fazem logon na interface de gerenciamento **Full Configuration**, eles veem os recursos que os pares de função e escopo atribuídos contêm.



Os administradores com acesso a um locatário podem gerenciar somente objetos (por exemplo, catál-

ogo de máquinas, grupo de entrega) associados ao locatário.

Configurar o acesso personalizado para um administrador

Esse recurso permite definir permissões de acesso de administradores existentes ou administradores que você convidar de uma forma que se alinhe com a função que tem na sua organização.

As alterações feitas às permissões de acesso levam 5 minutos para entrarem em vigor. Sair da interface de gerenciamento Full Configuration e entrar novamente faz com que as alterações entrem em vigor imediatamente. Nos cenários em que os administradores continuam a usar a interface de gerenciamento depois que as alterações entram em vigor sem se reconectarem a ela, um aviso aparece quando tentam acessar itens para os quais não têm mais permissões.

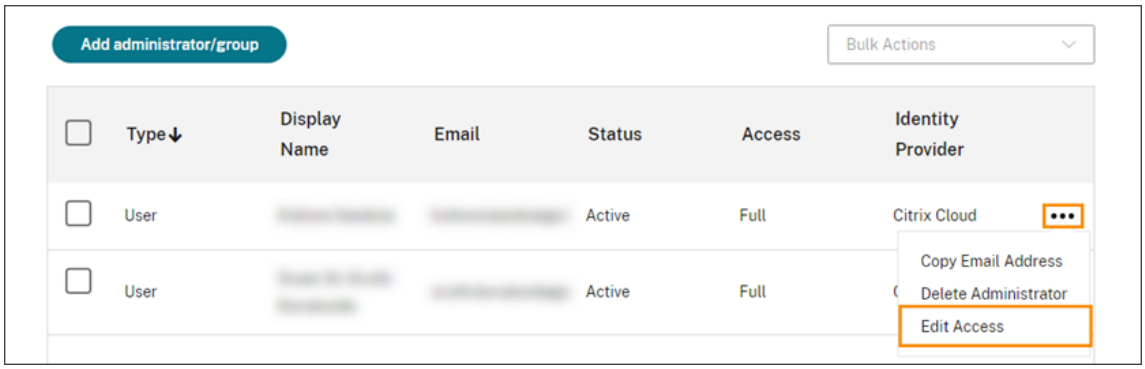
Por padrão, quando você convida administradores, eles têm acesso completo. O acesso completo permite que o administrador gerencie todos os serviços de assinante e todas as operações do Citrix Cloud (como convidar mais administradores). Uma implantação do Citrix Cloud precisa de pelo menos um administrador com acesso completo.

Você também pode conceder acesso personalizado quando convidar um administrador. O acesso personalizado permite que o administrador gerencie somente os serviços e as operações que você especificar.

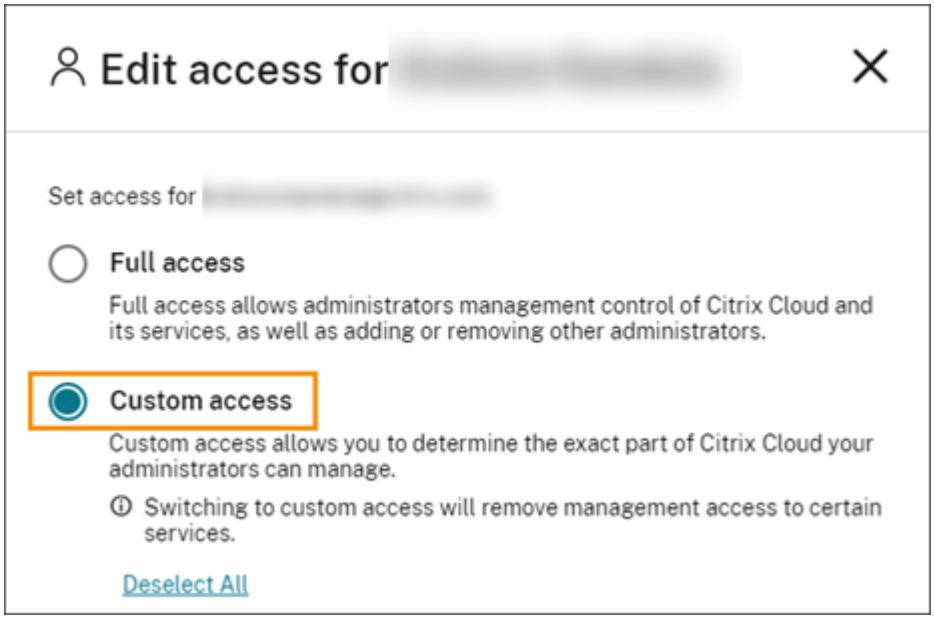
Quando você cria uma função ou escopo no Citrix DaaS, ele aparece na lista de acesso personalizado e pode ser selecionado. Ao selecionar uma função para um administrador, você pode modificar os escopos conforme necessário para refletir a função do administrador em sua organização.

Para configurar o acesso personalizado para um administrador:

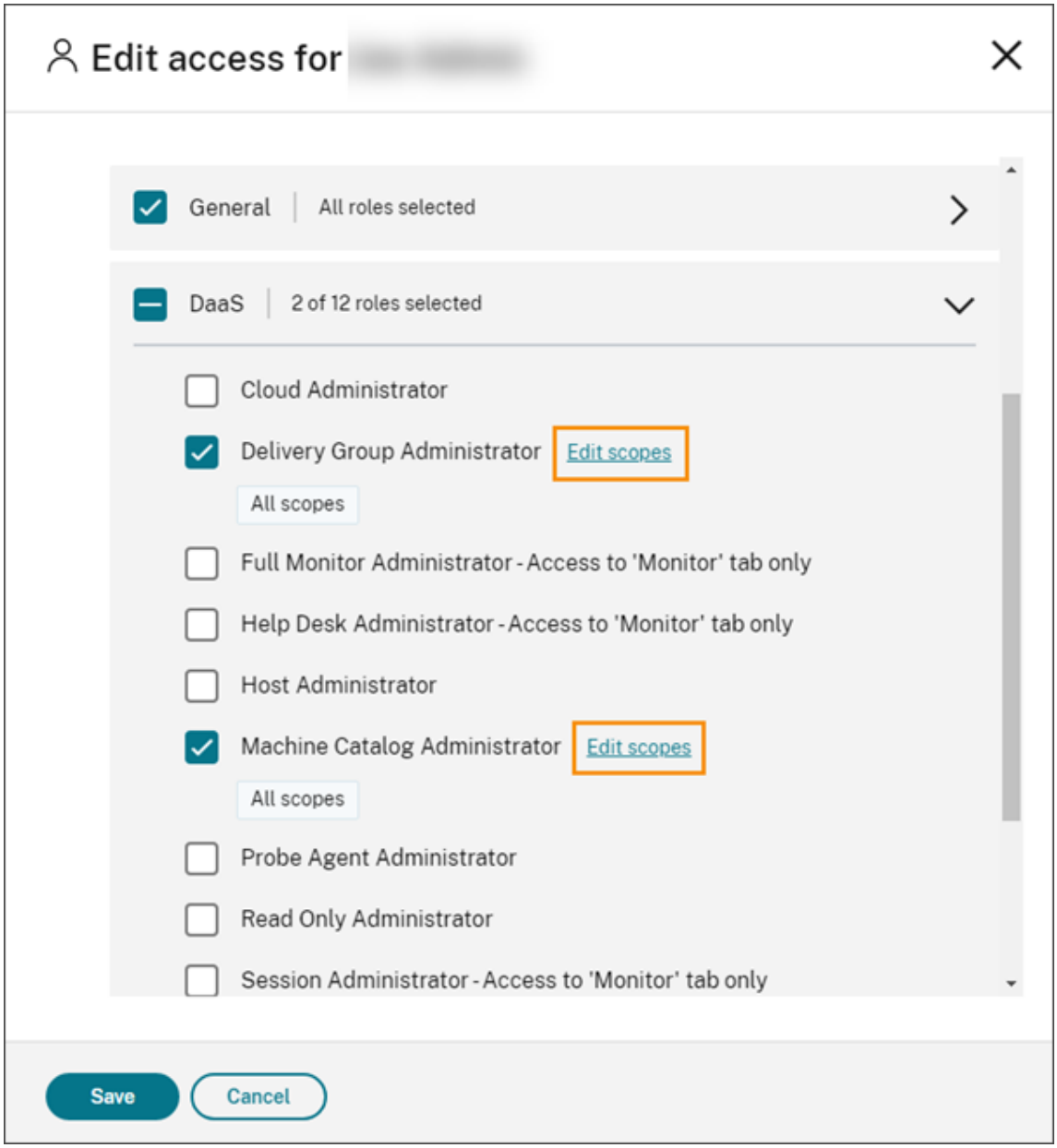
1. Faça logon no Citrix Cloud. Selecione **Identity and Access Management** > **Administrators** no menu superior esquerdo.
2. Localize o administrador que deseja gerenciar, selecione o menu de reticências e selecione **Edit access**.



3. Selecione **Custom access**.

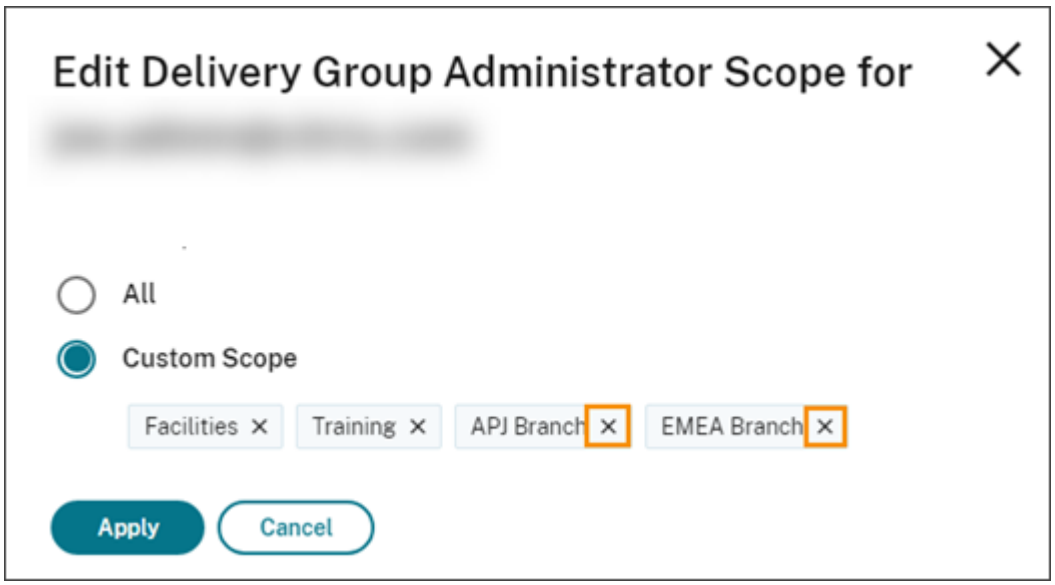


4. Em **DaaS**, selecione ou remova as marcas de seleção ao lado de uma ou mais funções. Para modificar os escopos associados a uma função atribuída, selecione **Edit scopes**.

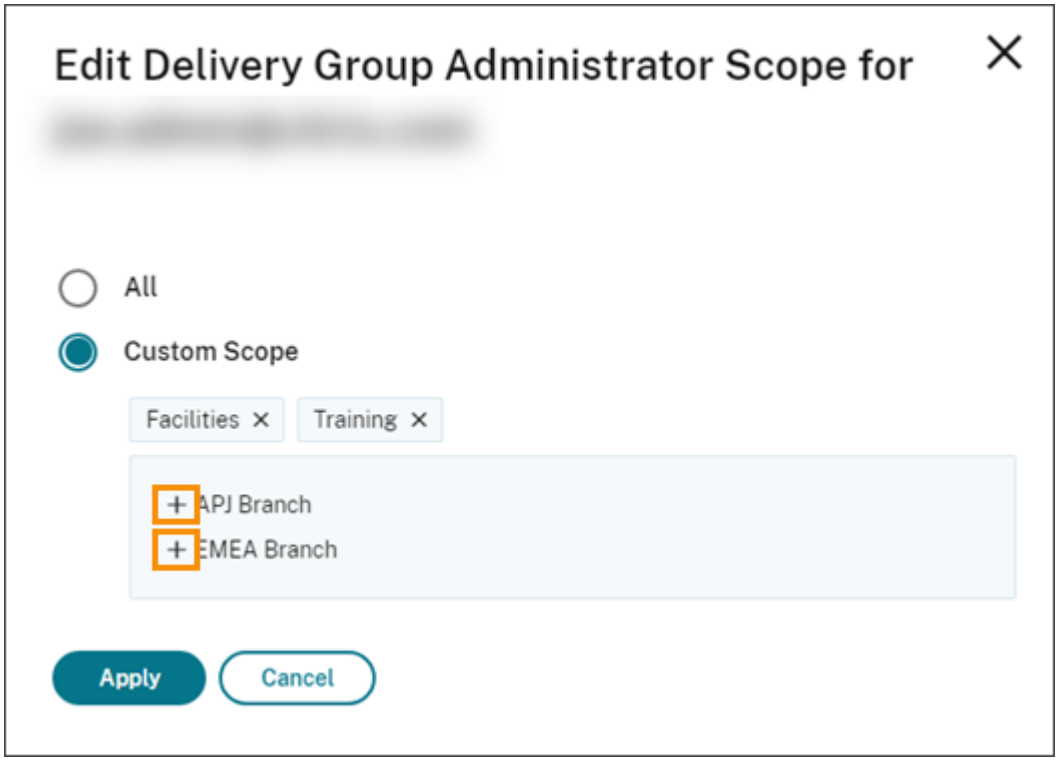


Por padrão, cada função selecionada tem todos os escopos selecionados, conforme indicado pelo rótulo **All scopes**.

5. Para especificar os escopos de uma função selecionada, selecione **Custom Scope** e 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.



Os escopos que foram removidos e estão disponíveis para serem adicionados à função aparecem em uma lista abaixo dos escopos que já foram adicionados. Para adicionar um escopo à função, selecione o ícone de adição do escopo.



6. Quando terminar de selecionar os escopos, selecione **Apply**.
7. Selecione **Save** para salvar as funções selecionadas para o administrador.

Diferenças do Citrix Virtual Apps and Desktops no local

Se você estiver familiarizado com a administração delegada no produto Citrix Virtual Apps and Desktops no local, a versão do Citrix DaaS tem várias diferenças.

No Citrix Cloud:

- Os administradores são identificados pelo login do Citrix Cloud, não pela conta do Active Directory. Você pode criar pares de função/escopo para indivíduos do Active Directory, mas não grupos.
- Os administradores são criados, configurados e excluídos no console do Citrix Cloud, em vez do Citrix DaaS.
- Os pares de função/escopo são atribuídos aos administradores no console do Citrix Cloud, em vez do Citrix DaaS.
- Os relatórios não estão disponíveis. Você pode visualizar as informações de administrador, função e escopo na interface **Manage > Full Configuration** do serviço.
- O Cloud Administrator de acesso personalizado é semelhante a um Full Administrator na versão local. Ambos têm permissões completas de gerenciamento e monitoramento para a versão do Citrix Virtual Apps and Desktops que está sendo usada.

  No entanto, no Citrix DaaS, não há função chamada Full Administrator. Não considere semelhantes "Full access"no Citrix Cloud e "Full administrator"no Citrix Virtual Apps and Desktops no local. Full Access no Citrix Cloud abrange os domínios, bibliotecas, notificações e locais de recursos no nível da plataforma, além de todos os serviços de assinantes.

Diferenças das versões anteriores do Citrix DaaS

Antes do lançamento do recurso de acesso personalizado expandido (setembro de 2018), havia duas funções de administrador de acesso personalizado: Full Administrator e Help Desk Administrator. Quando a sua implantação tiver a administração delegada habilitada (que é uma configuração de plataforma), essas funções são mapeadas automaticamente.

- Um administrador que foi configurado anteriormente como um **Virtual Apps and Desktops (ou XenApp e XenDesktop) Service: Full Administrator** de acesso personalizado, agora é um **Cloud Administrator** de acesso personalizado.
- Um administrador que foi configurado anteriormente como um **Virtual Apps and Desktops (ou XenApp e XenDesktop) Service: Help Desk Administrator** de acesso personalizado, agora é um **Help Desk Administrator** de acesso personalizado.

Mais informações

Consulte Administração delegada e monitoramento para obter informações sobre administradores, funções e escopos usados no console **Monitor** do serviço.

Página inicial da interface Full Configuration

November 9, 2023

Fornece uma visão geral da sua implantação e das cargas de trabalho do Citrix DaaS, além de informações que ajudam você a aproveitar ao máximo a sua assinatura. A página compreende as seguintes partes:

- Visão geral de serviços, em Service overview
- Alertas de integridade do serviço
- Recomendações, em Recommendations
- Novidades
- Recursos em Preview, em Preview features
- Introdução

Para acessar a página inicial, siga estas etapas:

1. Faça logon no Citrix Cloud.
2. No bloco **DaaS**, clique em **Manage**.
3. Selecione **Manage > Full Configuration**. A página inicial é exibida.

Visão geral de serviços, em Service overview

Fornece uma visão geral da implantação e das cargas de trabalho do Citrix DaaS:

- **Resources**. Mostra o número de recursos implantados e as contagens por categoria.

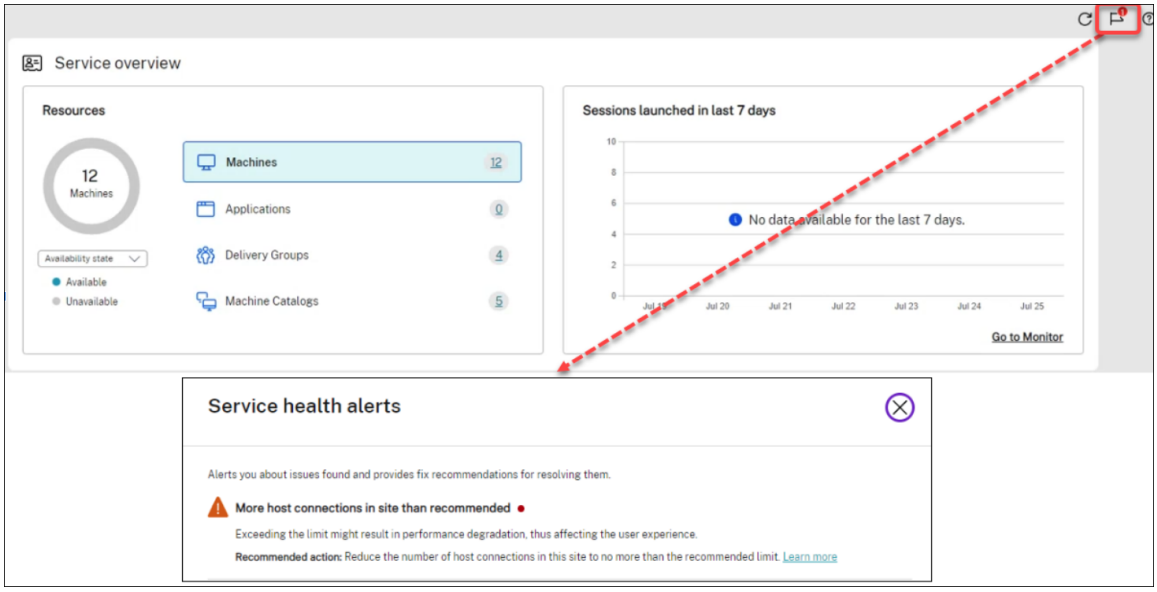
Recurso	Para exibir contagens por categoria
Máquinas	Clique em **Machines**, selecione um estado e passe o mouse sobre o gráfico de rosca para obter detalhes. Opções disponíveis: **Availability state** (Available, In use, Off e Unavailable), **Registration state** (Registered e Unregistered) e **Maintenance state** (In maintenance e Not in maintenance). Ao visualizar as contagens de máquinas por estado de disponibilidade, você pode clicar em um estado para ver os detalhes da máquina correspondente.
Aplicativos	Clique em **Applications** e passe o mouse sobre o gráfico de rosca para obter detalhes.
Grupos de entrega	Clique em **Delivery Groups** e passe o mouse sobre o gráfico de rosca para obter detalhes.
Catálogos de máquinas	Clique em **Machine Catalogs** e passe o mouse sobre o gráfico de rosca para obter detalhes.

- **Sessions launched in last 7 days**. Mostra o número de sessões de áreas de trabalho e aplicativos iniciadas diariamente nos últimos sete dias. Para se aprofundar em mais detalhes, clique em **Go to Monitor**.

Alertas de integridade do serviço

Alerta você sobre problemas encontrados e fornece recomendações para resolvê-los. Os alertas aparecem com símbolos de aviso e erro.

> **Nota:**
>
> Os diagnósticos são atualizados de hora em hora.
>
> Exemplo de alerta:



Recomendações, em Recommendations

Recomenda recursos que estão disponíveis com a sua assinatura, como o Workspace Environment Management e o AutoScale. Para interagir conosco, selecione se gostou ou não de uma recomendação e deixe seu feedback.

> **Nota:**
>
> Se você não gostar de uma recomendação, a recomendação desaparecerá. Se você não gostar de nenhuma recomendação ou do widget de recomendação, o widget de recomendação desaparecerá.

Novidades

Mostra uma lista selecionada dos recursos mais recentes do Citrix DaaS que são mais valiosos para sua empresa. Usar esses recursos ajuda você a aproveitar ao máximo sua assinatura. Para obter uma lista completa dos novos recursos, consulte Novidades.

Recursos em Preview, em Preview features

Mostra os recursos que estão atualmente na versão Preview. Como administrador do Citrix Cloud com acesso total, você pode ativar ou desativar os recursos em Preview sem entrar em contato com a Citrix. Demora até 15 minutos para que as alterações entrem em vigor.

Os recursos em Preview não são recomendados para uso em ambientes de produção. Os problemas encontrados nos recursos em Preview não recebem o Suporte Técnico da Citrix.

Introdução

Mostra as etapas que o orientam na configuração inicial de aplicativos e áreas de trabalho.

As etapas de configuração são as seguintes:

1. Criar locais de recursos

   Locais de recursos referem-se a locais que contêm aplicativos e áreas de trabalho que você deseja entregar aos seus usuários. Esta etapa permite adicionar seus locais de recursos ao DaaS e instalar os Cloud Connectors neles. Os Cloud Connectors servem como canais que autenticam e criptografam toda a comunicação entre o Citrix Cloud e seus recursos.

2. Criar uma conexão de host

   Os hosts são hipervisores ou serviços em nuvem que estão em uso em seus locais de recursos. Esta etapa permite especificar as informações que o DaaS usa para se comunicar com as VMs em um host. As informações detalhadas incluem a localização do recurso, o tipo de host, as credenciais de acesso, o método de armazenamento a ser usado e quais redes as VMs do host podem usar.

3. Preparar uma imagem mestre

   Uma imagem mestre inclui o sistema operacional, todos os aplicativos necessários e o Virtual Delivery Agent (VDA). Os VDAs estabelecem e mantêm conexões entre máquinas virtuais e dispositivos do usuário.

4. Criar um catálogo de máquinas

   Um catálogo de máquinas é uma coleção de VMs idênticas com SO de sessão única ou multissessão que você atribui aos usuários. Esta etapa permite criar um catálogo de máquinas especificando a tecnologia de provisionamento, a imagem mestre e o tamanho da máquina virtual.

5. Atribuir usuários

   Um grupo de entrega é uma coleção de máquinas selecionadas de um ou mais catálogos de máquinas. Essa etapa permite criar grupos de entrega para especificar quais equipes, departamentos ou tipos de usuários podem usar quais máquinas.

6. Configurar o Workspace

   Compartilhe o URL do Workspace em **Workspace Configuration > Access** com os seus usuários.

Licenças

June 24, 2022

Este artigo aborda tarefas e recursos para licenças Microsoft e licenças Citrix.

Configurar um servidor de licenças Microsoft RDS para cargas de trabalho do Windows Server

Essas informações se aplicam quando você entrega 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 2019. Normalmente, isso requer uma licença de acesso ao cliente dos Serviços de Área de Trabalho Remota (RDS CAL). O VDA deve poder entrar em contato com um servidor de licença 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 este método, você pode fazer com que esse 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 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 da Microsoft:

1. Instale um Servidor de Licenças de Serviços de Área de Trabalho Remota em uma máquina virtual disponível. A máquina virtual deve estar sempre disponível. As cargas de trabalho do serviço Citrix devem poder acessar 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 Model 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 de licença Citrix

Para obter informações sobre o uso da licença Citrix, consulte:

- Monitorar a licença e o uso ativo para serviços em nuvem
- Monitore a licença e o uso ativo do Citrix DaaS

Licenciamento multitipos

August 17, 2023

O licenciamento multitipos suporta o consumo de diferentes direitos de licença em uma única implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Este artigo se aplica a você, caso tenha mais de um direito de licença Citrix. Um direito da Citrix é uma combinação de:

- Produto, que no contexto atual do DaaS é sempre Citrix DaaS
- Edição do serviço (por exemplo: Advanced, Advanced Plus, Premium ou Premium Plus)
- Modelo da licença (por exemplo: usuário/dispositivo ou simultâneo)

Regras para misturar direitos

As regras para misturar as edições de serviço são as seguintes:

- Apenas a combinação de DaaS Advanced e Advanced Plus é permitida
- Apenas a combinação de DaaS Premium e Premium Plus é permitida
- O DaaS Standard não pode ser combinado com nenhuma outra edição

Você pode misturar os modelos de licenças quando as regras da edição de serviço anteriores são seguidas.

Direitos no nível de local e de grupo de entrega

Você pode configurar e usar os direitos de licença nos dois níveis a seguir:

- Site (sua implantação do produto Citrix DaaS)
- Grupo de entrega

Se você ainda não configurou os direitos de site ou de grupo de entrega, esteja ciente do seguinte comportamento padrão:

- Se você tiver mais de um direito, o mais capaz entre os direitos disponíveis será selecionado como direito em todo o site, desde que tenham sido solicitados ao mesmo tempo. Caso contrário, o primeiro que surgiu se torna o padrão em todo o site, a menos que seja explicitamente alterado posteriormente.
- O direito do site é usado, a menos que um direito de grupo de entrega esteja configurado.

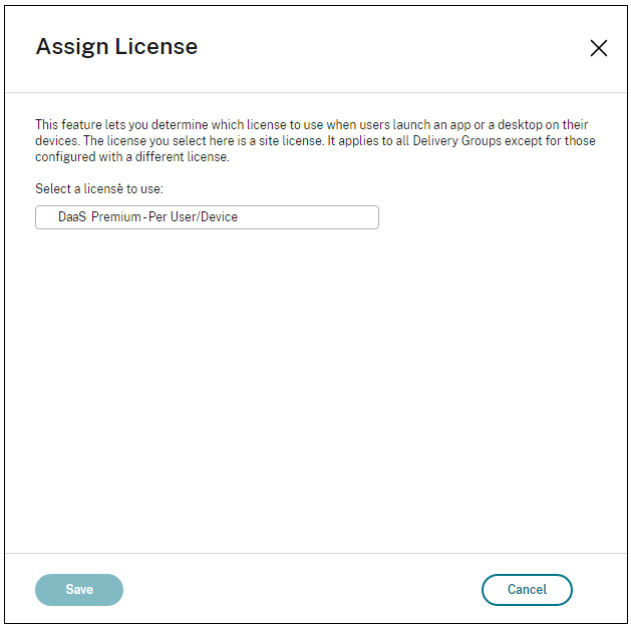
> **Nota:**
>
> A configuração de direitos para um site ou grupo de entrega afeta como o consumo de licença é

> computado nas exibições de uso da licença no Citrix Cloud.

Exibir e atualizar o direito no nível do site

Para especificar qual direito de licença usar em todo o site, navegue até **Full Configuration > Settings > Assign license** e clique em **Edit**. A folha **Assign License** é exibida. Para obter informações sobre como acessar a página **Full Configuration**, consulte a documentação do Citrix DaaS.

Na folha **Assign License**, selecione uma licença que você deseja que o site use. A licença selecionada se aplica a todos os grupos de entrega no site, exceto aqueles grupos de entrega configurados com uma licença diferente.



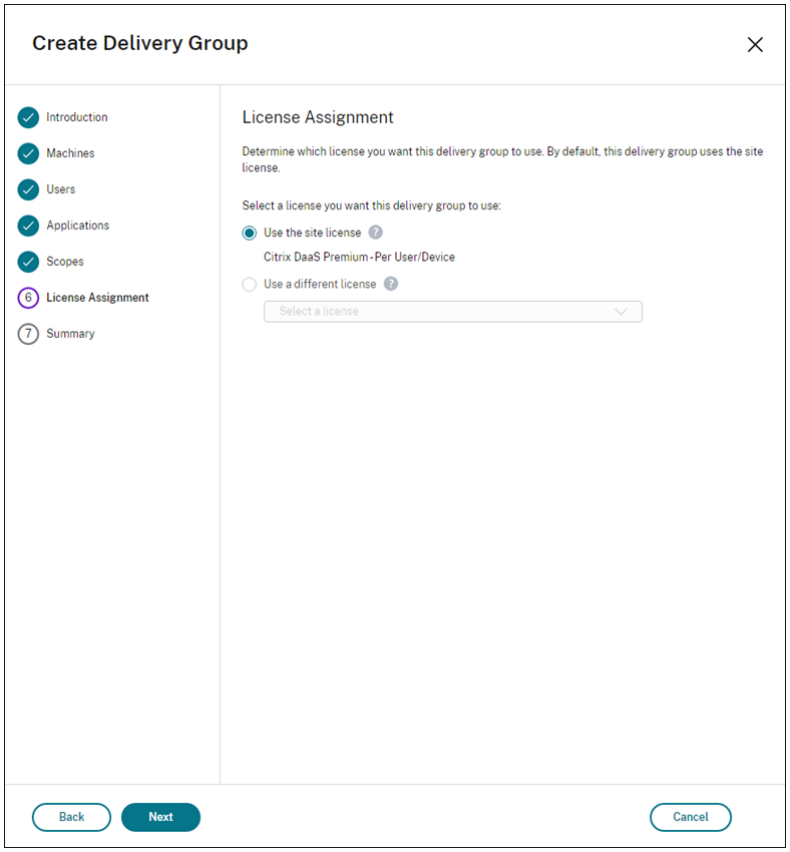
As possíveis licenças disponíveis para você selecionar são as seguintes:

- Citrix DaaS Premium —Por usuário/dispositivo
- Citrix DaaS Premium —Simultâneo
- Citrix DaaS Premium para Google Cloud —Por usuário/dispositivo
- Citrix DaaS Premium para Google Cloud —Simultâneo
- Citrix DaaS Advanced —Por usuário/dispositivo
- Citrix DaaS Advanced —Simultâneo
- Citrix DaaS Advanced Plus —Por usuário/dispositivo
- Citrix DaaS Advanced Plus —Simultâneo
- Citrix DaaS Standard for Azure –Por usuário/dispositivo
- Citrix DaaS Standard for Azure –Simultâneo
- Citrix DaaS Standard para Google Cloud —Por usuário/dispositivo
- Citrix DaaS Standard para Google Cloud —Simultâneo

Se você tiver uma licença expirada, entre em contato com o representante de vendas da Citrix para renová-la ou comprar novas licenças.

Exibir e atualizar um direito de nível de grupo de entrega

Você pode especificar qual licença deseja que um grupo de entrega use ao criar ou editar um grupo de entrega. Na página **License Assignment**, selecione uma opção.



Opções:

- **Use the site license**. Uma licença de site se aplica a todos os grupos de entrega, exceto àqueles grupos de entrega configurados com uma licença diferente. A licença que aparece sob essa opção é a licença do site em uso. Para configurar a licença do site, vá para **Manage > Full Configuration**, selecione o nó **Settings** e edite **Assign license**.
- **Use a different license**. Essa opção permite configurar esse grupo de entrega para usar uma licença diferente da licença do site. Lembre-se de que um direito de licença é uma combinação de código de produto, edição e modelo de licença. O grupo de entrega deve usar a mesma edição de licença (Standard, Premium ou Advanced) do site. Se configurado, o grupo de entrega consumirá somente a licença selecionada. Mesmo quando a licença selecionada é totalmente consumida ou se torna inválida, o grupo de entrega não recai para a licença do site.

Por padrão, o grupo de entrega usa a licença do site.

Quando uma licença de grupo de entrega expirar e não for mais válida, use uma licença diferente.

> **Nota:**
>
> Se posteriormente você configurar um grupo de entrega para usar uma licença diferente, os usuários conectados consumindo a licença atual poderão perder temporariamente o acesso a suas áreas de trabalho e aplicativos.

Um exemplo de mistura de direitos

Por exemplo, considere que o Cliente A comprou inicialmente a edição Advanced e depois comprou a edição Advanced Plus. Nesse caso, o Cliente A continua a ter uma licença para todo o site apenas da edição Advanced. A Citrix não modifica a configuração inicialmente definida no nível do site pelo Cliente A. É responsabilidade do Cliente A modificar a edição da licença para Advanced Plus no nível do site.

Da mesma forma, o Cliente A também pode atualizar a edição da licença para Advanced Plus no grupo de entrega. Se essa configuração não for configurada, o grupo de entrega herdará a edição de licença definida no nível do site.

O administrador do Cliente A pode atualizar a edição da licença usando as seguintes formas:

- Atualizar a edição da licença em nível de site –vá para **Manage > Full Configuration**, selecione o nó **Settings** e edite **Assign license**.
- Atualizar a edição da licença em nível de grupo de entrega –vá para **Manage > Full Configuration** e selecione o nó **Delivery groups**. Edite o grupo de entrega de destino para fazer as alterações.

Atualizar o grupo de entrega usando o comando do PowerShell

O comando do PowerShell para atualizar o grupo de entrega é o seguinte:

```
Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
    code> -LicenseModel <The type of license model>
<!--NeedCopy-->
```

Atualize o comando anterior, com base nos seus detalhes.

Por exemplo, veja o seguinte:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (Defina a configuração no nível do grupo de entrega com a configuração definida no nível do site)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Considere que o modelo de licença e o código de produto não estão definidos no nível do grupo de entrega. Nesse cenário, essas duas propriedades definidas no nível do site são usadas para o grupo de entrega.

Para obter mais informações sobre o Citrix DaaS Remote PowerShell SDK, consulte a documentação de SDKs e APIs.

Mais informações

- Licenças
- Criar grupos de entrega
- Gerenciar grupos de entrega

Balanceamento da carga das máquinas

December 6, 2023

> **Nota:**
>
> Esse recurso se aplica a todos os seus catálogos —catálogos de SO de sessão única ou SO multissessão. O balanceamento de carga vertical se aplica somente a máquinas com SO multissessão.

O balanceamento de carga pode ser configurado no nível do site e no nível do grupo de entrega. Você tem duas opções: vertical e horizontal. Por padrão, o balanceamento de carga horizontal está habilitado.

Configurações de balanceamento de carga no nível do site

- **Balanceamento de carga vertical**. Atribui uma sessão de usuário de entrada à máquina mais carregada que ainda não atingiu a carga máxima. Isso satura as máquinas existentes antes de passar para as novas máquinas. Os usuários que se desconectam das máquinas existentes liberam a capacidade nessas máquinas. As cargas de entrada são então atribuídas a essas máquinas. O balanceamento de carga vertical degrada a experiência do usuário, mas reduz os custos (as sessões maximizam a capacidade de energia da máquina ligada).

Exemplo: 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.

> **Dica:**
>
> Para especificar o número máximo de sessões que uma máquina pode hospedar, use a configuração de política Maximum number of sessions.

Como alternativa, 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.

- **Balanceamento de carga horizontal**. Atribui uma sessão de usuário de entrada à máquina ligada menos carregada e disponível. O balanceamento de carga horizontal melhora a experiência do usuário, mas aumenta os custos (porque mais máquinas são mantidas ligadas). Por padrão, o balanceamento de carga horizontal está habilitado.

  Exemplo: você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com cinco sessões simultâneas. A segunda máquina também lida com cinco.

Para configurar esse recurso, em **Manage > Full Configuration**, selecione **Settings** no painel esquerdo. Selecione uma opção em **Load balance multi-session catalogs**.

Configurações de balanceamento de carga no nível do grupo de entrega

A configuração do balanceamento de carga no nível do grupo de entrega permite que você substitua as configurações de balanceamento de carga herdadas do nível do site. Você pode atingir a utilização máxima de cada máquina ao selecionar o balanceamento de carga vertical no nível do grupo de entrega. Isso ajudará a reduzir custos com nuvens públicas. Essa configuração pode ser feita durante a criação de um novo grupo de entrega ou na edição de um grupo de entrega existente.

Balanceamento de carga horizontal. As sessões são distribuídas entre máquinas ligadas. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina manipulará cinco sessões simultâneas e a segunda também manipulará cinco.

Balanceamento de carga vertical. As sessões maximizam a capacidade da máquina ligada e economizam custos com a máquina. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina manipulará as primeiras 10 sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

Cache do host local

November 21, 2023

> **Dica:**
>
> Em **Full Configuration > Home**, o recurso de alertas de integridade do serviço fornece alertas proativos para garantir que o seu cache do host local e as zonas estejam configurados corretamente. Assim, quando ocorre uma interrupção, o cache do host local funciona e seus usuários não são afetados. Os alertas vêm em dois níveis: alertas de todo o site mostrados na página Home (ícone de bandeira) e alertas relacionados à zona exibidos na guia Troubleshoot de cada zona. Para obter mais informações, consulte Zonas.

O Cache do host local permite que as operações de intermediação de conexão em uma implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) continuem quando um Cloud Connector não pode se comunicar com o Citrix Cloud. O Cache de host local é ativado quando a conexão de rede é perdida por 60 segundos.

Com o Cache de host local, os usuários que estão conectados quando ocorre uma interrupção podem continuar trabalhando sem interrupções. Reconexões e novas conexões sofrem atrasos mínimos de conexão.

> **Importante:**
>
> Se estiver usando uma implantação local do StoreFront, você deve adicionar todos os Cloud Connectors que tenham (ou possam ter) VDAs registrados com eles ao StoreFront como Delivery Controllers. Um Cloud Connector que não é adicionado ao StoreFront não pode fazer a transição para o modo de interrupção, o que pode resultar em falhas de inicialização do usuário.
>
> Para implantações sem o StoreFront local, use o recurso da plataforma do Citrix Workspace de continuidade de serviço para permitir que os usuários se conectem a recursos durante interrupções. Para obter mais informações, consulte Continuidade do serviço.

Conteúdo de dados

O Cache de host local inclui as seguintes informações, que são um subconjunto das informações no banco de dados principal:

- Identidades de usuários e grupos que têm direitos aos recursos publicados no site.
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados no site.
- Identidades de máquinas VDA (incluindo máquinas Remote PC Access) configuradas no site.

- Identidades (nomes e endereços IP) de máquinas cliente do aplicativo Citrix Workspace que estão sendo usadas ativamente para a conexão a recursos publicados.

Ele também contém informações para conexões atualmente ativas que foram estabelecidas enquanto o banco de dados principal estava indisponível:

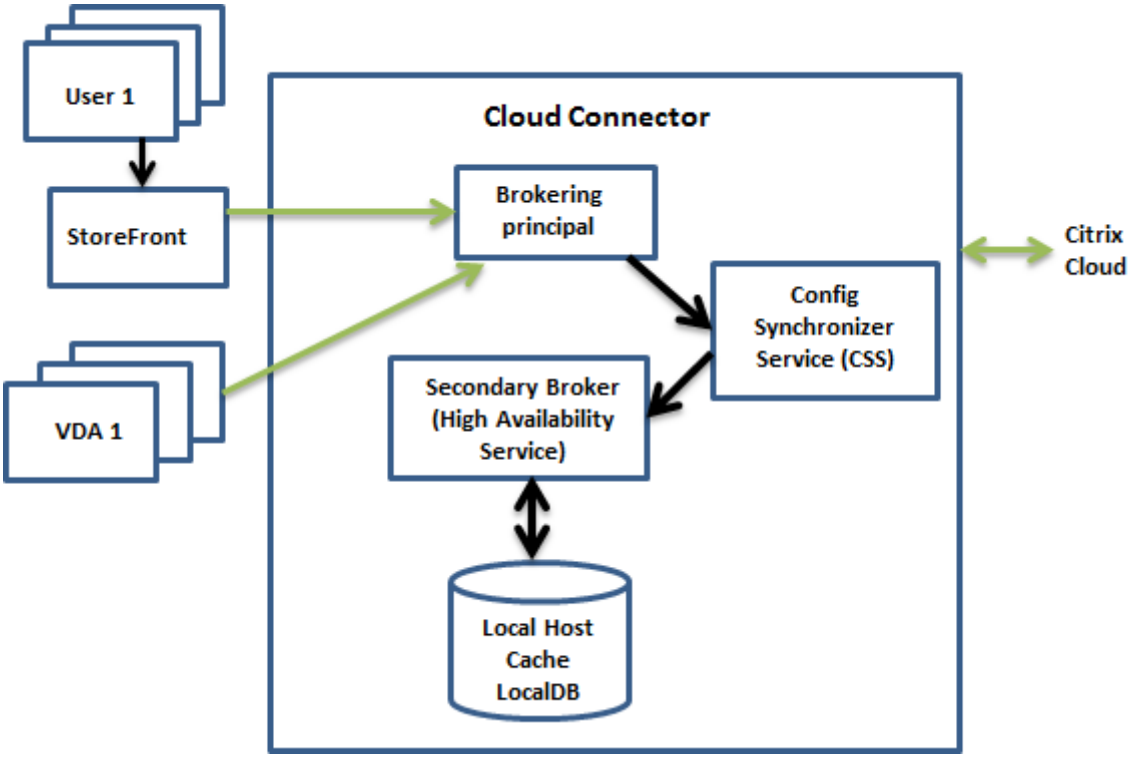
- Resultados análises de ponto de extremidade de máquina cliente realizadas pelo aplicativo Citrix Workspace.
- Identidades de máquinas de infraestrutura (como servidores Citrix Gateway e StoreFront) envolvidas em operações do site.
- Data, hora e tipo das atividades recentes dos usuários.

Como funciona

Veja como o Cache do host local interage com o Citrix Cloud.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

Durante as operações normais



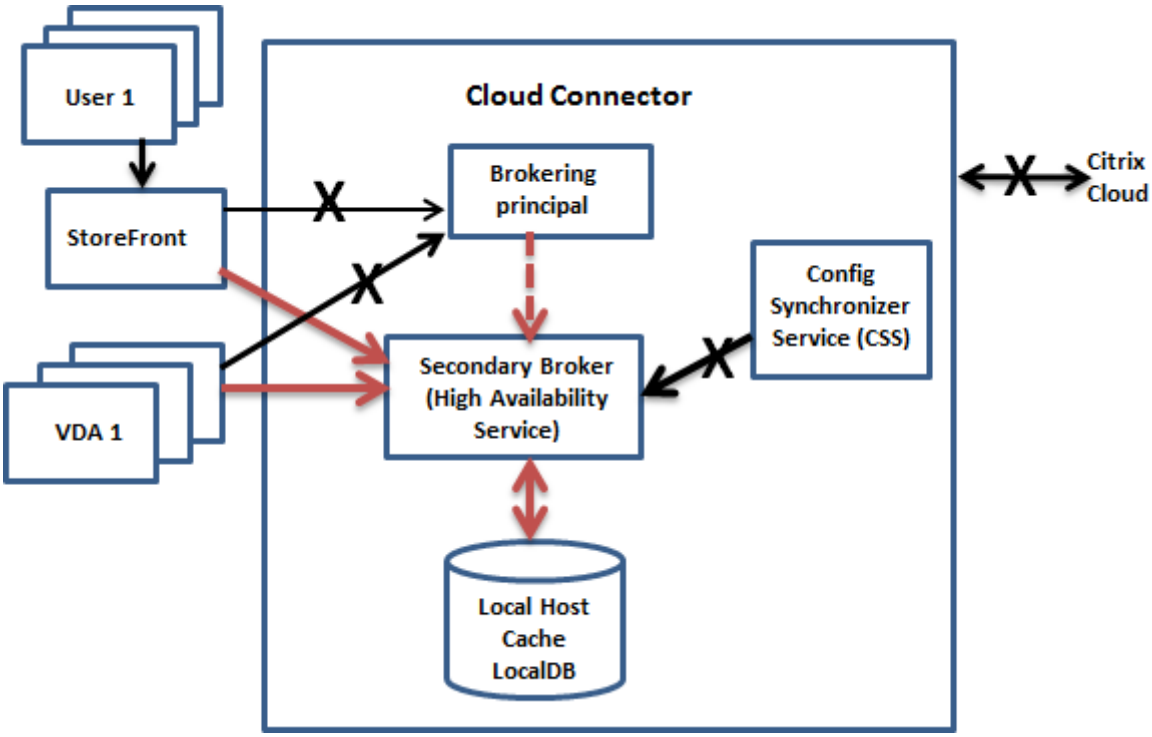
- O Brokering Principal (também conhecido como Citrix Remote Broker Provider Service) em um Cloud Connector aceita solicitações de conexão do StoreFront. O Brokering Principal se comunica com o Citrix Cloud para conectar usuários com VDAs registrados no Cloud Connector.

- O Citrix Config Synchronizer Service (CSS) consulta o agente no Citrix Cloud a cada 5 minutos, aproximadamente, para ver se foi feita alguma alteração na configuração. As alterações podem ser iniciadas pelo administrador (como alterar uma propriedade de grupo de entrega) ou podem ser ações do sistema (como atribuições de máquina).
- Se uma alteração de configuração tiver ocorrido desde a verificação anterior, o CSS sincroniza (copia) as informações com um agente secundário no Cloud Connector. (O agente secundário também é conhecido como Serviço de Alta Disponibilidade, corretor de HA ou agente de HA, conforme mostra a figura anterior.)

  Todos os dados de configuração são copiados, não apenas os itens que foram alterados desde a verificação anterior. O CSS importa os dados de configuração para um banco de dados do Microsoft SQL Server Express LocalDB no Cloud Connector. Esse banco de dados é referido como o banco de dados do cache de host local. O CSS garante que as informações no banco de dados do Cache de host local correspondam às informações no banco de dados do site no Citrix Cloud. O banco de dados do cache de host local é recriado toda vez que a sincronização ocorre.

  O Microsoft SQL Server Express LocalDB (usado pelo banco de dados do Cache de host local) é instalado automaticamente quando você instala um Cloud Connector. O banco de dados do Cache de host local não pode ser compartilhado entre os Cloud Connectors. Você não precisa fazer backup do banco de dados do cache de host local. 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.

Durante uma interrupção



Quando uma interrupção começa:

- O agente secundário começa a escutar e processar as solicitações de conexão.
- Quando a interrupção começa, o agente secundário não tem dados de registro do VDA atuais, mas quando o VDA se comunica com ele, um processo de registro é disparado. Durante esse processo, o agente secundário também obtém as informações de sessão atuais sobre o VDA.
- Enquanto o agente secundário está lidando com as conexões, o Brokering Principal continua a monitorar a conexão ao Citrix Cloud. Quando a conexão é restaurada, o Brokering Principal instrui o agente secundário a parar de escutar informações de conexão, e o Brokering Principal retoma as operações de intermediação. A próxima vez que um VDA se comunicar com o Brokering Principal, um processo de registro é disparado. O agente secundário remove quaisquer registros de VDA restantes da interrupção anterior. O CSS retoma a sincronização de informações quando detecta que ocorreram alterações de configuração no Citrix Cloud.

No caso improvável de uma interrupção começar durante uma sincronização, a importação atual é descartada e a última configuração conhecida é usada.

O log do evento indica quando ocorrem sincronizações e interrupções.

Não há limite de tempo imposto para operar no modo de interrupção.

Você também pode disparar uma interrupção intencionalmente. Consulte Forçar uma interrupção para obter detalhes sobre por que e como fazer isso.

Locais de recursos com vários Cloud Connectors

Entre suas outras tarefas, o CSS fornece rotineiramente ao agente secundário informações sobre todos os Cloud Connectors no local do recurso. Com essas informações, cada agente secundário sabe sobre todos os agentes secundários de mesmo nível em execução em outros Cloud Connectors no local do recurso.

Os agentes secundários comunicam-se uns com os outros em um canal separado. Esses agentes usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual agente secundário intermediará as operações na zona se ocorrer uma interrupção. Durante a interrupção, todos os VDAs se registram novamente no agente secundário eleito. Os agentes secundários não eleitos na zona rejeitam ativamente as solicitações de entrada de conexão e registro de VDA.

Se um agente secundário eleito falhar durante uma interrupção, outro agente secundário é eleito para assumir o controle, e os VDAs se registram no agente secundário recém-eleito.

Durante uma interrupção, se um Cloud Connector for reiniciado:

- Se esse Cloud Connector não for o agente eleito, a reinicialização não terá impacto.
- Se esse Cloud Connector for o agente eleito, um Cloud Connector diferente será escolhido, fazendo com que os VDAs se registrem. Depois que o Cloud Connector reiniciado liga, ele assume automaticamente a intermediação, o que faz com que os VDAs se registrem novamente. Nesse cenário, o desempenho pode ser afetado durante os registros.

O log do evento fornece informações sobre as escolhas.

O que não está disponível durante uma interrupção e outras diferenças

Não há limite de tempo imposto para operar no modo de interrupção. No entanto, se a interrupção ocorrer devido à perda da conectividade do Citrix Cloud do local do recurso, a Citrix recomenda restaurar a conectividade do local do recurso o mais rápido possível.

Durante uma interrupção:

- Você não pode usar as interfaces **Manage**.
- Você tem acesso limitado ao Remote PowerShell SDK.
  - Você deve primeiro:
    * Adicionar uma chave de registro `EnableCssTestMode` com um valor de 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Definir a autenticação do SDK como `OnPrem` para que o proxy do SDK não tente redirecionar as chamadas do cmdlet: `$XDSDKAuth="OnPrem"`

    * Usar a porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - Depois de executar esses comandos, você pode acessar:
    * Todos os cmdlets `Get-Broker*`.

- Os dados de monitoramento não são enviados para o Citrix Cloud durante uma interrupção. Portanto, as funções **Monitor** não mostram a atividade de um intervalo de interrupção.
- As credenciais do Hypervisor não podem ser obtidas do Host Service. Todas as máquinas estão em um estado de energia desconhecido e nenhuma operação de energia pode ser emitida. No entanto, as VMs no host que estão ligadas podem ser usadas para solicitações de conexão.
- Uma máquina atribuída só pode ser usada se a atribuição ocorreu durante as operações normais. Novas atribuições não podem ser feitas durante uma interrupção.
- O registro e a configuração automática de máquinas Remote PC Access não são possíveis. No entanto, as máquinas que foram registradas e configuradas durante a operação normal são utilizáveis.
- Aplicativos hospedados no servidor e usuários de área de trabalho podem usar mais sessões do que seus limites de sessão configurados, se os recursos estiverem em zonas diferentes.
- Os usuários podem iniciar aplicativos e áreas de trabalho somente a partir de VDAs registrados na zona que contém o agente eleito/ativo atualmente. As inicializações entre zonas (de um agente em uma zona para um VDA em uma zona diferente) não são suportadas durante uma interrupção.
- Se uma interrupção do banco de dados do site ocorrer antes de uma reinicialização programada começar para os VDAs em um grupo de entrega, as reinicializações começam quando a interrupção termina. Esse cenário pode ter resultados inesperados. Para obter mais informações, consulte Reinicializações agendadas atrasadas devido à interrupção do banco de dados.
- A preferência de zona não pode ser configurada. Se configuradas, as preferências não serão consideradas na inicialização da sessão.
- As restrições de marcas, em que as marcas são usadas para designar locais de recursos, não são suportadas no início de sessão. Quando tais restrições de marca são configuradas e a opção advanced health check de uma loja do StoreFront está habilitada, as sessões podem falhar intermitentemente na inicialização.

Requisito do StoreFront

Se estiver usando uma implantação local do StoreFront, você deve adicionar todos os Cloud Connectors que tenham (ou possam ter) VDAs registrados com eles ao StoreFront como Delivery Controllers.

Um Cloud Connector que não é adicionado ao StoreFront não pode fazer a transição para o modo de interrupção, o que pode resultar em falhas de inicialização do usuário.

Disponibilidade de recursos

Você pode garantir a disponibilidade de recursos (aplicativos e áreas de trabalho) durante uma interrupção de duas maneiras:

- Publique os recursos em cada local de recurso em sua implantação.
- Se você estiver usando o StoreFront 1912 CU4 ou posterior, publique os recursos em pelo menos um local de recursos e ative a verificação avançada de integridade em todos os servidores StoreFront. Nas versões anteriores ao StoreFront 2308, a verificação avançada de integridade está desativada por padrão e deve ser ativada por um administrador. No StoreFront versão 2308 e posteriores, esse recurso está ativado por padrão. Para obter mais informações e instruções sobre como ativar a verificação avançada de integridade, consulte Verificação avançada de integridade.

Suporte a aplicativos e áreas de trabalho

O cache de host local oferece suporte a aplicativos e áreas de trabalho hospedados em servidor e a áreas de trabalho estáticas (atribuídas).

O cache de host local oferece suporte a VDAs de área de trabalho (sessão única) em grupos de entrega em pool, como se segue.

- Por padrão, os VDAs de área de trabalho com gerenciamento de energia em grupos de entrega em pool (criados pelo MCS ou Citrix Provisioning) que têm a propriedade `ShutdownDesktopsAfterUse` ativada não estão disponíveis para novas conexões durante um evento de cache de host local. Você pode alterar esse padrão para permitir que essas áreas de trabalho sejam usadas durante o cache do host local.

  No entanto, você não pode contar necessariamente com o gerenciamento de energia durante a interrupção. (O gerenciamento de energia é retomado depois das operações normais serem retomadas.) Além disso, essas áreas de trabalho podem conter dados do usuário anterior, porque não foram reiniciadas.

- Para substituir o comportamento padrão, ele deve ser ativado em todo o site e em cada grupo de entrega afetado usando os comandos do PowerShell.

  Para todo o site, execute o seguinte comando:

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```


Por padrão, nenhum dos grupos de entrega está habilitado para esse recurso. Há duas opções para ativá-los no nível do grupo de entrega:

- **Habilitar para os grupos de entrega selecionados:** para cada grupo de entrega afetado, execute o seguinte comando.

  ```
  Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOuta
   $true
  ```

- **Habilitar para todos os grupos de entrega:** para habilitar a configuração do nível do grupo de entrega por padrão, execute o seguinte comando. Essa configuração se aplica a todos os grupos de entrega recém-criados (ou seja, todos os grupos de entrega criados após habilitar a configuração).

  ```
  Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage
  $true
  ```

  Para habilitar isso para grupos de entrega existentes, execute o comando observado anteriormente (`Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdow $true`).

Ativar esse recurso no site e nos grupos de entrega não afeta como a propriedade configurada `ShutdownDesktopsAfterUse` funciona durante as operações normais.

> **Importante:**
>
> Sem ativar ReuseMachinesWithoutShutdownInOutageAllowed no nível de Site e ReuseMachinesWithoutShutdownInOutage no nível do grupo de entrega, todas as tentativas de inicialização de sessão de VDAs de área de trabalho com gerenciamento de energia em grupos de entrega em pool falharão durante um evento de cache de host local.

Verificar se o Cache de Host Local está funcionando

Veja como verificar se o Cache do Host Local está configurado corretamente.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

Para verificar se o Cache de Host Local está configurado e funcionando corretamente:

- Se estiver usando o StoreFront, verifique se a implantação local do StoreFront aponta para todos os Cloud Connectors nesse local de recursos.
- Certifique-se de que as importações de sincronização sejam concluídas com êxito. Verifique os logs de eventos.
- Certifique-se de que o banco de dados de 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`.
  - Confirme que `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.

- Force uma interrupção em todos os Cloud Connectors no local do recurso. Depois de verificar se o Cache de Host Local funciona, lembre-se de colocar todos os Cloud Connectors de volta no modo normal. Isso pode levar aproximadamente 15 minutos.

Logs de eventos

Os logs de eventos indicam quando ocorrem sincronizações e interrupções. Nos logs do visualizador do evento, o modo da interrupção é referido como *HA mode*.

Config Synchronizer Service

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados do Cache de Host Local usando o agente de cache de host local.

- 503: o Citrix Config Sync Service recebeu uma configuração atualizada. Esse evento ocorre sempre que uma configuração atualizada é recebida do Citrix Cloud. Ele indica o início do processo de sincronização.
- 504: o Citrix Config Sync Service importou uma configuração atualizada. A importação da configuração foi concluída com sucesso.
- 505: o Citrix Config Sync Service falhou na importação. A importação da configuração não foi concluída com sucesso. Se uma configuração anteriormente bem-sucedida estiver disponível, ela será usada se ocorrer uma interrupção. No entanto, ela não estará atualizada com a configuração atual. Se não houver nenhuma configuração anterior disponível, o serviço não poderá participar da intermediação de sessão durante uma interrupção. Nesse caso, consulte a seção de Resolução de problemas e entre em contato com o Suporte Citrix.
- 507: o Citrix Config Sync Service abandonou uma importação porque o sistema está no modo de interrupção e o agente de cache de host local está sendo usado para a intermediação. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque ocorreu uma interrupção. Esse é o comportamento esperado.
- 510: não há dados de configuração do Configuration Service recebidos do Configuration Service principal.
- 517: houve um problema de comunicação com o agente primário.
- 518: script Config Sync anulado porque o agente secundário (High Availability Service) não está em execução.

High Availability Service

Este serviço também é conhecido como agente de cache de host local.

- 3502: ocorreu uma interrupção e o agente de cache de host local está executando operações do agente.
- 3503: uma interrupção foi resolvida e as operações normais foram retomadas.
- 3504: indica qual agente de Cache de Host Local é eleito, além de outros agentes de Cache de Host Local envolvidos na eleição.
- 3507: fornece uma atualização de status do Cache de Host Local a cada 2 minutos, o que indica que o modo Cache de Host Local está ativo no agente eleito. Contém um resumo da interrupção, incluindo a duração da interrupção, o registro do VDA e as informações da sessão.
- 3508: anuncia que o Cache do Host Local não está mais ativo no agente escolhido e que as operações normais foram restauradas. Contém um resumo da interrupção, incluindo a duração da interrupção, o número de máquinas registradas durante o evento do Cache do Host Local e o número de lançamentos bem-sucedidos durante o evento do LHC.
- 3509: notifica que o Cache do Host Local está ativo no(s) agente(s) não eleito(s). Contém uma duração de interrupção a cada 2 minutos e indica o agente eleito.
- 3510: anuncia que o Cache do Host Local não está mais ativo no(s) agente(s) não eleito(s). Contém a duração da interrupção e indica o agente eleito.

Forçar uma interrupção

Você pode, deliberadamente, forçar uma interrupção.

- Se a operação da sua rede é interrompida repetidamente. Forçar uma interrupção até que os problemas de rede sejam resolvidos evita a transição contínua entre os modos normal e de interrupção (e as tempestades de registros de VDA frequentes resultantes).
- Para testar um plano de recuperação de desastres.
- Para ajudar a garantir que o Cache de Host Local está funcionando corretamente.

Embora um Cloud Connector possa ser atualizado durante uma interrupção forçada, problemas imprevistos podem ocorrer. Recomendamos que você defina uma programação para atualizações do Cloud Connector que evite intervalos de modo de interrupção forçada.

Para forçar uma interrupção, edite o registro de cada servidor do Cloud Connector. Em `HKLM\Software\Citrix\DesktopServer\LHC`, crie e defina `OutageModeForced` como `REG_DWORD` para 1. Essa configuração instrui o agente de cache do host local a entrar no modo de interrupção, independentemente do estado da conexão com o Citrix Cloud. Definir o valor para `0` retira o agente de Cache de Host Local do modo de interrupção.

Para verificar eventos, monitore o arquivo de log `Current_HighAvailabilityService` em `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`.

Solução de problemas

Várias ferramentas de solução de problemas estão disponíveis quando uma importação de sincronização para o banco de dados do Cache de Host Local falha e um evento 505 é publicado.

CDF tracing: contém opções para os módulos ConfigSyncServer e BrokerLHC. Essas opções, juntamente com outros módulos de agentes, podem identificar o problema.

Report: se uma importação de sincronização falhar, você pode gerar um relatório. Esse relatório para no objeto que está causando o erro. Esse recurso de relatório afeta a velocidade de sincronização, portanto, a Citrix recomenda desativá-lo quando não estiver em uso.

Para ativar e produzir um relatório de rastreamento CSS, insira o seguinte comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

O relatório HTML é publicado em: `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`

Depois que o relatório for gerado, insira o seguinte comando para desativar o recurso de relatório:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Comandos do PowerShell de Cache de host local

Você pode gerenciar o cache de host local em seus Cloud Connectors usando comandos do PowerShell.

O módulo PowerShell está localizado no seguinte local nos Cloud Connectors:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Importante:**
>
> Execute esse módulo somente nos Cloud Connectors.

Importar módulo PowerShell Para importar o módulo, execute o seguinte no seu Cloud Connector:

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```


Comandos do PowerShell para gerenciar o LHC Os cmdlets a seguir ajudam você a ativar e gerenciar o modo LHC nos Cloud Connectors.

Cmdlets	Função
`Enable-LhcForcedOutageMode`	Colocar o Broker no modo LHC. Os arquivos do banco de dados do Cache de host local devem ter sido criados com sucesso pelo ConfigSync Service para `Enable-LhcForcedOutageMode` funcionar corretamente. Esse cmdlet só força o LHC no Cloud Connector em que ele foi executado. Para que o LHC se torne ativo, esse cmdlet deve ser executado em todos os Cloud Connectors no local de recursos.
`Disable-LhcForcedOutageMode`	Retira o Broker do modo LHC. Esse cmdlet desativa somente o modo LHC no Cloud Connector em que foi executado. `Disable-LhcForcedOutageMode` deve ser executado em todos os Cloud Connectors dentro do local de recursos.
`Set-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o Citrix Config Synchronizer Service (CSS) verifica as 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 só se aplica ao Cloud Connector no qual ela foi executada. Para obter consistência em todos os Cloud Connectors, considere executar esse cmdlet em cada Cloud Connector. Por exemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`

Cmdlets	Função
`Clear-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o Citrix Config Synchronizer Service (CSS) verifica as alterações de configuração no site do Citrix DaaS para o valor padrão de 300 segundos (cinco minutos). Essa configuração só se aplica ao Cloud Connector no qual ela foi executada. Para obter consistência em todos os Cloud Connectors, considere executar esse cmdlet em cada Cloud Connector.
`Enable-LhcHighAvailabilitySDK`	Permite o acesso a todo o cmdlet `Get-Broker*` no Cloud Connector em que ele foi executado.
`Disable-LhcHighAvailabilitySDK`	Desativa o acesso aos comandos do Broker PowerShell no Cloud Connector em que ele 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 LHC Broker no Cloud Connector só contém informações de configuração.
- Durante o modo LHC, o LHC Broker no Cloud Connector selecionado contém as seguintes informações:
  - Estados de recursos
  - Detalhes da sessão
  - Registros de VDA
  - Informações de configuração

Mais informações

Consulte Considerações de escala e tamanho para o cache do host local para obter informações sobre:

- Metodologias de teste e resultados
- Considerações sobre o tamanho da RAM
- Considerações de configuração do núcleo e do soquete da CPU

- Considerações sobre armazenamento

Gerenciar chaves de segurança

April 14, 2023

> **Nota:**
>
> - Você deve usar este recurso em combinação com o StoreFront 1912 LTSR CU2 ou posterior.
> - O recurso Secure XML é suportado apenas no Citrix ADC e no Citrix Gateway versão 12.1 ou superior.

Este recurso permite que você autorize apenas máquinas StoreFront e Citrix Gateway aprovadas para se comunicarem com Citrix Delivery Controllers. Depois que você habilitar esse recurso, todas as solicitações que não contenham a chave serão bloqueadas. Use esse recurso para adicionar uma camada extra de segurança para se proteger contra ataques originados na rede interna.

Eis aqui um fluxo de trabalho geral para usar esse recurso:

1. Exiba as configurações da chave de segurança na interface Full Configuration. (Use o SDK do PowerShell remoto)
2. Defina as configurações para sua implantação. (Use a interface Full Configuration ou o SDK do PowerShell remoto.)
3. Defina as configurações no StoreFront. (Use o PowerShell.)
4. Defina as configurações no Citrix ADC.

Exibir as configurações da chave de segurança na interface Full Configuration

Por padrão, as configurações das chaves de segurança estão ocultas na interface Full Configuration. Para exibi-las nessa interface, use o Remote PowerShell SDK. Para obter mais informações sobre o Remote PowerShell SDK, consulte SDKs e APIs.

As etapas detalhadas são as seguintes:

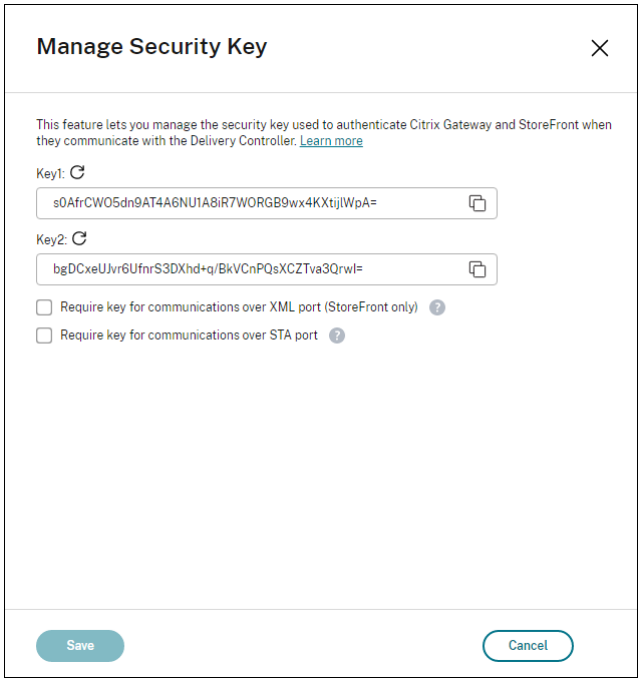
1. Execute o SDK do PowerShell remoto.
2. Em uma janela de comando, execute os seguintes comandos:
   - `Add-PSSnapIn Citrix*`. Esse comando adiciona os snap-ins da Citrix.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

Definir as configurações para sua implantação

Você pode definir as configurações para a sua implantação usando Full Configuration ou PowerShell.

Usar a interface Full Configuration

Depois de ativar o recurso, navegue até **Full Configuration > Settings > Manage security key** e clique em **Edit**. A folha **Manage Security Key** é exibida. Clique em **Save** para aplicar as alterações e sair da folha.



> **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 de cada vez. A chave não utilizada é usada apenas para a rotação de chaves.
> - Não clique no ícone de atualização para atualizar a chave já em uso. Se você fizer isso, ocorrerá a interrupção do serviço.

Clique no ícone de atualização para gerar novas chaves.

Require key for communications over XML port (StoreFront only). Se selecionada, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por essa porta. Para obter informações sobre como alterar a porta XML, consulte o artigo do Knowledge Center CTX127945.

Require key for communications over STA port. Se selecionada, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por essa porta. Para obter informações sobre como alterar a porta STA, consulte o artigo do Knowledge Center CTX101988.

Depois de aplicar suas alterações, clique em **Close** para sair da folha **Manage Security Key**.

Usar o Remote PowerShell SDK

A seguir estão as etapas do PowerShell equivalentes às operações executadas na interface Full Configuration.

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 Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Execute os seguintes comandos para gerar uma chave e configurar Key2:
   - `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 do PowerShell para obter orientação e sintaxe.

Definir configurações no StoreFront

Depois de concluir as configurações da sua implantação, você precisa definir as configurações relevantes no StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos do PowerShell:

- Para configurar a chave para comunicações pela porta XML, use os comandos `Get-STFStoreServie` e `Set-STFStoreService`. Por exemplo:

  ```
  PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>
  ```

- Para configurar a chave para comunicações pela porta STA, use o comando `New-STFSecureTicketAuth` . Por exemplo:

  ```
  PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL> -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>
  ```

Consulte a ajuda do comando do PowerShell para obter orientação e sintaxe.

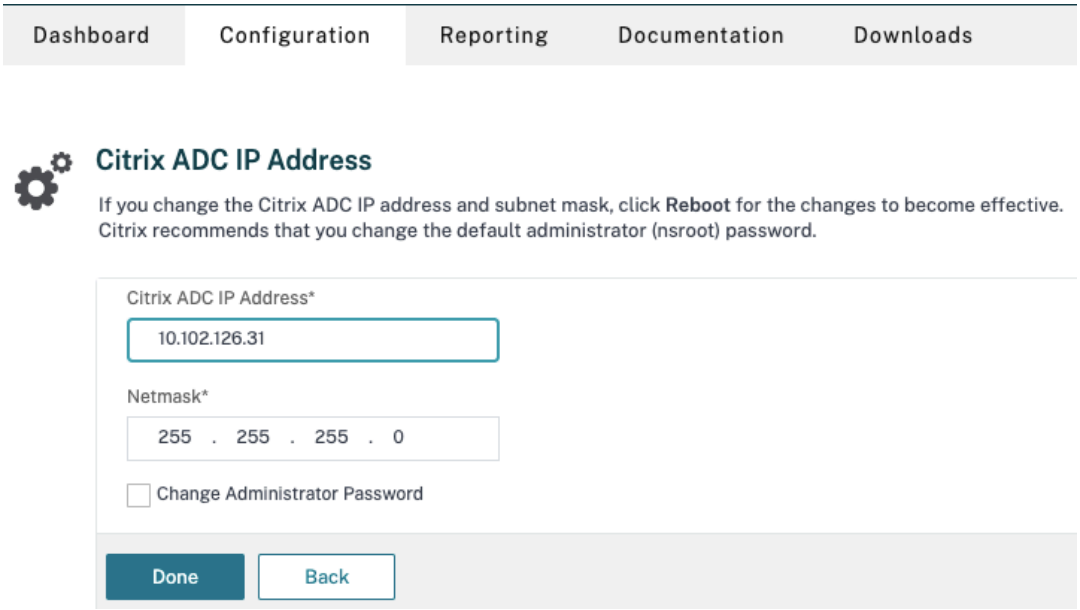
Definir configurações no Citrix ADC

> **Nota:**
>
> A configuração desse recurso no Citrix ADC não é necessária, a menos que você use o Citrix ADC como gateway. Se você usa o Citrix ADC, siga as etapas abaixo.

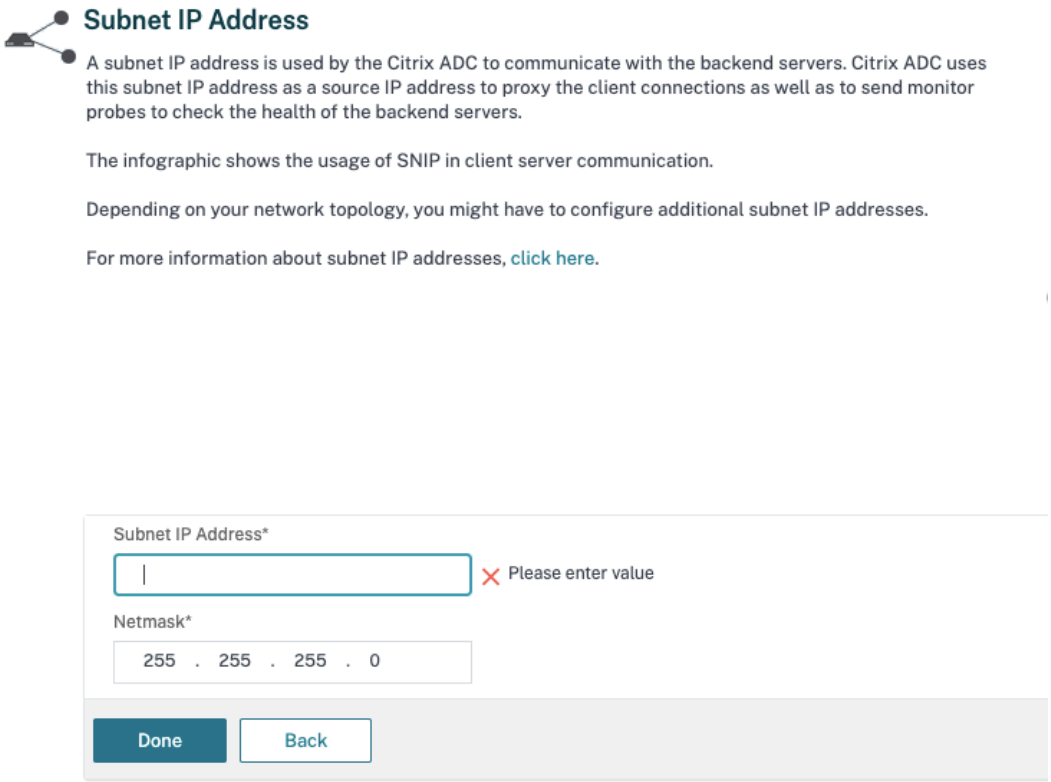
1. Verifique se a seguinte configuração de pré-requisito já está em vigor:

   - Os seguintes endereços IP relacionados ao Citrix ADC são configurados.

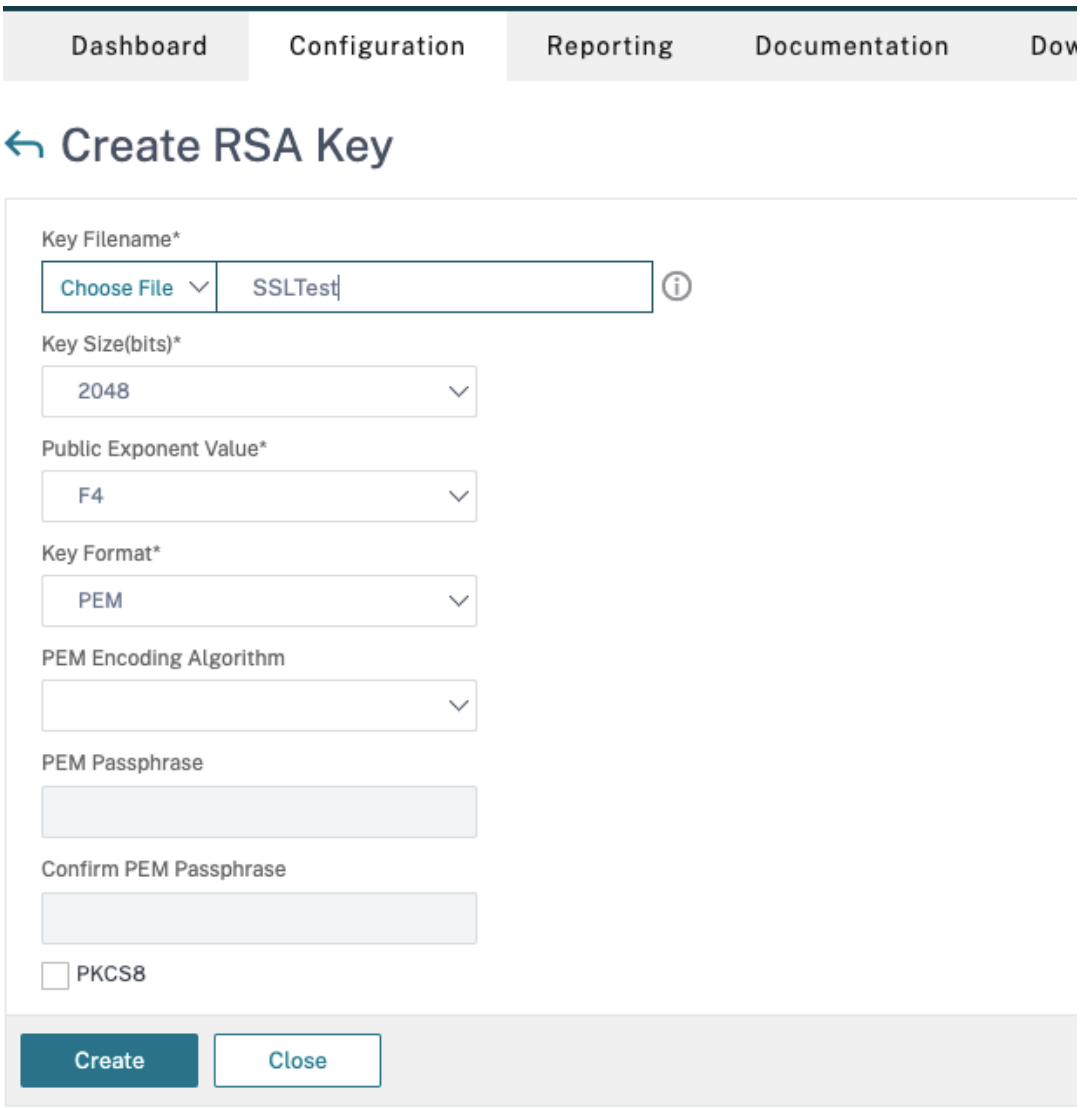
     – Endereço IP de gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



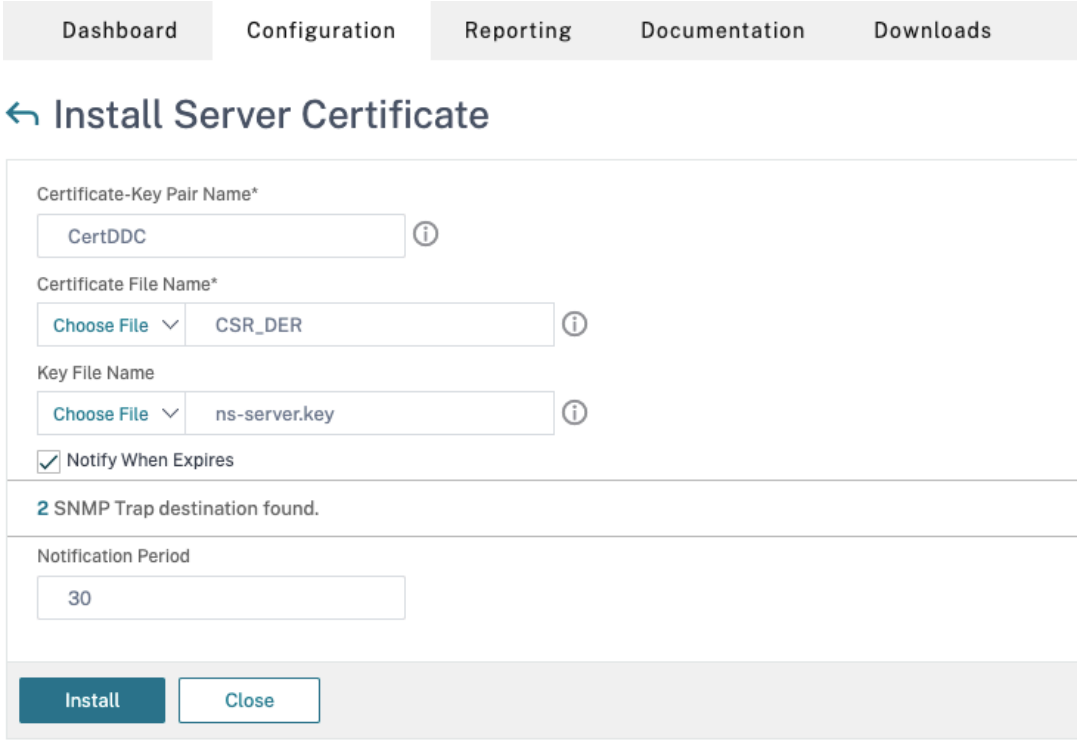
  - Endereço IP de sub-rede (SNIP) para permitir a comunicação entre o appliance Citrix ADC e os servidores back-end. Para obter detalhes, consulte Configuração de endereços IP de sub-rede.
  - Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no appliance ADC para iniciar a sessão. Para obter detalhes, consulte Criar um servidor virtual.

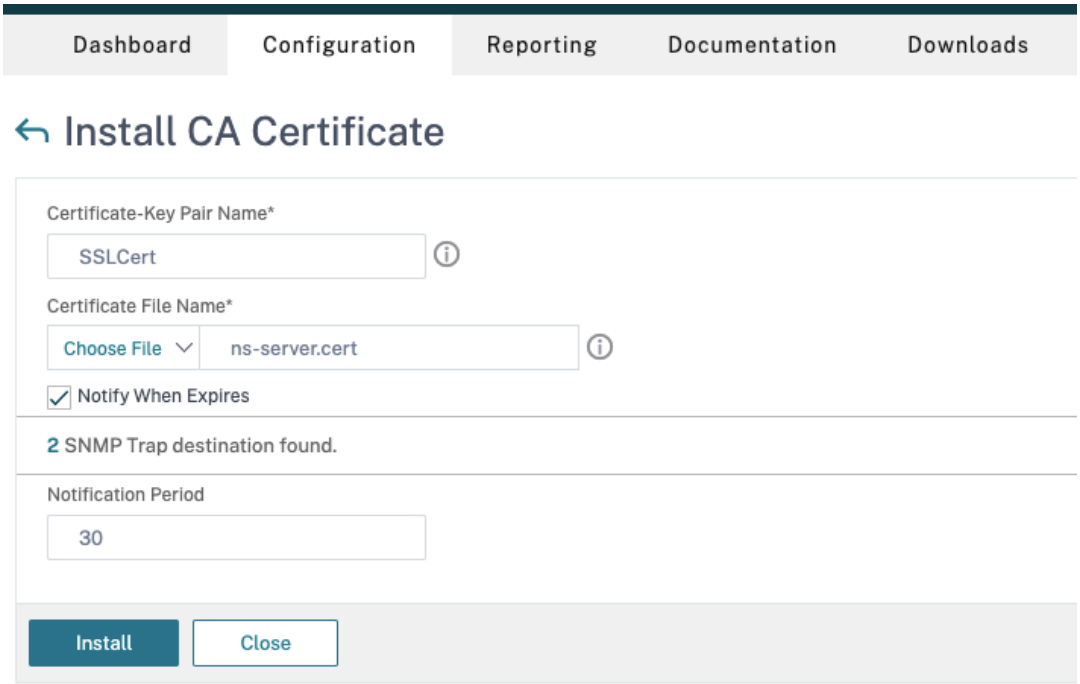


- Os modos e recursos necessários no dispositivo Citrix ADC estão ativados.
  - Para ativar os modos, na GUI do Citrix ADC, navegue até **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, navegue até **System > Settings > Configure Basic Features**.
- As configurações relacionadas aos certificados estão completas.
  - A solicitação de assinatura de certificado (CSR) é criada. Para obter detalhes, consulte Criar um certificado.

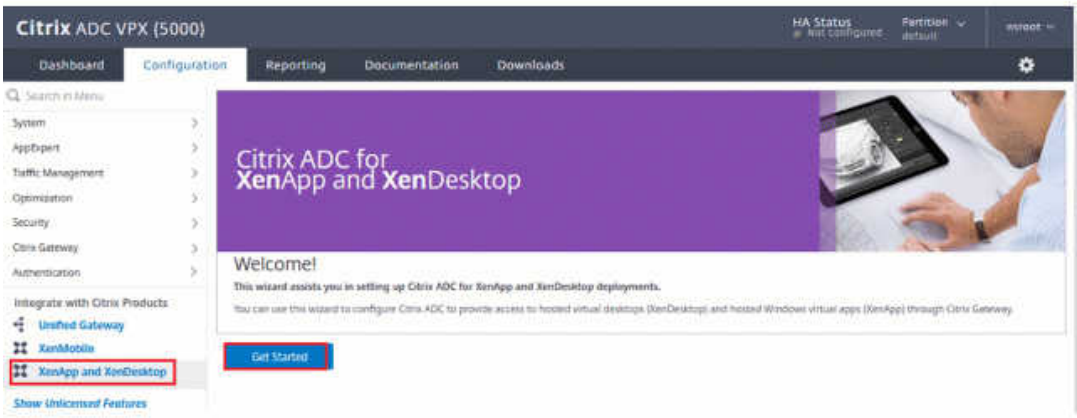


– O servidor e os certificados CA e os certificados raiz estão instalados. Para obter detalhes, consulte Instalação, link e atualizações.



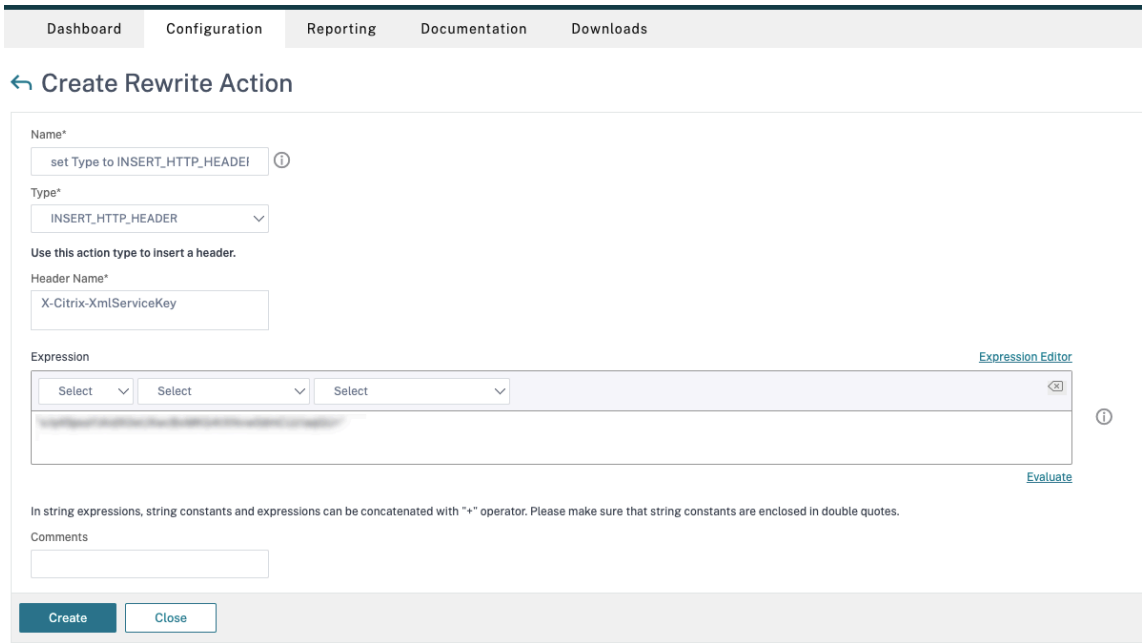


- Um Citrix Gateway foi criado para o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Teste a conectividade clicando no botão **Test STA Connectivity** para confirmar se os servidores virtuais estão online. Para obter detalhes, consulte Configuração do Citrix ADC para Citrix Virtual Apps and Desktops.



2. Adicione uma ação de regravação Para obter detalhes, consulte Configurando uma ação de regravação.

   a) Navegue até **AppExpert > Rewrite > Actions**.
   b) Clique em **Add** para adicionar uma nova ação de regravação. Você pode nomear a ação como “set Type to INSERT_HTTP_HEADER”.



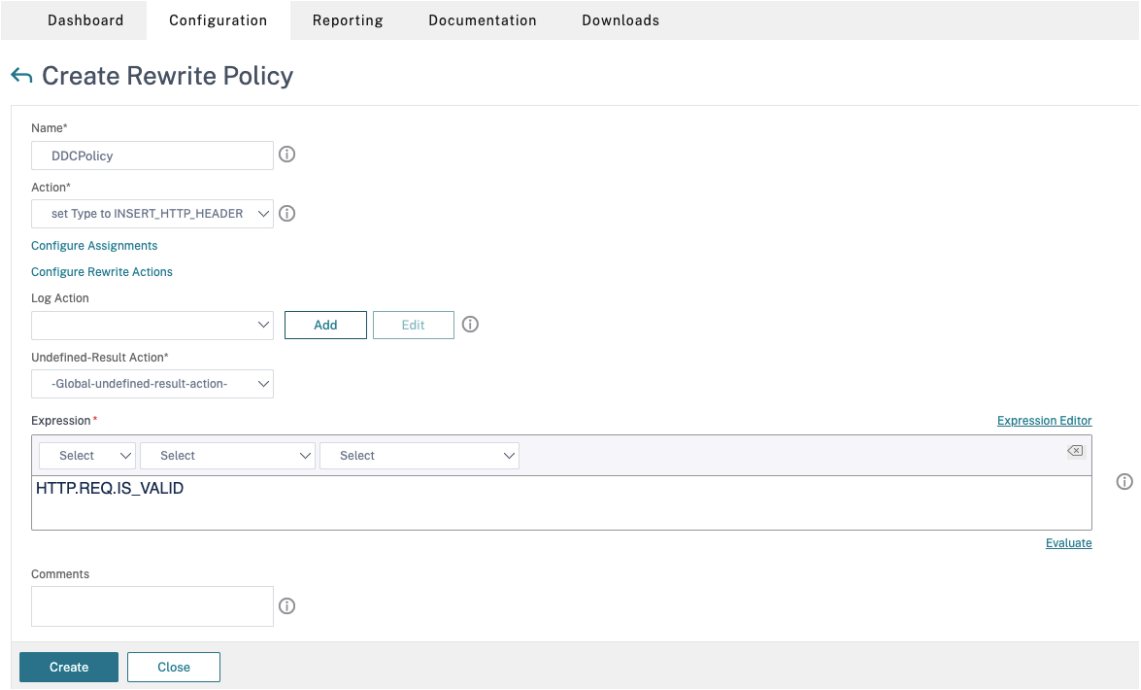
   a) Em **Type**, selecione **INSERT_HTTP_HEADER**.
   b) Em **Header Name**, insira X-Citrix-XMLServiceKey.
   c) Em **Expression**, adicione <`XmlServiceKey1 value`> com as aspas. Você pode copiar o valor XmlServiceKey1 da configuração do Desktop Delivery Controller.


```
PS C:\Users\tyadmin> Get-BrokerSite


BaseOU                                          :
BrokerServiceGroupUid                           :
ColorDepth                                      :
ConfigLastChangeTime                            :
ConfigurationServiceGroupUid                    :
ConnectionLeasingEnabled                        :
DefaultMinimumFunctionalLevel                   :
DesktopGroupIconUid                             :
DnsResolutionEnabled                            :
IsSecondaryBroker                               :
LicenseEdition                                  :
LicenseGraceSessionsRemaining                   :
LicenseModel                                    :
LicenseServerName                               :
LicenseServerPort                               :
LicensedSessionsActive                          :
LicensingBurnIn                                 :
LicensingBurnInDate                             :
LicensingGraceHoursLeft                         :
LicensingGracePeriodActive                      :
LicensingOutOfBoxGracePeriodActive              :
LocalHostCacheEnabled                           :
MetadataMap                                     :
Name                                            :
PeakConcurrentLicenseUsers                      :
RequireXmlServiceKeyForNFuse                    :
RequireXmlServiceKeyForSta                      :
ReuseMachinesWithoutShutdownInOutageAllowed     :
SecureIcaRequired                               :
TotalUniqueLicenseUsers                         :
TrustManagedAnonymousXmlServiceRequests         :
TrustRequestsSentToTheXmlServicePort            :
UseVerticalScalingForRdsLaunches                :
XmlServiceKey1                                  :
XmlServiceKey2                                  :
```

3. Adicione uma política de regravação. Para obter detalhes, consulte Configurando uma política de regravação.

   a) Navegue até **AppExpert > Rewrite > Policies**.

   b) Clique em **Add** para adicionar uma nova política.



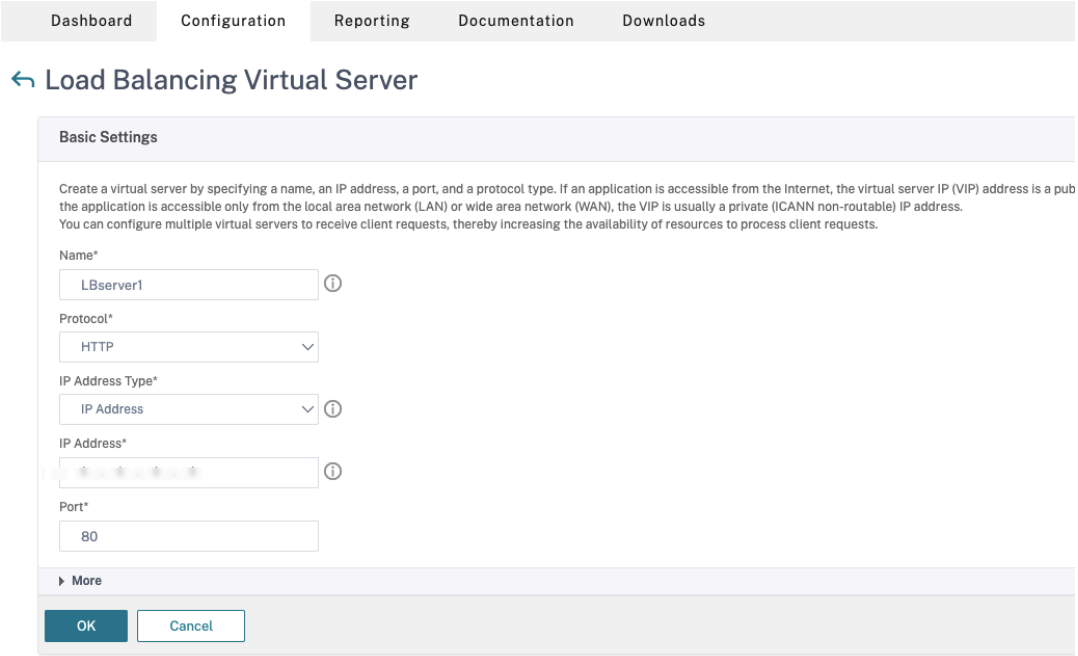
a) Em **Action**, selecione a ação criada na etapa anterior.
b) Em **Action**, adicione HTTP.REQ.IS_VALID.
c) Clique em **OK**.

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 o balanceamento de carga básico.

   a) Crie um servidor virtual de balanceamento de carga.

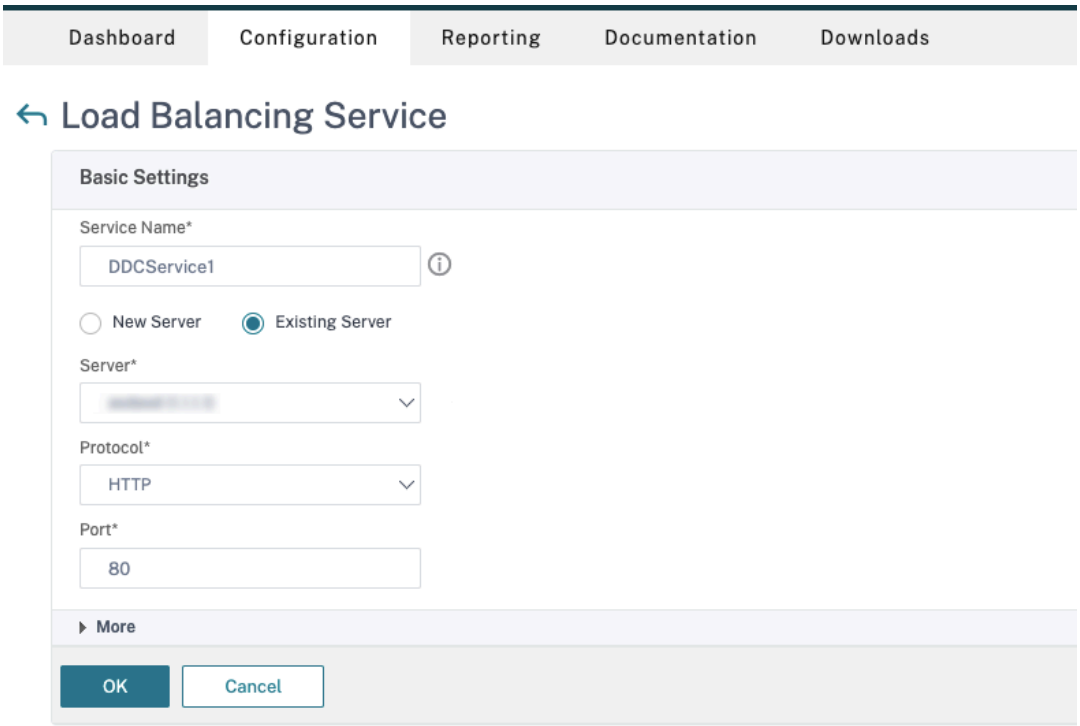
      - Navegue até **Traffic Management > Load Balancing > Servers**.
      - Na página **Virtual Servers**, clique em **Add**.



- Em **Protocol**, selecione **HTTP**.
- Adicione o endereço IP virtual de balanceamento de carga e, em **Port**, selecione **80**.
- Clique em **OK**.

b) Crie um serviço de balanceamento de carga.

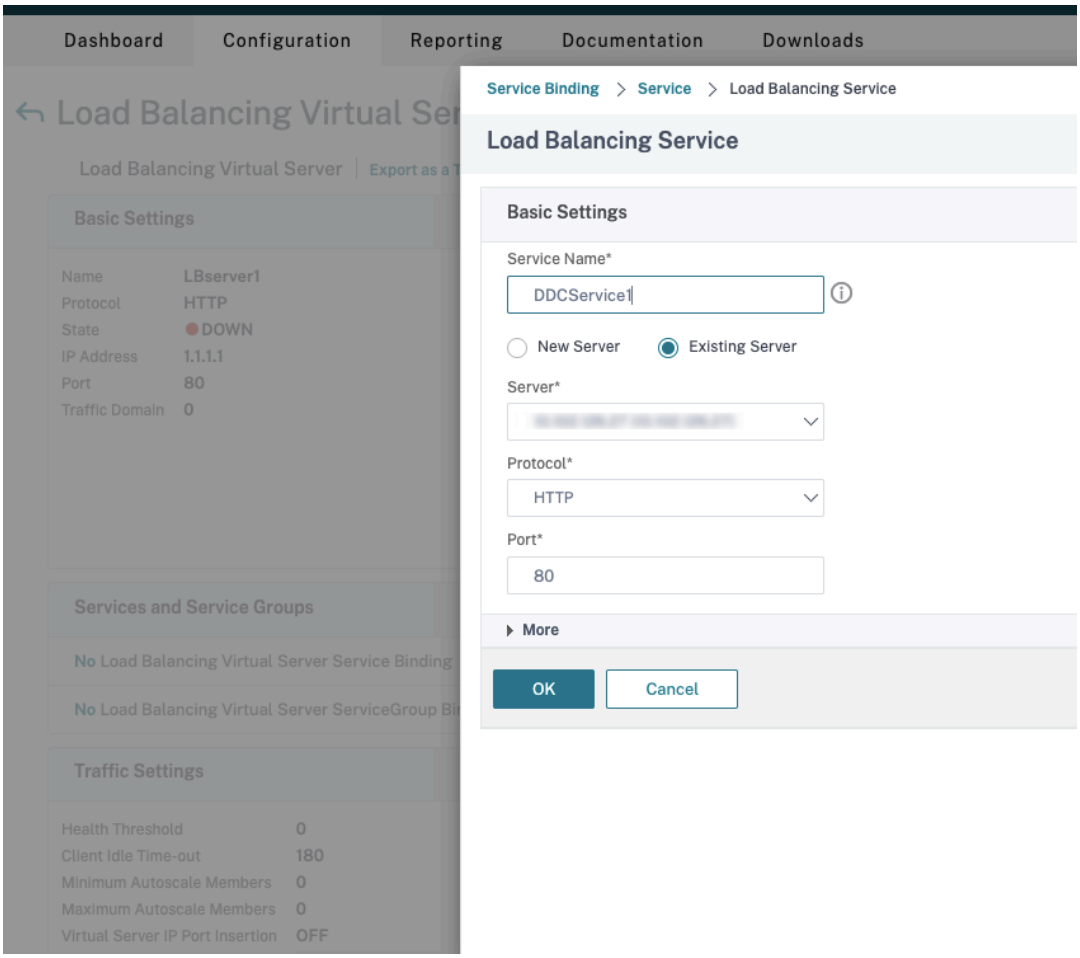
- Navegue até **Traffic Management > Load Balancing > Services**.



- Em **Existing Server**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocol**, selecione **HTTP** e, em **Port**, selecione **80**.
- Clique em **OK** e clique em **Done**.

c) Vincule o serviço ao servidor virtual.

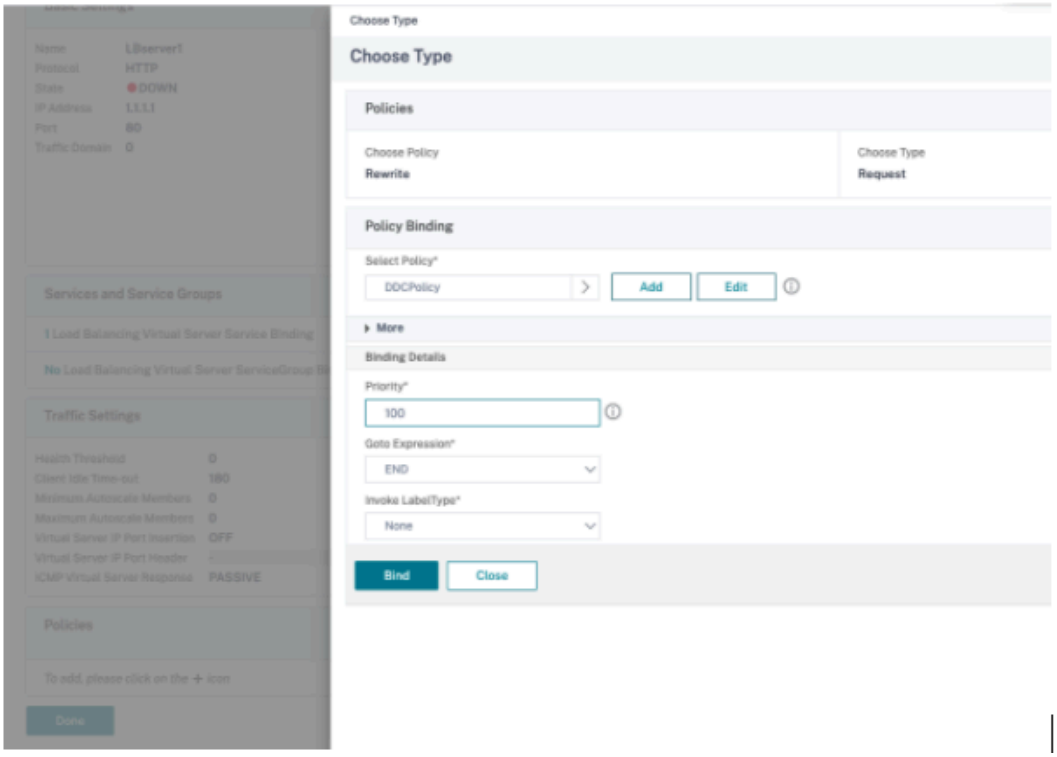
- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Services and Service Groups**, clique em **No Load Balancing Virtual Server Service Binding**.



- Em **Service Binding**, selecione o Citrix DaaS criado anteriormente.
- Clique em **Bind**.

d) Vincule a política de regravação criada anteriormente ao servidor virtual.

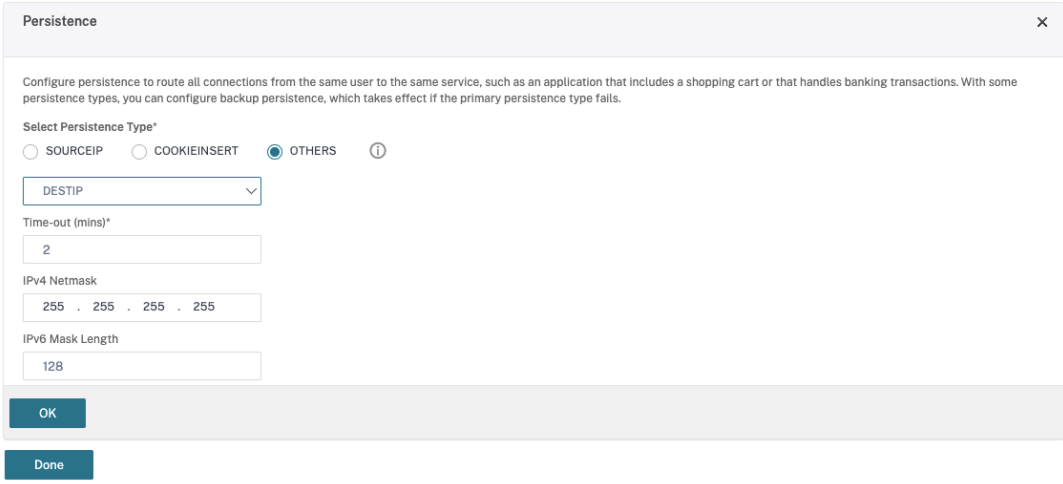
- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Advanced Settings**, clique em **Policies** e então, na sessão **Policies**, clique em **+**.



- Em **Choose Policy**, selecione **Rewrite** e em **Choose Type**, selecione **Request**.
- Clique em **Continue**.
- Em **Select Policy**, selecione a política de regravação criada anteriormente.
- Clique em **Bind**.
- Clique em **Concluído**.

e) Configure a persistência para o servidor virtual, se necessário.

- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Advanced Settings**, clique em **Persistence**.



- Selecione o tipo de persistência como **Others**.

- Selecione **DESTIP** para criar sessões de persistência com base no endereço IP do serviço selecionado pelo servidor virtual (o endereço IP de destino)
- Em **IPv4 Netmask**, adicione uma máscara de rede igual à do DDC.
- Clique em **OK**.

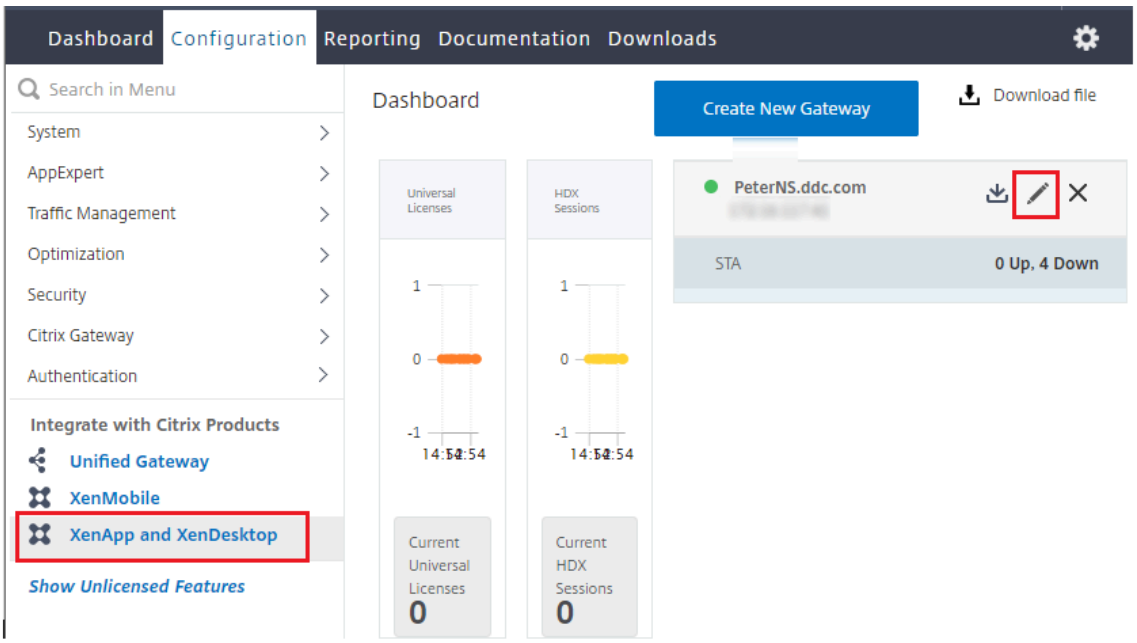
f) Repita essas etapas para o outro servidor virtual também.

Mudanças de configuração se o dispositivo Citrix ADC já estiver configurado com o Citrix DaaS

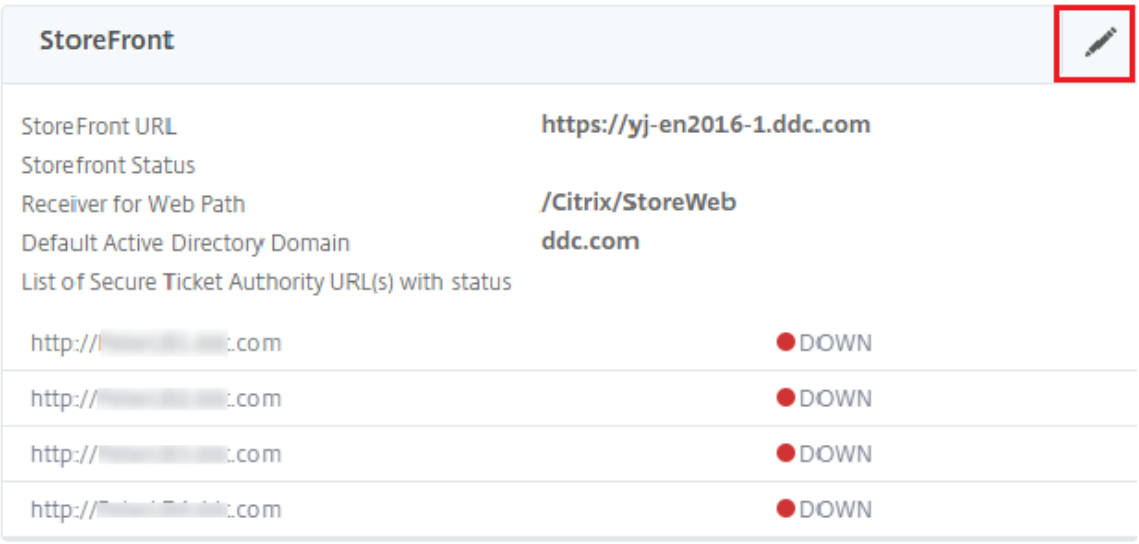
Se você já configurou o dispositivo Citrix ADC com o Citrix DaaS, para usar o recurso Secure XML, faça as seguintes alterações de configuração.

- Antes do início da sessão, altere o **Security Ticket Authority URL** do gateway para usar os FQDNs dos servidores virtuais de balanceamento de carga.
- Verifique se o parâmetro `TrustRequestsSentToTheXmlServicePort` está definido como False. Por padrão, o parâmetro `TrustRequestsSentToTheXmlServicePort` é definido como False. No entanto, se o cliente já tiver configurado o Citrix ADC para o Citrix DaaS, o `TrustRequestsSentToTheXmlServicePort` é definido como True.

1. Na GUI do Citrix ADC, navegue até **Configuration > Integrate with Citrix Products** e clique em **XenApp and XenDesktop**.
2. Selecione a instância do gateway e clique no ícone de edição.

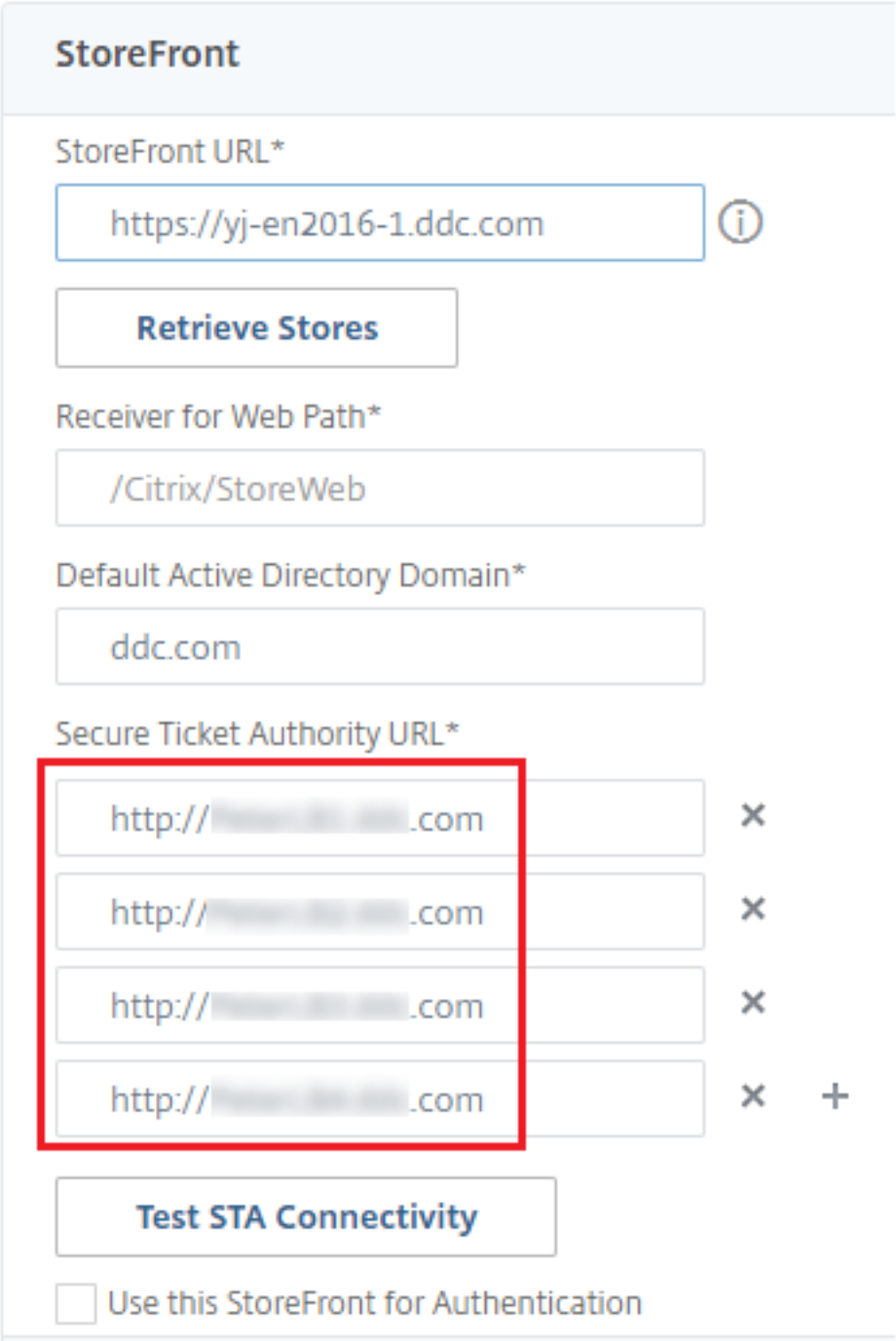


3. No painel StoreFront, clique no ícone de edição.



4. Adicione o **Secure Ticket Authority URL**.

   - Se o recurso XML seguro estiver habilitado, a URL STA deverá ser a URL do serviço de balanceamento de carga.
   - Se o recurso XML seguro estiver desativado, a URL STA deverá ser a URL do STA (endereço do DDC) e o parâmetro TrustRequestsSentToTheXmlServicePort no DDC deve ser definido como True.



Sessões

January 27, 2023

Manter a atividade da sessão é fundamental para oferecer a melhor experiência de usuário. Perder

conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode deixar o usuário tenso. Ser capaz de se mover rapidamente entre estações de trabalho e acessar o mesmo conjunto de aplicativos sempre que fazem logon é uma prioridade para muitos funcionários móveis, como os profissionais de saúde em um hospital.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões e reduzem inconvenientes, tempo de inatividade e perda de produtividade. Usando esses recursos, os usuários móveis podem mudar de forma rápida e fácil entre dispositivos.

Você também pode fazer logoff de usuário, desconectar uma sessão e configurar a pré-inicialização e a permanência da sessão; consulte Gerenciar grupos de entrega.

Confiabilidade da sessão

A opção Session Reliability 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.

Esse recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel e perde a conectividade momentaneamente. 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 no outro lado do túnel. O usuário continua acessando a tela durante a interrupção e pode retomar a interação com o aplicativo quando a conexão de rede é restaurada. A Confiabilidade de Sessão reconecta usuários sem solicitar a reautenticação.

Os usuários do aplicativo Citrix Workspace não podem substituir a configuração do Controller.

Você pode usar a Confiabilidade da Sessão com TLS (Transport Layer Security). O TLS criptografa apenas os dados enviados entre o dispositivo do usuário e o Citrix Gateway.

Ative e configure a Confiabilidade da Sessão com as seguintes configurações de política:

- A configuração da política de conexões de confiabilidade da sessão permite ou evita a confiabilidade da sessão.
- A configuração da política de tempo limite de confiabilidade da sessão tem um padrão de 180 segundos ou três minutos. Embora você possa estender a quantidade de tempo que a Confiabilidade da Sessão mantém uma sessão aberta, esse recurso foi projetado para a conveniência do usuário e, portanto, não solicita que o usuário faça uma nova autenticação. À medida que você estende o tempo que uma sessão é mantida aberta, aumentam as chances de um usuário se distrair e se afastar do dispositivo, podendo deixar a sessão acessível a usuários não autorizados.

- As conexões de confiabilidade de sessão recebidas usam a porta 2598, a menos que você altere o número da porta na configuração da política de número de porta de confiabilidade da sessão.
- Se você não quiser que os usuários sejam capazes de se reconectar a sessões interrompidas sem precisar se autenticar novamente, use o recurso Reconexão automática de cliente. Você pode definir a configuração da política de Autenticação de reconexão automática de cliente para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usa a Confiabilidade da sessão e a Reconexão automática de cliente, os dois recursos funcionam em sequência. A Confiabilidade da Sessão fecha ou desconecta a sessão do usuário após o tempo especificado na configuração da política de tempo limite de confiabilidade da sessão. Depois disso, as configurações da política de Reconexão automática de cliente entram em vigor, tentando reconectar o usuário à sessão desconectada.

Reconexão automática de cliente

Com o recurso de Reconexão automática de cliente, o aplicativo Citrix Workspace pode detectar desconexões não intencionais de sessões ICA e reconectar os usuários às sessões afetadas automaticamente. Quando esse recurso está ativado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Em 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.

Em sessões de área de trabalho, o aplicativo Citrix Workspace tenta se reconectar à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, esse período 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 não são feitas mais tentativas para reconectar a sessão.

Ative e configure a Reconexão automática de cliente com as seguintes configurações de política:

- **Reconexão automática de cliente:** ativa ou desativa a reconexão automática pelo aplicativo Citrix Workspace após uma conexão ter sido interrompida.
- **Autenticação de reconexão automática de cliente:** ativa ou desativa o requisito de autenticação do usuário após a reconexão automática.
- **Log de reconexão automática de cliente:** ativa ou desativa o log de eventos de reconexão no log de eventos. O log é desativado por padrão. Quando ativado, o log do sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e com falha. Cada

servidor armazena informações sobre eventos de reconexão no log do seu próprio sistema. O site não fornece um log combinado de eventos de reconexão para todos os servidores.

A Reconexão automática de cliente 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 ao servidor para reconexão. O servidor descriptografa as credenciais e as envia ao logon do Windows para autenticação. Quando os cookies expiram, os usuários devem se autenticar novamente para se reconectar às sessões.

Os cookies não são usados se você ativar a configuração de autenticação de reconexão automática de cliente. Em vez disso, uma caixa de diálogo solicita as credenciais aos usuários 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.

Desative a Reconexão automática de cliente no aplicativo Citrix Workspace para Windows usando o arquivo icaclient.adm. Para obter mais informações, consulte a documentação correspondente à sua versão do aplicativo Citrix Workspace para Windows.

As configurações das conexões também afetam a reconexão automática de cliente:

- Por padrão, a reconexão automática de cliente é ativada por meio de configurações de política no nível do site, conforme descrito acima. A reautenticação do usuário não é exigida. 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. A reconexão automática de cliente só funciona se o servidor desconectar sessões quando houver uma conexão interrompida ou expirada. Nesse contexto, a conexão ICA TCP refere-se à porta virtual de um servidor (em vez de uma conexão de rede real) que é usada para sessões em redes TCP/IP.
- Por padrão, a conexão ICA TCP em um servidor é definida para desconectar sessões com conexões interrompidas ou expiradas. As sessões desconectadas permanecem intactas na memória do sistema e ficam disponíveis para reconexão pelo aplicativo Citrix Workspace.
- A conexão pode ser configurada para redefinir ou fazer o logoff de sessões com conexões interrompidas ou expiradas. Quando uma sessão é redefinida, tentar reconectar inicia uma nova sessão. Em vez de restaurar um usuário no mesmo local no aplicativo em uso, o aplicativo é reiniciado.
- Se o servidor estiver configurado para redefinir sessões, a reconexão automática de cliente criará uma sessão. Esse processo exige que os usuários insiram suas credenciais para fazer logon no servidor.
- A reconexão automática pode falhar se o aplicativo Citrix Workspace ou o plug-in enviar informações de autenticação incorretas, o que pode ocorrer durante um ataque ou se o servidor

determinar que decorreu muito tempo desde que ele detectou a conexão interrompida.

ICA Keep-Alive

Permitir o recurso ICA Keep-Alive impede que conexões interrompidas sejam desconectadas. Quando ativado, se o servidor não detectar nenhuma atividade (por exemplo, nenhuma mudança de relógio, nenhum movimento do mouse, nenhuma atualização de tela), esse recurso impede que os Serviços de Área de Trabalho Remota desconectem a 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 marca a sessão 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 interrompidas sejam desconectadas. Configure o ICA Keep-Alive somente para conexões que não usam a confiabilidade da sessão.

As configurações do ICA Keep-Alive substituem as configurações do keep-alive definidas na Política de grupo do Microsoft Windows.

Ative e configure o ICA Keep-Alive com as seguintes configurações de política:

- **ICA keep alive timeout:** especifica o intervalo (1–3600 segundos) usado para enviar mensagens de ICA keep-alive. Não configure essa opção se quiser que seu software de monitoramento de rede feche conexões inativas em ambientes onde as conexões interrompidas são tão pouco frequentes que permitir que os usuários se reconectem às sessões não é uma preocupação.

  O intervalo padrão é 60 segundos: os 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.

- **ICA keep alives:** envia ou impede o envio de mensagens ICA keep-alive.

Controle do espaço de trabalho

O controle do espaço de trabalho permite que as áreas de trabalho e os aplicativos sigam um usuário de um dispositivo para outro. Essa capacidade de movimento permite que um usuário acesse todas as áreas de trabalho ou aplicativos abertos de qualquer lugar simplesmente fazendo logon, sem ter que reinicializar as áreas de trabalho ou aplicativos em cada dispositivo. Por exemplo, o controle do espaço de trabalho pode ajudar os profissionais de saúde em um hospital que precisam se mover

rapidamente entre diferentes estações de trabalho e acessar o mesmo conjunto de aplicativos sempre que fazem logon. Se você configurar as opções de controle do espaço de trabalho para permitir isso, esses trabalhadores poderão se desconectar de vários aplicativos em um dispositivo cliente e se reconectar para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle do espaço de trabalho afeta as seguintes atividades:

- **Entrar:** por padrão, o controle do espaço de trabalho permite que os usuários se reconectem automaticamente a todas as áreas de trabalho e aplicativos em execução ao fazer logon, ignorando a necessidade de reabri-los manualmente. Por meio do controle do espaço de trabalho, os usuários podem abrir áreas de trabalho ou aplicativos desconectados e outros que estejam ativos em outro dispositivo cliente. Desconectar-se de uma área de trabalho ou aplicativo o mantém em execução no servidor. Se tiver usuários em roaming que devem manter algumas áreas de trabalho ou aplicativos em execução em um dispositivo cliente enquanto se reconectam a um subconjunto de suas áreas de trabalho ou aplicativos em outro dispositivo cliente, você pode configurar o comportamento de reconexão de logon para abrir somente as áreas de trabalho ou aplicativos das quais o usuário se desconectou anteriormente.
- **Reconexão:** depois de fazer logon no servidor, os usuários podem se reconectar a todas as áreas de trabalho ou aplicativos a qualquer momento clicando em Reconectar. Por padrão, Reconectar abre áreas de trabalho e aplicativos que estão desconectados, além dos que estão em execução no momento em outro dispositivo cliente. Você pode configurar Reconectar para abrir apenas as áreas de trabalho ou aplicativos das quais o usuário se desconectou anteriormente.
- **Sair:** para usuários que abrem áreas de trabalho ou aplicativos pelo StoreFront, você pode configurar o comando Log Off para fazer o logoff do usuário do StoreFront e de todas as sessões ativas juntas, ou fazer o log off somente do StoreFront.
- **Desconexão:** os usuários podem se desconectar de todas as áreas de trabalho e aplicativos em execução de uma só vez, sem precisar se desconectar de cada um individualmente.

O controle do espaço de trabalho está disponível para usuários que acessam áreas de trabalho e aplicativos por meio de uma conexão Citrix StoreFront ou por meio do aplicativo Citrix Workspace. Por padrão, o controle do espaço de trabalho está desativado para sessões de área de trabalho virtual, mas está ativado para aplicativos hospedados. O compartilhamento de sessão não ocorre por padrão entre áreas de trabalho publicadas e aplicativos publicados executados dentro dessas áreas de trabalho.

As políticas de usuário, os mapeamentos de unidade e as configurações da impressora mudam adequadamente quando um usuário se move para um novo dispositivo cliente. Políticas e mapeamentos são aplicados de acordo com o dispositivo cliente onde o usuário está conectado à sessão. Por exemplo, se um profissional de saúde fizer logoff de um dispositivo cliente na sala de emergência de um hospital e, em seguida, fizer logon em uma estação de trabalho no laboratório de raios-X do hospital, as políticas, os mapeamentos de impressora e os mapeamentos da unidade de disco cliente apropri-

ados para a sessão no laboratório de raios-X entrarão em vigor na inicialização da sessão.

Você pode personalizar quais impressoras aparecem para os usuários quando eles mudam de localização. 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 ativar e configurar o controle do espaço de trabalho para usuários, consulte a documentação do StoreFront.

Roaming de sessão

> **Nota:**
>
> As informações a seguir orientam você a configurar o roaming de sessão usando o PowerShell. Você pode usar a interface de gerenciamento Full Configuration em seu lugar. Para obter mais informações, consulte Gerenciar grupos de entrega.

Por padrão, as sessões se movem 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 disponíveis nos dois dispositivos simultaneamente. Você pode exibir os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo, ou se existem ou não sessões atuais. Muitas vezes, as impressoras e outros recursos atribuídos ao aplicativo também seguem.

Embora esse comportamento padrão ofereça muitas vantagens, talvez não seja ideal em todos os casos. Você pode impedir o roaming de sessão usando o SDK do PowerShell.

Exemplo 1: um profissional de medicina está usando dois dispositivos: preenchendo um formulário de seguro em um PC desktop e olhando as informações do paciente em um tablet.

- Se o roaming de sessão estiver ativado, os dois aplicativos aparecem nos dois dispositivos (um aplicativo iniciado em um dispositivo fica visível em todos os dispositivos em uso). Isso talvez não atenda aos requisitos de segurança.
- Se o roaming da sessão estiver desativado, o prontuário 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 no escritório. O nome e o local do dispositivo determinam quais impressoras e outros recursos estão disponíveis para a sessão. Mais tarde, ele vai a um escritório no prédio ao lado para uma reunião que exigirá que ele use uma impressora.

- Se o roaming de sessão estiver ativado, o gerente de produção provavelmente não conseguirá acessar as impressoras perto da sala de reuniões, isso porque os aplicativos que ele iniciou anteriormente em seu escritório resultaram na atribuição de impressoras e outros recursos próximos àquele local.

- Se o roaming de sessão estiver desativado, e se ele fizer 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 da área de trabalho:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões do aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Always:** as sessões sempre fazem o roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.
- **DisconnectedOnly:** reconectar-se apenas às sessões que já estão desconectadas; caso contrário, iniciar uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente primeiro desconectando-os ou usando o controle do espaço de trabalho para fazer o roaming explicitamente.) Uma sessão conectada ativa de outro dispositivo cliente nunca é usada. Em vez disso, uma nova sessão é iniciada.
- **SameEndpointOnly:** um usuário obtém uma sessão exclusiva para cada dispositivo cliente que usa. Isso desativa completamente o roaming. Os usuários podem se reconectar somente 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 "Allow only one instance of the application per user"nas propriedades do aplicativo no grupo de entrega.

- Se você desativar o roaming de sessão, desative a opção de limite de aplicativo "Allow only one instance of the application per user".
- Se você ativar o limite de aplicativo "Allow only one instance of the application per user", não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos.

Intervalo de logon

Se uma máquina virtual contendo um VDA de área de trabalho fechar antes que o processo de logon seja concluído, você pode alocar mais tempo ao processo. O padrão para a versão 7.6 e versões posteriores é 180 segundos (o padrão para as versões 7.0 a 7.5 é 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 período em segundos, em formato decimal, no intervalo de 0 a 3600.

Se você alterar a imagem mestre, implemente a nova imagem ao catálogo. Para obter mais informações, consulte Alterar a imagem mestre.

Essa configuração se aplica somente a máquinas virtuais com VDAs de área de trabalho (estação de trabalho) de sessão única. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor multissessão.

Marcas

November 21, 2023

Introdução

Marcas são cadeias de caracteres que identificam itens como máquinas, aplicativos, áreas de trabalho, grupos de entrega, grupos de aplicativos e políticas. Depois de criar uma marca e adicioná-la a um item, você pode personalizar certas operações para aplicá-las apenas a itens que têm uma marca especificada.

- Adapte as exibições de pesquisa na interface de gerenciamento Full Configuration.

  Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma marca chamada “test”e adicione-a (aplique-a) aos aplicativos em questão. Agora você pode filtrar a pesquisa com a marca “test”.

- Publique aplicativos de um grupo de aplicativos ou áreas de trabalho específicas de um grupo de entrega, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Isso é chamado de *restrição de marca*.

Com as restrições de marcas, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando nos custos associados com a implantação e gerenciamento de mais máquinas. Uma restrição de marca pode ser considerada como uma subdivisão (ou partição) de máquinas em um grupo de entrega. Sua funcionalidade é semelhante, mas não idêntica, a worker groups em versões do XenApp anteriores à 7.x.

Usar um grupo de aplicativos ou áreas de trabalho com restrição de marca pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Detalhes e exemplos de uso de uma restrição de marca são descritos mais adiante neste artigo.

- Programe reinicializações periódicas para um subconjunto de máquinas em um grupo de entrega.

  O uso de uma restrição de marca para máquinas permite que você use novos cmdlets do PowerShell para configurar várias programações de reinicialização para subconjuntos de máquinas em um grupo de entrega. Para obter exemplos e detalhes, consulte Gerenciar grupos de entrega.

- Adapte a aplicação (atribuição) das políticas Citrix a máquinas em grupos de entrega, tipos de grupo de entrega ou unidades organizacionais que tenham (ou não tenham) uma marca especificada.

  Por exemplo, se você quiser aplicar uma política Citrix apenas às estações de trabalho mais poderosas, adicione uma marca chamada "high power"a essas máquinas. Em seguida, na página **Assign Policy** do assistente de criação de política, selecione a marca e a caixa de seleção **Enable**. Você também pode adicionar uma marca a um grupo de entrega e aplicar uma política Citrix a esse grupo. Para obter detalhes, consulte Criar políticas.

Você pode aplicar marcas a:

- Máquinas
- Aplicativos
- Catálogos de máquinas
- Grupos de entrega
- Grupos de aplicativos

Você pode configurar uma restrição de marca ao criar ou editar o seguinte na interface de gerenciamento Full Configuration:

- Uma área de trabalho em um grupo de entrega compartilhado
- Um grupo de aplicativos

Restrições de marcas para uma área de trabalho ou grupo de aplicativos

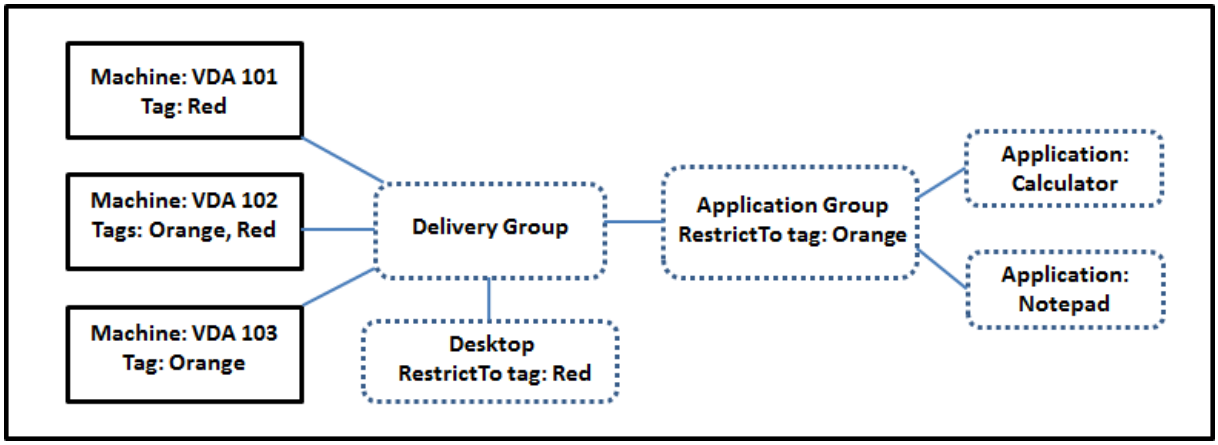
Uma restrição de marca envolve várias etapas:

- Criar a marca e adicioná-la (aplicá-la) às máquinas.
- Criar ou editar um grupo com a restrição de marca (em outras palavras, restringir inicializações a máquinas com a marca *x*).

Uma restrição de marca estende o processo de seleção da máquina do Controller. O Controller seleciona uma máquina de um grupo de entrega associado sujeito a política de acesso, listas de usuários configurados, preferência de zona e prontidão de inicialização, além da restrição de marca (se presente). Para aplicativos, o Controller faz o fallback a outros grupos de entrega em ordem prioritária, aplicando as mesmas regras de seleção de máquina a cada grupo de entrega considerado.

Exemplo 1: layout simples

Este exemplo apresenta um layout simples que usa restrições de marca para limitar quais máquinas são consideradas para determinadas inicializações de áreas de trabalho e aplicativos. Existe um grupo de entrega compartilhado, uma área de trabalho publicada e um grupo de aplicativos configurado com dois aplicativos.



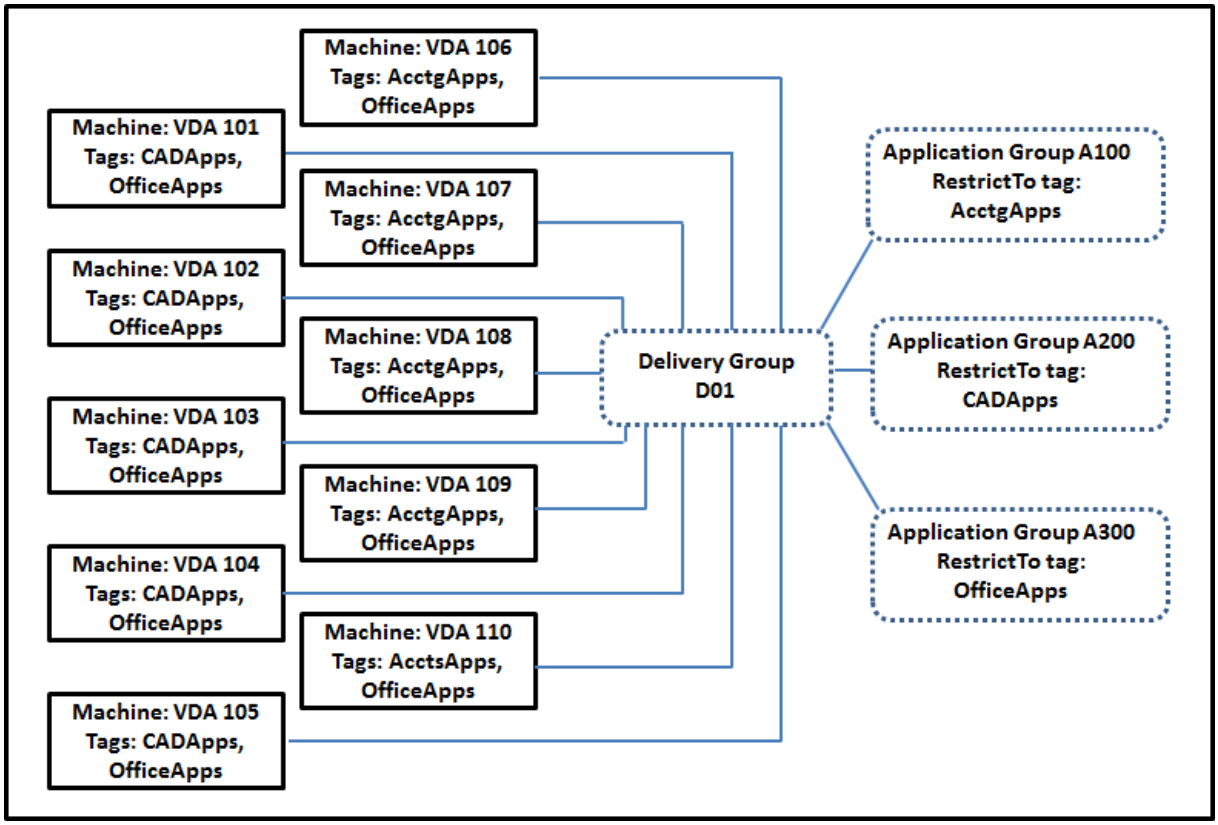
- As marcas forem adicionadas a cada uma das três máquinas (VDA 101-103).
- A área de trabalho no grupo de entrega foi criada com uma restrição de marca chamada `Red`. Assim, essa área de trabalho só pode ser iniciada em máquinas desse grupo de entrega que tenham a marca `Red`: VDA 101 e 102.
- O grupo de aplicativos foi criado com a restrição de marca `Orange`. Assim, cada um de seus aplicativos (`Calculator` e `Notepad`) pode ser iniciado apenas em máquinas desse grupo de entrega que possuem a tag `Orange`: VDA 102 e 103.

A máquina VDA 102 tem as duas marcas (`Red` e `Orange`), por isso pode ser considerada para iniciar os aplicativos e a área de trabalho.

Exemplo 2: layout mais complexo

Este exemplo contém vários grupos de aplicativos que foram criados com restrições de marca. Isso resulta na capacidade de entregar mais aplicativos com menos máquinas do que seriam necessárias se você usasse apenas grupos de entrega.

Como configurar o exemplo 2 mostra as etapas usadas para criar e aplicar as marcas e depois configurar as restrições de marca no exemplo.



Esse exemplo usa 10 máquinas (VDA 101-110), um grupo de entrega (`D01`) e três grupos de aplicativos (`A100`, `A200`, `A300`). Ao aplicar marcas a cada máquina e especificar restrições de marca ao criar cada grupo de aplicativos:

- Os usuários de contabilidade no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 101—105)
- Os designers de CAD no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 106-110)
- Os 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 marcas e restrições de marca

As marcas são criadas, adicionadas (aplicadas), editadas e excluídas dos itens selecionados por meio da ação **Manage Tags** na interface de gerenciamento Full Configuration.

(Exceção: as marcas usadas para atribuições de política são criadas, editadas e excluídas por meio da ação **Manage Tags**. No entanto, você aplica (atribui) marcas ao criar a política. Consulte Criar políticas para obter detalhes.)

As restrições de marca são configuradas quando você cria ou edita áreas de trabalho em grupos de entrega e quando cria e edita grupos de aplicativos.

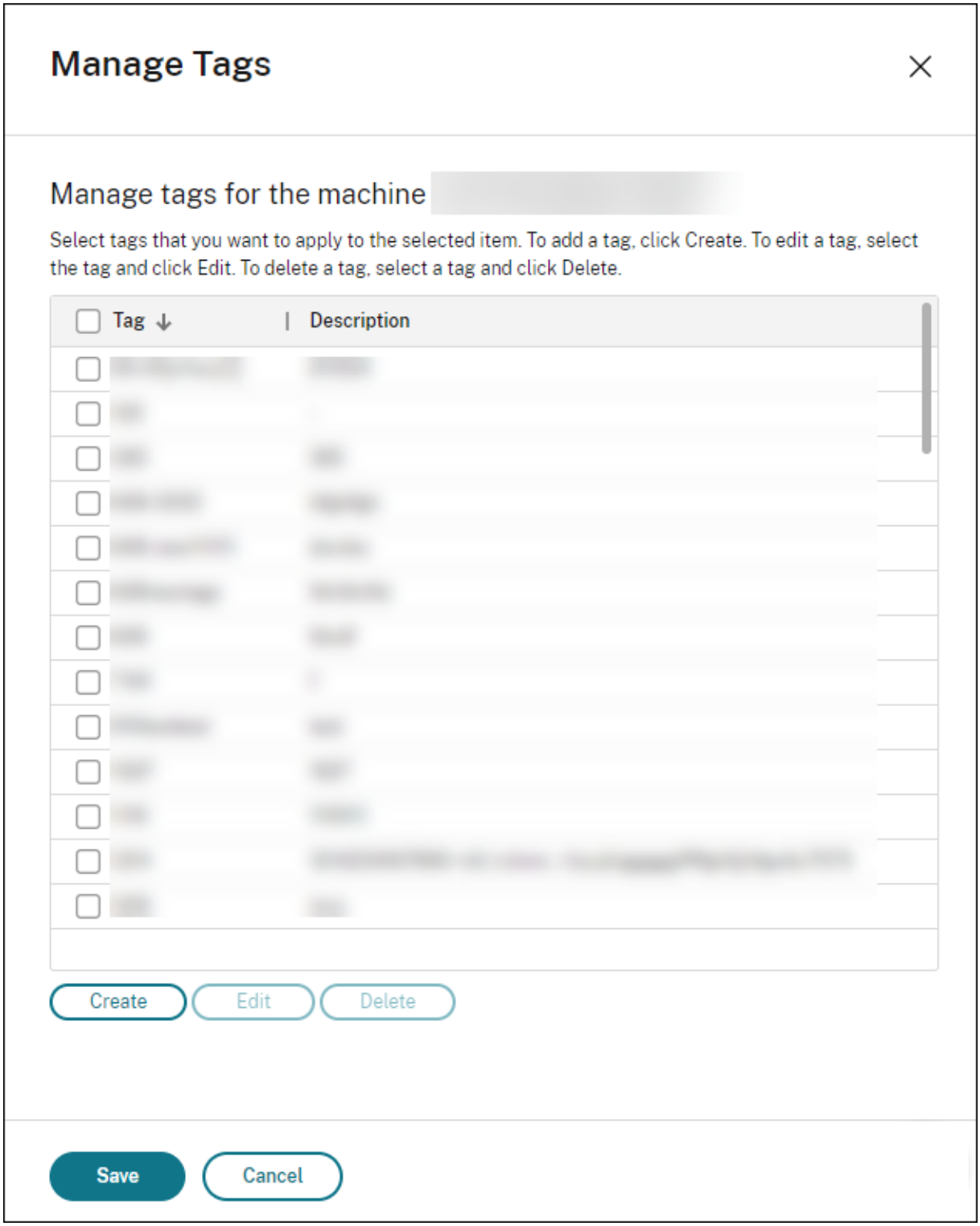
Usar o recurso Manage Tags

Em **Manage > Full Configuration**, selecione os itens aos quais deseja aplicar uma marca. Os itens incluem:

- Uma ou mais máquinas
- Um ou mais aplicativos
- Uma área de trabalho, um grupo de entrega ou um grupo de aplicativos
- Um catálogo de máquinas

Depois, selecione **Manage Tags** na barra de ações. A caixa de diálogo **Manage Tags** lista todas as marcas existentes, não apenas aquelas para os itens selecionados.

- Uma caixa de seleção ativada indica que a marca já foi adicionada aos itens selecionados. (Na captura de tela abaixo, a máquina selecionada tem uma marca 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 marca adicionada.



As ações a seguir estão disponíveis na caixa de diálogo **Manage Tags**. Consulte Cuidados ao trabalhar com marcas.

- **Para criar uma marca:**

Selecione **Create.** Insira um nome e uma descrição. O nome das marcas deve ser exclusivo, e não faz diferença entre maiúsculas e minúsculas. Em seguida, selecione **Save**.

Criar uma marca não a aplica automaticamente a itens selecionados. Use as caixas de seleção para aplicar a marca.

- **Para adicionar (aplicar) uma ou mais marcas:**

  Ative a caixa de seleção ao lado do nome da marca. Uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados já têm a marca aplicada. Quando você seleciona vários itens e a caixa de seleção de uma marca tem um hífen, alterá-la para uma marca de seleção afeta todas as máquinas selecionadas.

  Se você tentar adicionar uma marca às máquinas, e a marca for usada como restrição em um grupo de aplicativos, você receberá um aviso de que a ação pode disponibilizar as máquinas para inicialização. Se é isso o que você quer, prossiga.

- **Para remover uma ou mais marcas:**

  Desmarque a caixa de seleção ao lado do nome da marca. Uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados já têm a marca aplicada. Quando você seleciona vários itens e a caixa de seleção de uma marca tem um hífen, desmarcar a caixa de seleção remove a marca de todas as máquinas selecionadas.

  Se você tentar remover uma restrição de marca de uma máquina, receberá um aviso de que a ação pode afetar as máquinas consideradas para a inicialização. Se é isso o que você quer, prossiga.

- **Para editar uma marca:**

  Selecione uma marca e selecione **Edit**. Insira um novo nome e descrição. Você pode editar apenas uma marca de cada vez.

- **Para excluir uma ou mais marcas:**

  Selecione as marcas e selecione **Delete**. A caixa de diálogo **Delete Tag** indica quantos itens usam atualmente as marcas selecionadas (por exemplo, “2 machines”). Selecione um item para exibir mais informações (por exemplo, os nomes das duas máquinas que têm a marca aplicada). Confirme se deseja excluir as marcas.

  Você não pode excluir uma marca que é usada como uma restrição. Primeiro, edite o grupo de aplicativos e remova a restrição de marca ou selecione uma marca diferente.

Quando terminar de usar a caixa de diálogo **Manage Tags**, selecione **Save**.

Para ver se uma máquina tem marcas aplicadas: selecione **Delivery Groups** no painel esquerdo. Selecione um grupo de entrega e selecione **View Machines** na barra de ações. Selecione uma máquina e, em seguida, selecione a guia **Tags** no painel **Details**.

Gerenciar restrições de marca

Configurar uma restrição de marca é um processo de várias etapas: primeiro você cria a marca e a adiciona/aplica às máquinas. Em seguida, você adiciona a restrição ao grupo de aplicativos ou à área de trabalho.

- **Criar e aplicar uma marca:**

  Crie a marca e adicione-a (aplique-a) às máquinas que serão afetadas pela restrição de marca, usando as ações **Manage Tags**.

- **Para adicionar uma restrição de marca a um grupo de aplicativos:**

  Crie ou edite o grupo de aplicativos. Na página **Delivery Groups**, selecione **Restrict launches to machines with the tag** e depois selecione a marca na lista.

- **Para alterar ou remover a restrição de marca em um grupo de aplicativos:**

  Edite o grupo. Na página **Delivery Groups**, selecione uma marca diferente na lista ou remova a restrição de marca completamente desmarcando **Restrict launches to machines with the tag**.

- **Para adicionar uma restrição de marca a uma área de trabalho:**

  Crie ou edite um grupo de entrega. Selecione **Add** ou **Edit** na página **Desktops**. Na caixa de diálogo **Add Desktop**, selecione **Restrict launches to machines with the tag** e depois selecione a marca de tag no menu.

- **Para alterar ou remover a restrição de marca em um grupo de entrega:**

  Edite o grupo. Na página **Desktops**, selecione **Edit**. Na caixa de diálogo, selecione uma marca diferente na lista ou remova a restrição de marca completamente desmarcando **Restrict launches to machines with the tag**.

Cuidados ao trabalhar com marcas

Uma tag aplicada a um item pode ser usada para diferentes propósitos. Lembre-se de que adicionar, remover e excluir uma marca pode ter efeitos indesejados. Você pode usar uma marca para classificar a exibição das máquinas ao usar a pesquisa na interface de gerenciamento Full Configuration. Você pode usar a mesma marca como restrição ao configurar um grupo de aplicativos ou uma área de trabalho. Essa ação limita a consideração de inicialização a apenas máquinas em grupos de entrega especificados que tenham essa marca.

Se você adicionar uma marca às máquinas depois que essa marca for configurada como uma restrição de marca de área de trabalho ou grupo de aplicativos, você será avisado de que pode tornar as máquinas disponíveis para iniciar mais aplicativos ou áreas de trabalho. Se é isso o que você quer, prossiga. Caso contrário, cancele a operação.

Por exemplo, digamos que você crie um grupo de aplicativos com a restrição de marca Red. Mais tarde, você adiciona várias outras máquinas nos mesmos grupos de entrega usados por esse grupo de aplicativos. Se você tentar adicionar a marca Red a essas máquinas, verá uma mensagem semelhante a: "A marca Red é usada como uma restrição nos seguintes grupos de aplicativos. Adicionar essa marca pode disponibilizar as máquinas selecionadas para iniciar aplicativos neste grupo de aplicativos."Você pode confirmar ou cancelar a adição da tag às 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-lo como uma restrição. (Se você tiver permissão para excluir essa marca, isso pode resultar na permissão de que os aplicativos podem ser iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição contra a exclusão de uma marca se aplica se a marca estiver sendo usada como uma restrição a inicializações de áreas de trabalho. Depois de editar o grupo de aplicativos ou áreas de trabalho no grupo de entrega para remover essa restrição de marca, você pode excluir a marca.

Nem todas as máquinas têm os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada qual com uma restrição de marca diferente e conjuntos diferentes ou sobrepostos de máquinas de grupos de entrega. A tabela a seguir ilustra como as considerações de máquina são decididas.

Quando um aplicativo é adicionado a	Estas máquinas nos grupos de entrega selecionados são consideradas para inicialização
Um grupo de aplicativos sem restrição de marca	Qualquer máquina.
Um grupo de aplicativos com restrição de marca A	Máquinas que têm a marca A aplicada.
Dois grupos de aplicativos, um com restrição de marca A e outro com restrição de marca B	Máquinas que têm a marca A e a marca B. Se nenhuma estiver disponível, as máquinas que têm a marca A ou a marca B.
Dois grupos de aplicativos, um com restrição de marca A e outro sem restrição de marca	Máquinas que têm a marca A. Se nenhuma estiver disponível, então qualquer máquina.

Se você usou uma restrição de marca em uma programação de reinicialização de máquina, quaisquer alterações feitas que afetem as aplicações ou restrições de marcas afetam o próximo ciclo de reinicialização da máquina. Isso não afeta nenhum ciclo de reinicialização que está em andamento enquanto as alterações estão sendo feitas.

Como configurar, exemplo 2

A sequência a seguir mostra as etapas para criar e aplicar marcas e depois configurar restrições de marca 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 marcas às máquinas:

1. Em **Manage > Full Configuration**, selecione **Delivery Groups** no painel esquerdo. Selecione o grupo de entrega `D01` e selecione **View Machines** na barra de ações.
2. Selecione as máquinas VDA 101-105 e, em seguida, selecione **Manage Tags** no painel de ação.
3. Na caixa de diálogo **Manage Tags**, selecione **Create**. Crie uma marca chamada `CADApps`. Selecione **OK**.
4. Selecione **Create** novamente e crie uma marca chamada `OfficeApps`. Selecione **OK**.
5. Adicione (aplique) as marcas recém-criadas às máquinas selecionadas marcando as caixas de seleção ao lado do nome de cada marca (`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** no painel de ação.
8. Na caixa de diálogo **Manage Tags**, selecione **Create**. Crie uma marca chamada `AcctgApps`. Selecione **OK**.
9. Aplique a marca `AcctgApps` recém-criada e a marca `OfficeApps` às máquinas selecionadas marcando as caixas de seleção ao lado do nome de cada marca. Em seguida, feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de marca.

1. Em **Manage > Full Configuration**, selecione **Applications** no painel esquerdo.
2. Selecione **Create Application Group** na barra de ações. O assistente é iniciado.
3. Na página **Delivery Groups**, selecione o grupo de entrega `D01`. Selecione **Restrict launches to machines with tag** e depois selecione a marca `AcctgApps` na lista.
4. Conclua o assistente, especificando os usuários de contabilidade e os aplicativos de contabilidade. (Ao adicionar o aplicativo, escolha a origem **From Start menu**, que procura o aplicativo nas máquinas que têm a marca `AcctgApps`.) Na página **Summary**, dê o nome `A100` ao grupo.
5. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando máquinas com a marca `CADApps`, além dos usuários e aplicativos apropriados.
6. Repita as etapas para criar o grupo de aplicativos `A300`, especificando máquinas com a marca `OfficeApps`, além dos usuários e aplicativos apropriados.

Aplicar marcas aos catálogos de máquinas

Você pode usar **Manage > Full Configuration** ou o PowerShell para aplicar marcas a catálogos de máquinas.

- O uso da interface de gerenciamento é descrito em Manage tags. As exibições do catálogo não indicam se as marcas são aplicadas ou não.
- Para usar o PowerShell, consulte Usar o PowerShell para aplicar marcas a catálogos.

Aqui está um exemplo de uso de marcas com catálogos:

- Um grupo de entrega contém máquinas de vários catálogos, mas você quer que uma operação (como uma programação de reinicialização) afete apenas as máquinas em um catálogo específico. Aplicar uma marca a esse catálogo atende ao seu requisito.

Usar o PowerShell para aplicar marcas 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 marcas.
- `Get-BrokerCatalog` tem uma propriedade chamada `Tags`.

Por exemplo, os cmdlets a seguir adicionam uma marca 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.

Marcações automáticas (prévia)

A marcação automática permite que os administradores definam e removam tags em vários objetos DaaS automaticamente, com base em regras personalizadas. Esse aprimoramento elimina a necessidade de manter scripts diferentes que são executados periodicamente para otimizar o ambiente.

Casos de uso

Com a marcação automática, você pode implementar regras relevantes para seus impulsionadores de negócios, como reduzir custos, otimizar a infraestrutura e impulsionar o consumo. A seguir estão 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 o pool disponível.
- **Remover a sobrecarga de aplicativos** –para reduzir a sobrecarga de aplicativos, identificando os aplicativos que não foram usados por mais de um número pré-configurado de dias.
- **Grupos de entrega com menos de X nível funcional** –para encontrar grupos de entrega com menos de um determinado nível funcional.
- **Usuários inativos** –para recuperar recursos de usuários que não estão conectados há mais de um número pré-configurado de dias.

Comandos do PowerShell

Você pode criar marcações automáticas usando comandos do PowerShell. Depois que uma regra de marcação automática é criada, ela é avaliada com uma frequência de 600 segundos. Para obter mais informações, consulte New-BrokerAutoTagRule.

Exemplos `New-BrokerAutoTagRule` usa os mesmos parâmetros de filtro e tipo de objeto que o commandlet `Get-BrokerMachine`. Para obter mais informações, consulte GetBrokerMachine.

1. Marque VDIs dedicados que não foram usados por mais de 30 dias com um ID 123:

   a) Defina uma tag para marcar os VDIs não usados, por exemplo, **unused-VDI**.

      - Nome da tag: unused-VDI
      - ID da tag : 123

   b) Crie a regra de marcação automática para marcar máquinas não utilizadas. Defina os parâmetros da regra:

      - Nome : nome genérico da regra.
      - Tipo de objeto: Machine.
      - Texto da regra : máquinas estáticas atribuídas cujo último tempo de conexão é > 30 dias ou nenhum valor.
      - Tag Uid : o ID da tag à qual você deseja se associar, 123.

      ```
      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
      ```

   c) Verifique as máquinas marcadas com a tag **unused-VDI** e libere-as.

2. Para marcar grupos de entrega com menos de X nível funcional (usando **L7_20** como nível funcional limite):


```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-
RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid
 123
```

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 123
```

Mais informações

Postagem do blog: How to assign desktops to specific servers.

Configuração de fuso horário

November 9, 2023

A configuração **Date and time** em **Settings** no console de gerenciamento permite que você personalize o formato de data e hora de acordo com as suas preferências.

Clique em **Edit** para configurar as seguintes opções:

- **Time format:**
  - Selecione para exibir a hora usando um relógio de 12 horas (9 da noite, por exemplo) ou um relógio de 24 horas (21h, por exemplo).

> **Nota:**
>
> Selecione a opção **Same as local** se quiser que o formato se alinhe ao fuso horário do seu navegador.

- **Date format:**
  - Configure o formato de data para corresponder às suas preferências, por exemplo, aaaa/MM/dd.

> **Nota:**
>
> Selecione a opção **Same as local** se quiser que o formato se alinhe ao fuso horário do seu navegador.

- **Time zone:**

- **UTC:** exibe a data e a hora em UTC em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações no seu fuso horário local.
- **Local time zone:** exiba a data e a hora no seu fuso horário local em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações em UTC.

Solucionar problemas de registro do VDA e início de sessão

June 24, 2022

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 do VDA e inicialização de sessão por meio da interface de gerenciamento Full Configuration.

Ao contrário do Cloud Health Check, uma ferramenta independente para avaliar a integridade e a disponibilidade do site e de seus outros componentes, o recurso está disponível como a ação **Run Health Check** na interface de gerenciamento Full Configuration.

A ação **Run Health Check** pode executar as mesmas verificações que Cloud Health Check, exceto:

- No registro do VDA:
  - Disponibilidade da porta de comunicação VDA
- Nas inicializações em VDAs:
  - Disponibilidade da porta de comunicação de início de sessão
  - Caminho de início do aplicativo VDA

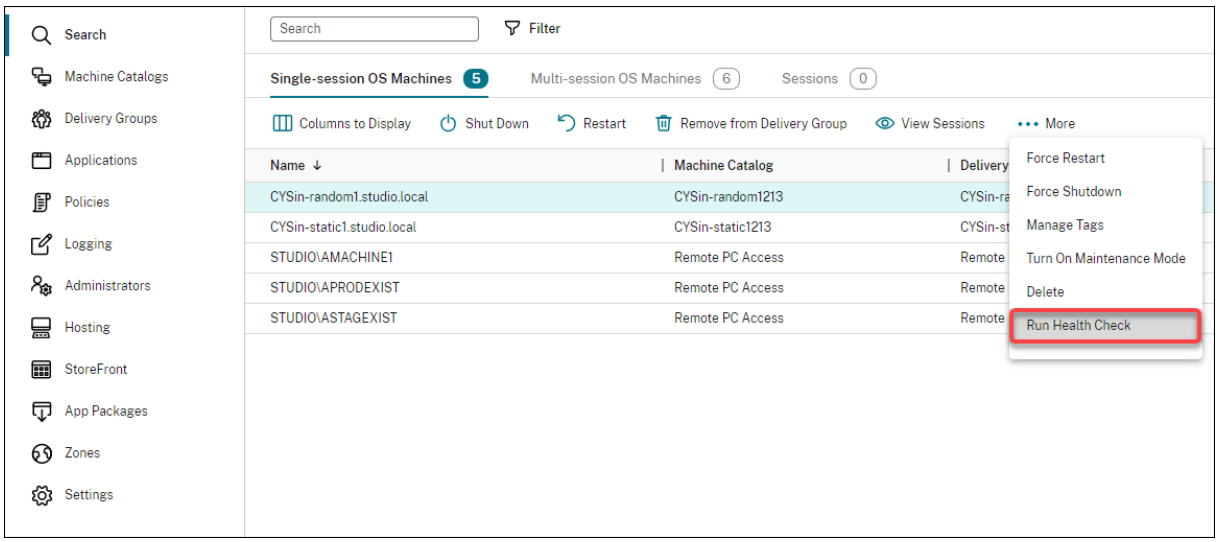
Pré-requisitos

Antes de usar o recurso, verifique se você atende aos seguintes pré-requisitos:

- Windows VDAs
- VDA versão 2109 ou posterior
- VDAs estão registrados

Executar verificações de integridade para VDAs

1. Na interface de gerenciamento Full Configuration, vá para o nó **Search**.
2. Selecione uma ou mais máquinas e, em seguida, selecione **Run Health Check** na barra de ações.

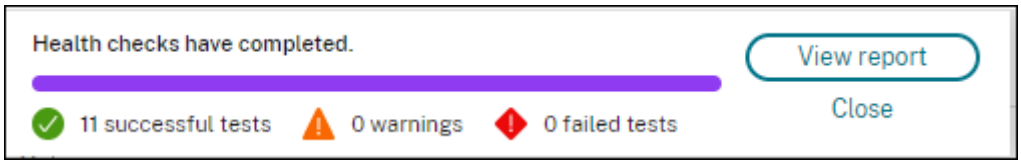


> **Nota:**
>
> Atualmente, você pode executar verificações de integridade somente para VDAs registrados. A ação **Run Health Check** não está disponível para VDAs não registrados.

Depois de selecionar **Run Health Check**, uma janela é exibida, mostrando o progresso das verificações de integridade. Aguarde até que as verificações de integridade sejam concluídas ou clique em **Cancel** para cancelar as verificações. Se necessário, você pode mover a janela.

> **Nota:**
>
> Nos cenários em que já existe uma janela “health checks in progress”, você não pode executar verificações de integridade adicionais até que as verificações de integridade existentes sejam concluídas.

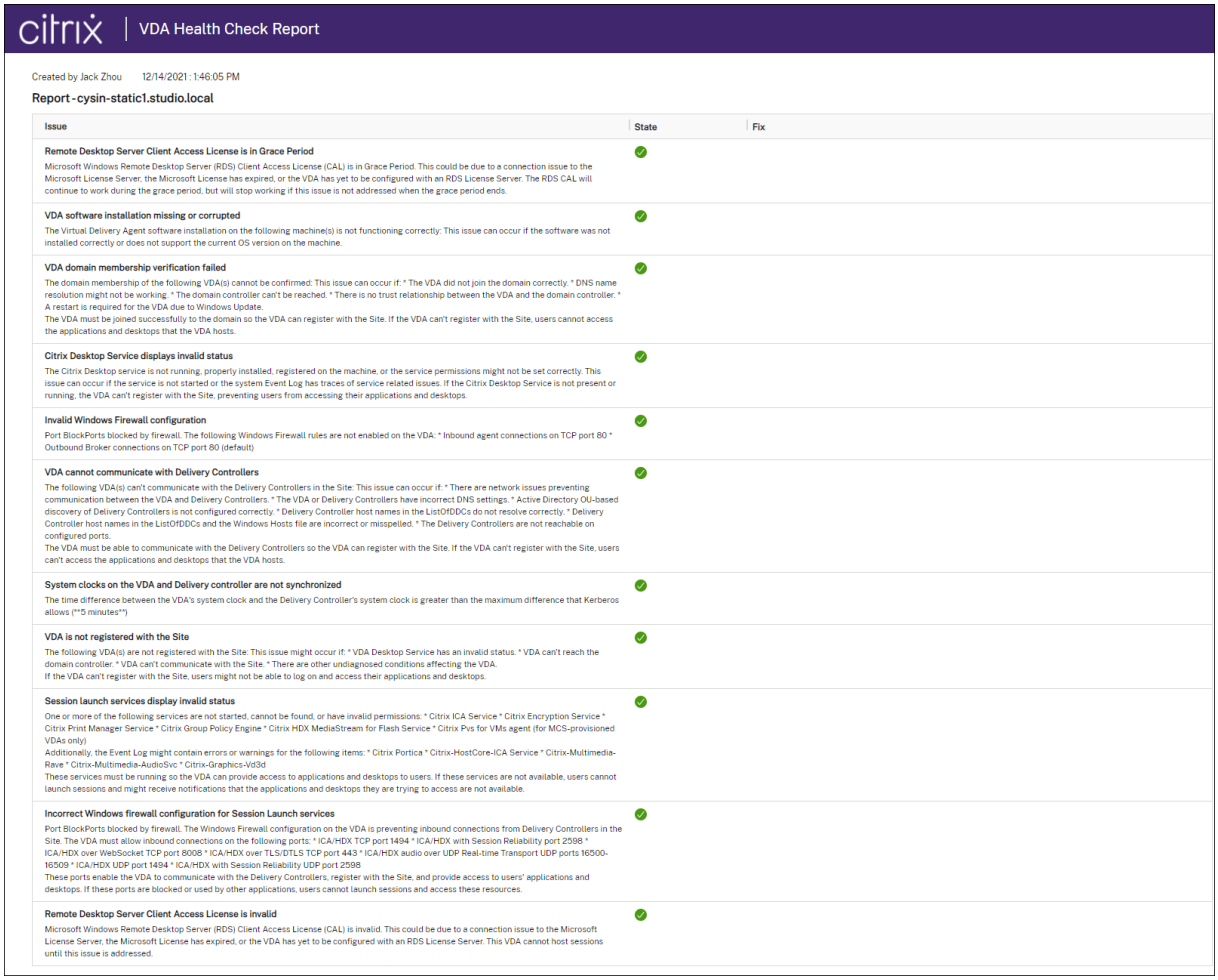
Depois que as verificações de integridade forem concluídas, os dois botões a seguir são exibidos: **View report** e **Close**. Para ver os resultados das verificações de integridade, clique em **View report**.



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 realizou as verificações de integridade
- As 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:**
>
> Quando executar verificações de integridade em lotes, selecione no máximo 10 máquinas. Caso contrário, a ação **Run Health Check** não estará disponível.

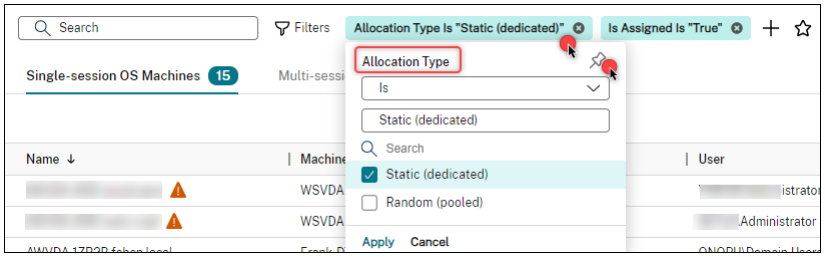
Usar a pesquisa na interface de gerenciamento Full Configuration

December 20, 2023

Introdução

Use o recurso de pesquisa Search para exibir informações sobre máquinas, sessões, catálogos de máquinas, aplicativos, grupos de entrega específicos e mais.
Em **Full Configuration > Search**, você tem várias opções:

- Use guias para listar máquinas por tipo (SO de sessão única ou multissessão) ou listar todas as sessões.
- Digite o nome na caixa de pesquisa para fazer uma pesquisa rápida sem aplicar filtros.
- Refine a pesquisa usando filtros.
  - Selecione **Match all** (operador AND) se quiser que a pesquisa retorne resultados que correspondam a todos os critérios do filtro. Selecione **Match any** (operador OR) se quiser que a pesquisa retorne resultados que correspondam a qualquer um dos critérios do filtro.
  - Selecione o ícone de filtros para abrir o painel de filtros. Você pode selecionar vários critérios de filtro no painel.
  - Clique no filtro para abrir o painel com o pino. Clique no ícone de **pino** para fixar o campo de filtro usado para a pesquisa. Você pode fixar os campos de filtro usados com frequência para facilitar a acessibilidade.



  - Salve seus filtros em uso clicando no símbolo da estrela. O item salvo é conhecido como filter set. Os itens salvos aparecem em **Saved filter sets** (para acessar a lista, selecione a caixa de pesquisa). Você pode clicar em um conjunto de filtros salvo para aplicar os filtros à sua pesquisa. Para excluir um conjunto de filtros salvo, passe o mouse sobre ele e selecione o ícone **X**. Para gerenciar conjuntos de filtros salvos, selecione **Manage**.

    > **Nota:**
    >
    > Os conjuntos de filtros são salvos por administrador, garantindo uma experiência de filtragem personalizada e adaptada a cada administrador.

Pesquisar sem filtros

Digite na caixa de pesquisa e pressione **Enter** para fazer uma pesquisa geral sem aplicar filtros.

Ao realizar uma pesquisa geral, o DaaS procura correspondências com os seguintes critérios e fornece resultados relevantes:

- **Name**. Pesquisa pelo nome de máquina ou nome DNS.
- **Machine Catalog**. Pesquisa pelo nome do catálogo da máquina.
- **Delivery Group**. Pesquisa pelo nome do grupo de entrega.
- **User**. Pesquisa pelo nome de usuário da sessão.
- **Client**. Pesquisa pelo nome do cliente da sessão.
- **VM**. Pesquisa pelo nome da máquina hospedada. É o nome amigável da máquina hospedada usada por seu hipervisor.
- **Hosting Server Name**. Pesquisa pelo nome do servidor de hospedagem.

Quando você pesquisa um item específico, como um usuário, grupo de área de trabalho, catálogo ou máquina, a pesquisa geral fornece uma maneira conveniente de encontrar as informações de que você precisa.

Pesquisar catálogos de máquinas ou grupos de entrega

Você pode pesquisar e localizar recursos nos nós de **catálogos de máquinas** e **grupos de entrega**. A funcionalidade de pesquisa nesses nós fornece a mesma interface do nó de **pesquisa**, fornecendo uma excelente experiência de pesquisa em todo o DaaS.

Você pode realizar pesquisas gerais e pesquisas baseadas em filtros. No nó **Machine Catalogs**, os seguintes filtros estão disponíveis:

- **Catalog Name**. Pesquisa pelo nome do Catálogo de Máquinas.
- **Allocation Type**. Filtra por alocação estática (dedicada) ou aleatória (em pool), ou ambas.
- **Provisioning Type**. Filtra por método de provisionamento manual ou MCS, ou ambos.
- **Session Support**. Filtra por máquina de sessão única ou multissessão, ou ambas.
- **Allocated Count**. Filtra pelo número de máquinas alocadas.
- **Persistence**. Filtra por alterações na máquina não persistentes (descarte) ou persistentes (no disco local), ou ambas.
- **Machine Type**. Filtra por tipo de máquina física ou virtual, ou ambos.

No nó **Delivery Groups**, os seguintes filtros estão disponíveis:

- **Group Name**. Pesquisa pelo nome do grupo de entrega.
- **Description**. Filtra pela descrição do grupo de entrega especificada durante a criação do grupo de entrega.
- **Session Support**. Filtra por máquina de sessão única ou multissessão, ou ambas.
- **Machine Identity**. Filtra pela identidade da máquina.
- **Remote PC Access**. Filtra por máquina com acesso ao PC remoto.

- **Maintenance mode**. Filtra por máquinas em modo de manutenção (ligado ou desligado, ou ambos).
- **Group State**. Filtra pelo estado do grupo. (A opção **Enable delivery group** em **Edit Delivery Group > User Settings** controla se a entrega de aplicativos e áreas de trabalho deve ser interrompida.)
- **Allocation Type**. Filtra por tipo estático (dedicado) ou aleatório (em pool), ou ambos.

Ao realizar uma pesquisa geral, o DaaS procura itens com base nos seguintes critérios e fornece resultados relevantes:

- **Machine Catalogs**:
  - Nome: pesquisa o catálogo de máquinas por nome, incluindo o caminho da pasta.
  - Catálogo de máquinas: pesquisa catálogos de máquinas por nome.
  - Descrição: pesquisa pela descrição do catálogo de máquinas especificada durante a criação do catálogo.
- **Delivery Groups**:
  - Nome do grupo de entrega: pesquisa grupos de entrega pelo nome.
  - Descrição: pesquisa pela descrição do grupo de entrega especificada durante a criação do grupo de entrega.

Personalizar colunas para exibir

Ao personalizar colunas, você pode ver as colunas marcadas com o rótulo **Degrades performance**. Selecionar essas colunas pode prejudicar o desempenho do console. Depois de concluir a personalização, a tabela é atualizada para exibir as colunas selecionadas. A presença delas pode resultar em atrasos quando você atualizar a tabela.

Se a personalização contiver colunas que degradam o desempenho, você será solicitado a determinar se deseja preservá-las. O aviso aparece depois que você atualiza a janela do navegador ou sai do console e volta a fazer login. Esteja ciente das seguintes considerações se decidir preservar as colunas:

- Para garantir o desempenho do console, você não pode atualizar a tabela mais de uma vez por minuto. Essa restrição se aplica a todas as guias: **Single-session OS Machines**, **Multi-session OS Machines** e **Sessions**. Se você precisar de atualizações mais frequentes, remova todas as colunas que prejudicam o desempenho.

Exportar resultados da pesquisa para um arquivo CSV

Você pode exportar os resultados da pesquisa (até 30,000 itens) para um arquivo CSV. O arquivo é salvo no local de download padrão do seu navegador.

Esse recurso está disponível para máquinas e sessões. Para exportar os resultados da pesquisa, clique no ícone de exportação no canto superior direito. A exportação pode levar alguns minutos para ser concluída.

Não é possível realizar outra exportação nas guias do nó Search enquanto uma exportação estiver em andamento.

Dicas para aprimorar uma pesquisa

Considere as dicas a seguir ao usar o recurso de pesquisa:

- No nó **Search**, selecione qualquer coluna para classificar os itens.
- Para mostrar mais características para incluir na exibição em que você pode pesquisar e classificar, selecione **Columns to Display** ou clique em qualquer coluna e selecione **Columns to Display**. Na janela **Columns to Display**, marque a caixa de seleção ao lado dos itens que deseja exibir e selecione **Save** para sair.

  > **Nota:**
  >
  > Os itens que degradam o desempenho são marcados com o rótulo **Degrades performance**.

- Para localizar um dispositivo de usuário conectado a uma máquina, use **Client (IP)** e **Is** e insira o endereço IP do dispositivo.
- Para localizar sessões ativas, use **Session State**, **Is** e **Connected**.
- Para listar todas as máquinas em um grupo de entrega, selecione **Delivery Groups** no painel esquerdo. Selecione o grupo e, em seguida, selecione **View Machines** na barra de ações ou no menu de contexto.

Tenha em mente as seguintes considerações ao realizar operações de classificação:

- Contanto que o número de itens não exceda 5.000, você pode clicar em qualquer coluna para classificar os itens nela. Quando o número excede 5.000, você pode classificar apenas por nome ou por usuário atual (dependendo da guia em que você está). Para ativar a classificação, use filtros para reduzir o número de itens para 5.000 ou menos.
- Quando o número de itens for maior que 500, mas não superior a 5.000:
  - Armazenamos todos os dados localmente em cache para melhorar o desempenho da classificação. Nas guias **Single-session OS Machines** e **Multi-session OS Machines**, armazenamos os dados em cache a primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Name**) para classificar. Na guia **Sessions**, armazenamos os dados em cache a primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna

Current User) 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 armazenados em cache: Last refreshed: <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.

O acesso do usuário

May 2, 2023

Há dois componentes principais que fornecem acesso a aplicativos e áreas de trabalho em uma implantação do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service):

- **Plataforma Citrix Workspace**: a plataforma Citrix Workspace é uma solução digital completa que permite fornecer acesso seguro a informações, aplicativos e outros conteúdos relevantes para a função de uma pessoa em sua organização. Os usuários assinam os serviços que você disponibiliza e podem acessá-los de qualquer lugar, em qualquer dispositivo. A plataforma Citrix Workspace ajuda a organizar e automatizar os detalhes mais importantes que seus usuários precisam para colaborar, tomar melhores decisões e se concentrar totalmente no trabalho.

  Não há grandes esforços para implantar o Citrix Workspace, e ele é mantido sempre funcional pela Citrix. A plataforma Citrix Workspace é recomendada para clientes novos e existentes, previews e provas de conceito.

- **Um StoreFront local**: os clientes também podem usar um StoreFront existente para agregar aplicativos e áreas de trabalho no Citrix Cloud. Esse caso de uso oferece maior segurança, incluindo suporte para autenticação de dois fatores, e impede que os usuários insiram suas senhas no serviço de nuvem. Também permite que os clientes personalizem seus nomes de domínio e URLs. Esse tipo de implantação é recomendado para qualquer cliente do Citrix Virtual Apps and Desktops que já tenha o StoreFront implantado.

  Consulte também Cache de host local e StoreFront.

Quando os usuários se conectam de fora do firewall corporativo, o Citrix Cloud pode usar a tecnologia Citrix Gateway (anteriormente NetScaler Gateway) para proteger essas conexões com SSL. O dispositivo virtual Citrix Gateway ou Citrix VPX é um dispositivo VPN SSL implantado na zona desmilitarizada (DMZ). Ele fornece um único ponto seguro de acesso através do firewall corporativo.

Usar o Citrix Workspace

O acesso aos espaços de trabalho é feito através de `https://<customername>.cloud.com`. Se necessário, você pode personalizar a parte `<customername>` do URL do espaço de trabalho. Em seguida, você pode configurar a conectividade para cada local de recurso que deseja usar, para que os usuários finais possam acessar os recursos em seus espaços de trabalho. Os usuários finais acessam seus espaços de trabalho usando a versão mais recente do aplicativo Citrix Workspace.

Para obter mais informações sobre como usar o Citrix Workspace, consulte:

- Configurar espaços de trabalho: para configurar o acesso e as personalizações.
- Proteger espaços de trabalho: para configurar a autenticação.
- Gerenciar sua experiência no espaço de trabalho: para entender como os usuários finais acessam seus espaços de trabalho e como se parecem.

Para fornecer acesso remoto aos usuários finais por meio do Citrix Workspace, você pode usar o serviço Citrix Gateway ou seu próprio Citrix Gateway.

- Para usar o serviço Citrix Gateway:

  1. Em **Citrix Cloud > Resource Locations**, selecione **Gateway** para o local do recurso que você deseja usar.
  2. Selecione **Gateway Service** e clique em **Save**.
  3. Em **Citrix Cloud > Workspace Configuration > Service Integrations**, localize o serviço Gateway e selecione **Enable** no menu de reticências.

- Para usar o seu próprio Citrix Gateway:

  1. Configure o Citrix Gateway como um proxy ICA (nenhuma autenticação ou políticas de sessão são necessárias).
  2. Configure um local de recursos para usar o Citrix Gateway:

     a) Em **Citrix Cloud > Resource Locations**, selecione **Gateway** para o local do recurso que você deseja usar.
     b) Selecione **Traditional Gateway** e insira o FQDN externo. Não adicione um protocolo. As portas são opcionais. O acesso remoto e interno combinados não é suportado no Citrix Workspace.

  3. Associe os Citrix Cloud Connectors como servidores Secure Ticket Authority (STA) ao Citrix Gateway. Para obter detalhes, consulte CTX232640.

     > **Nota:**
     >
     > Somente máquinas Citrix Cloud Connector são suportadas para uso como servidores STA com o Citrix Gateway. O uso de outros conectores como servidores STA, como o

> Connector Appliance, não é suportado.

Para obter mais informações sobre o serviço Citrix Gateway e o Citrix Gateway, consulte Citrix Gateway.

Usar um StoreFront local

Para obter informações sobre como configurar um StoreFront local, consulte a documentação do StoreFront.

Um benefício de usar um StoreFront existente é que o Citrix Cloud Connector fornece criptografia de senhas de usuário. O Cloud Connector criptografa credenciais usando o AES-256, usando uma chave de uso único gerada aleatoriamente. Essa chave é retornada diretamente para o aplicativo Citrix Workspace e nunca enviada para a nuvem. O aplicativo Citrix Workspace a fornece ao VDA durante o início da sessão para descriptografar as credenciais e fornecer uma experiência de logon único no Windows.

- Para transporte, selecione HTTP e porta 80. A máquina StoreFront deve ser capaz de acessar diretamente o Cloud Connector por meio do FQDN (nome de domínio totalmente qualificado) fornecido. O Cloud Connector deve ser capaz de acessar o URL do Cloud NFuse/STA em (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` e `ctxsta.dll`).
- Adicione Cloud Connectors como Delivery Controllers para alta disponibilidade.

Use a versão mais recente do StoreFront.

Acesso externo

Para fornecer acesso externo por meio do Citrix Gateway e do StoreFront local:

- Configure o Citrix Gateway normalmente, com políticas de autenticação e sessão. Consulte a documentação do Citrix Gateway para obter mais detalhes.
- Aponte os Delivery Controllers da sua loja StoreFront local para os Citrix Cloud Connectors. Associe os Cloud Connectors como servidores STA ao Citrix Gateway.
- O Citrix Gateway deve usar os mesmos URLs STA que o StoreFront. Se o gateway ainda não estiver configurado para usar o STA de um ambiente existente do Citrix Virtual Apps and Desktops, os Cloud Connectors poderão ser usados como STA.

Acesso interno

Para fornecer acesso interno por meio de um StoreFront local, aponte os Delivery Controllers da loja StoreFront local para os Citrix Cloud Connectors.

Acesso externo e interno

Para fornecer acesso externo e interno por meio do Citrix Gateway e do StoreFront local:

- Configure o Citrix Gateway normalmente, com políticas de autenticação e sessão. Consulte a documentação do Citrix Gateway para obter mais detalhes.
- Associe os Cloud Connectors como servidores STA ao Citrix Gateway.
- Aponte os Delivery Controllers da sua loja StoreFront local para os Cloud Connectors.

Cache de host local e StoreFront

O Cache de host local permite que as operações de intermediação de conexão em uma implantação do Citrix DaaS continuem quando os Cloud Connectors não podem se comunicar com o Citrix Cloud.

O recurso Cache de host local funciona somente em locais de recursos que contêm um StoreFront local implantado pelo cliente. O cache local do host não é suportado para uso com o Citrix Workspace.

Cada local de recurso deve ter um StoreFront local implantado pelo cliente. Verifique se o local do 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

June 24, 2022

> **Importante:**
>
> O Windows 10 Enterprise multissessão não suporta Virtualização IP de Área de Trabalho Remota (IP Virtual) e não oferecemos suporte a IP virtual nem loopback virtual em Windows 10 Enterprise multissessão.

Os recursos de IP virtual e loopback virtual são suportados em máquinas Windows Server 2016. Esses recursos não se aplicam a máquinas com SO Windows Desktop.

O recurso de endereço IP virtual da Microsoft fornece um aplicativo publicado com um endereço IP atribuído dinamicamente e exclusivo para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem das comunicações com o localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo do localhost (127.*).

Certos aplicativos, como CRM e Computer Telephony Integration (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros fins, e, portanto, exigem um endereço IP exclusivo ou um endereço de loopback nas sessões. Outros aplicativos podem se associar a uma porta estática, portanto, as tentativas de iniciar instâncias adicionais de um aplicativo em um ambiente multiusuário falharão porque a porta já está em uso. Para que esses 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 apenas um ou os dois.

Sinopse da ação do administrador:

- Para usar o IP virtual da Microsoft, ative-o e configure-o no Windows Server. (As configurações de política Citrix não são necessárias.)
- Para usar o loopback virtual do Citrix, configure dois parâmetros em uma política Citrix.

IP virtual

Quando o IP virtual está ativado e configurado no Windows Server, 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 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. Essa ferramenta lista todos os aplicativos que associam endereços IP específicos e portas.
2. Desative o recurso Resolver endereços IP para ver endereços em vez de 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 abrem essas portas.
4. Configure todos os processos que abrem o endereço IP de um 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 de Área de Trabalho Remota (RD) da Microsoft

- O endereçamento de IP virtual deve estar ativado no Microsoft Server.

Por exemplo, em um ambiente Windows Server 2016, a partir do Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões de Host da Sessão da Área de Trabalho Remota** para ativar a funcionalidade de Virtualização de IP de Área de Trabalho Remota e configurar as definições para atribuir endereços IP dinamicamente utilizando o servidor DHCP (Dynamic Host Configuration Protocol) por sessão ou por programa. Consulte a documentação da Microsoft para obter instruções.

- Depois que o recurso é ativado, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente a partir do servidor DHCP.
- O recurso de Virtualização de IP de Área de Trabalho Remota atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilham 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 para o 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 dentro da configuração de host da sessão de Área de Trabalho Remota, os aplicativos são associados a endereços IP específicos inserindo um componente "filter"entre as chamadas de função do aplicativo e do Winsock. Assim, o aplicativo vê apenas o endereço IP que deve usar. Qualquer tentativa do aplicativo de escutar as comunicações TCP ou UDP é associada automaticamente ao seu endereço IP virtual alocado (ou endereço de loopback), e todas as conexões de origem abertas pelo aplicativo se originam do endereço IP associado ao aplicativo.

Em funções que retornam um endereço (como `GetAddrInfo()`, que é controlada 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. Os aplicativos que tentam obter o endereço IP do servidor local através de tais funções de nome veem apenas o endereço IP virtual exclusivo atribuído à sessão. Esse endereço IP é frequentemente usado em chamadas subsequentes do soquete, tais como associação ou conexão. Para obter mais informações sobre as políticas do Windows, consulte RDS IP Virtualization in Windows Server.

Muitas vezes, um aplicativo solicita associar-se a uma porta para escuta 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 estão todos escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço IP virtual estiver ativado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentam se associar a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas são associadas a

VIPAddress1:9000 e VIPAddress2:9000, sem haver conflito.

Loopback virtual

Ativar as configurações de política de loopback de IP virtual da Citrix permite que cada sessão tenha o 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 de 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 octeto seguinte (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em um dos seguintes casos:

- O processo usa o endereço (localhost) de loopback do soquete do Windows (127.0.0.1)
- O processo usa um número de porta TCP codificado

Use as configurações de 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 do IP virtual, portanto, você não precisa configurar o servidor Microsoft.

- Suporte a loopback de IP virtual. Quando ativada, essa configuração de política permite que cada sessão tenha o seu próprio endereço de loopback virtual. Essa configuração é desativada por padrão. O recurso se aplica apenas a aplicativos especificados com a configuração de política de lista de programas de loopback virtual de IP virtual.
- Lista de programas de loopback virtual de IP virtual. Essa configuração de política especifica os aplicativos que usam o recurso de loopback de IP virtual. Essa configuração se aplica somente quando a configuração de política de suporte de 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, proceda com cautela:

- Use o loopback preferencial somente se o IP virtual e o loopback virtual estiverem ativados; caso contrário, você poderá ter resultados inesperados.
- Editar o registro incorretamente pode causar sérios problemas e exigir que você reinstale 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. Tenha o cuidado 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

December 20, 2023

Introdução

As implantações do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops) que abrangem locais amplamente dispersos conectados por uma WAN podem ter problemas com a latência e a confiabilidade da rede. O uso de zonas pode ajudar os usuários em regiões remotas a se conectarem aos recursos sem necessariamente forçar que as conexões atravessem grandes segmentos da WAN. No 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 áreas de trabalho mais próximos dos usuários, o que melhora o desempenho. 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 sobre a qual estamos falando. Por exemplo, "Um VDA se registra em um Cloud Connector local"significa que o VDA se registra em um Cloud Connector na zona onde o VDA está localizado.

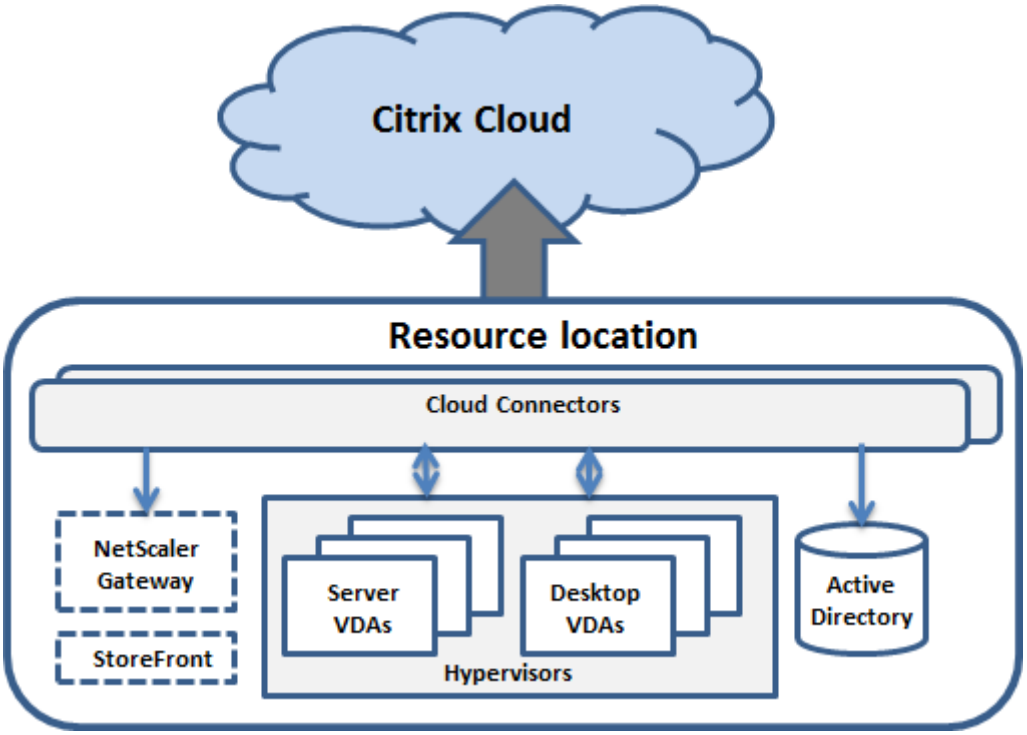
Diferenças das zonas em ambientes do Citrix Virtual Apps and Desktops no local

As zonas em um 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, um ambiente do 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, as zonas preferencial e de failover funcionam de forma diferente.

O que há em uma zona

Uma zona é equivalente a um local de recursos. Quando você cria um local de recurso e instala um Cloud Connector, uma zona é criada automaticamente para você. Cada zona pode ter um conjunto diferente de recursos, com base em suas necessidades e ambiente únicos.



Cada zona deve sempre ter pelo menos um Cloud Connector, mas, de preferência, dois ou mais, para redundância.

Você pode colocar catálogos de máquinas, hipervisores, conexões de host, usuários e aplicativos em uma zona. Uma zona também pode conter servidores Citrix Gateway e StoreFront. Para usar o recurso Cache de host local, uma zona deve ter um servidor StoreFront.

As zonas são suportadas no Citrix Workspace e no serviço Citrix Gateway.

Colocar itens em uma zona afeta a forma como o Citrix DaaS interage com eles e com outros objetos relacionados a eles.

- Quando uma conexão de hipervisor é colocada em uma zona, pressupõe-se que todos os hipervisores gerenciados por essa conexão também residam nessa zona.
- Quando um catálogo de máquina é colocado em uma zona, pressupõe-se que todos os VDAs no catálogo estejam na zona.
- As instâncias do Citrix Gateway podem ser adicionadas às zonas. Quando você cria um local de recurso, lhe é oferecida a opção de adicionar um Citrix Gateway. Quando um Citrix Gateway está associado a uma zona, é preferível que ele seja usado quando são usadas conexões a máquinas VDA nessa zona.

- O ideal é que o Citrix Gateway em uma zona seja usado para conexões de usuários que entram nessa zona a partir de outras zonas ou localizações externas. Você também pode usá-lo para conexões dentro da zona.
- Depois de criar mais locais de recursos e instalar o Cloud Connectors neles (o que cria automaticamente mais zonas), você pode mover recursos entre zonas. Essa flexibilidade vem acompanhada do risco de separar itens que funcionam melhor quando próximos. 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 indesejados antes de mover os itens entre as 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 de Cache de host local permitirá que um Cloud Connector na zona continue intermediando conexões com VDAs naquela zona. (A zona deve ter o StoreFront instalado.) Por exemplo, isso é eficaz em um escritório em que os funcionários 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 são registrados

Os VDAs devem ter, no mínimo, a versão 7.7 para usar esses recursos de registro de zona:

- Um VDA em uma zona é registrado em um Cloud Connector local.
  - Enquanto o Cloud Connector puder se comunicar com o Citrix Cloud, as operações normais continuarão.
  - Se o 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 Cache de host local.
  - Se um Cloud Connector falhar, os VDAs nessa zona tentarão se registrar em outros Cloud Connectors locais. Um VDA em uma zona nunca tenta se registrar em 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 ativada, os VDAs nessa zona receberão listas atualizadas dos Cloud Connectors locais disponíveis, para que eles saibam com quem podem se registrar e de quem aceitar conexões.
- Se você mover um catálogo de máquina para outra zona (usando a interface de gerenciamento Full Configuration), os VDAs nesse catálogo serão registrados novamente nos Cloud Connectors na zona para a qual o catálogo foi movido. Ao mover um catálogo, certifique-se de mover também as conexões de host associadas para a mesma zona.
- Durante uma interrupção (quando os Cloud Connectors em uma zona não podem se comunicar com o Citrix Cloud), somente os recursos associados às máquinas registradas nessa zona ficam disponíveis.

Preferência de zona

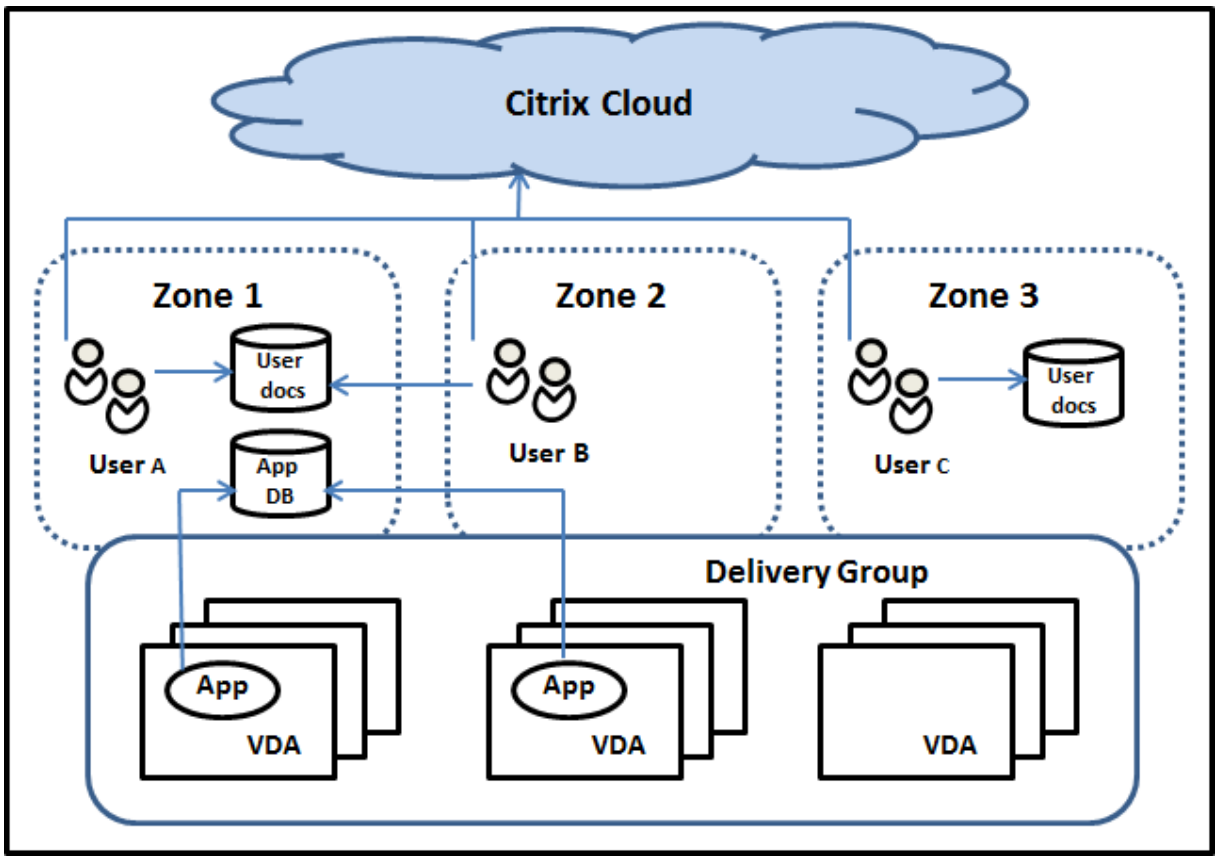
Em um site de várias zonas, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou área de trabalho.

Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma determinada zona com base em:

- Onde os dados do aplicativo são armazenados. Essa é a origem do aplicativo.
- A localização dos dados de origem do usuário, como um perfil ou compartilhamento. Essa é a origem do usuário.
- O local atual do usuário (onde o aplicativo Citrix Workspace está sendo executado). Essa é a localização do usuário. A localização do usuário requer, no mínimo, o StoreFront 3.7 e o Citrix Gateway (anteriormente NetScaler Gateway) 11.0-65.x.

O gráfico a seguir mostra um exemplo de configuração de várias zonas.



Neste exemplo, os VDAs estão distribuídos entre três zonas, mas estão todos no mesmo grupo de entrega. Portanto, o agente do Citrix DaaS pode ter a opção de qual VDA usar para uma solicitação de

inicialização do usuário. Este exemplo ilustra que os usuários podem estar executando seus pontos de extremidade do aplicativo Citrix Workspace em locais diferentes. 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 locais diferentes. 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 de origem para o usuário ou aplicativo. O agente usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se os recursos estiverem disponíveis. Você:

- Configura a zona de origem de um usuário adicionando um usuário a uma zona.
- Configura a zona de origem de um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona de origem por vez. (Pode ocorrer uma exceção a usuários quando várias associações de zona ocorrem devido à associação a grupos de usuários. No entanto, mesmo nesse caso, o agente usa apenas uma zona de origem.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o agente seleciona apenas uma zona preferencial para uma inicialização. A ordem de prioridade padrão para selecionar a zona preferencial é: origem do aplicativo > origem do usuário > localização do usuário. Quando um usuário inicia um aplicativo:

- Se o aplicativo tiver uma associação de zona configurada (uma origem de aplicativo), a zona preferencial é a zona de origem do aplicativo.
- Se o aplicativo não tiver uma associação de zona configurada, mas o usuário tiver (uma origem de usuário), a zona preferencial é a zona de origem desse usuário.
- Se nem o aplicativo nem o usuário tiverem uma associação de zona configurada, a zona preferencial será a zona em que o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, será usada uma seleção aleatória de VDA e zona. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver uma zona preferencial, o balanceamento de carga será aplicado a todos os VDAs no grupo de entrega.

Adaptar as preferências de zona

Quando você configura (ou remove) uma zona de origem para um usuário ou um aplicativo, você também pode restringir como a preferência de zona é (ou não é) usada.

- **Uso obrigatório da zona de origem do usuário:** em um grupo de entrega, você pode especificar "Launch the session in the user's home zone (if the user has a home zone), with no failover to a different zone if resources are not available in the home zone". Essa restrição é útil para

evitar o risco de copiar grandes perfis ou arquivos de dados entre zonas. Em outras palavras, você prefere negar um início de sessão a iniciar a sessão em uma zona diferente.

- **Uso obrigatório da zona de origem do aplicativo:** da mesma forma, quando você configura uma zona de origem para um aplicativo, você pode especificar: "launch the application only in that zone, with no failover to a different zone if resources are not available in the application's home zone".
- **Sem zona de origem do aplicativo, e ignora a zona de origem do usuário configurada:** se você não especificar uma zona de origem para um aplicativo, também pode especificar "do not consider any configured user zones when launching that application". Por exemplo, use a preferência de zona de localização do usuário se quiser que os usuários executem um aplicativo específico em um VDA próximo à máquina, mesmo que alguns usuários tenham uma zona de origem diferente.

Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia um aplicativo ou área de trabalho, o agente prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário iniciando um aplicativo ou área de trabalho já tem uma sessão adequada para o recurso que está sendo iniciado (por exemplo, que pode usar compartilhamento de sessão para um aplicativo, ou uma sessão que já está executando o recurso sendo iniciado), mas essa sessão está em um VDA em uma zona diferente da zona preferencial do usuário/aplicativo, o sistema pode criar uma nova sessão. Essa ação permite o início na zona correta (se tiver capacidade disponível), antes de se reconectar a uma sessão em uma zona menos preferida para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não possa mais ser acessada, a reconexão é permitida às sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem preferencial para o início das sessões é:

1. Reconectar-se a uma sessão existente na zona preferencial.
2. Reconectar-se a uma sessão desconectada existente em uma zona não preferencial.
3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar-se a uma sessão existente conectada em uma zona não preferencial.
5. Iniciar uma nova sessão em uma zona não preferencial.

Outras considerações de preferência de zona

- Se você configurar uma zona de origem 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 um membro de vários grupos de segurança

e, portanto, pode ter uma zona de origem diferente configurada por meio de outra associação de grupo. Nesses casos, a determinação da zona de origem desse usuário pode ser ambígua.

Se um usuário tem uma zona de origem configurada que não foi adquirida através da associação de grupo, essa zona é usada para a preferência de zona. Todas as associações de zona adquiridas por meio da associação de grupo são ignoradas.

Se o usuário tem várias associações de zonas diferentes adquiridas exclusivamente por meio da associação ao grupo, o agente escolhe entre as zonas aleatoriamente. Depois que o agente faz essa escolha, a zona é usada para inícios de sessão subsequentes, até que a associação do grupo do usuário mude.

- A preferência da zona de localização do usuário exige a detecção do aplicativo Citrix Workspace no dispositivo de ponto de extremidade pelo Citrix Gateway através do qual o dispositivo está se conectando. O Citrix deve ser configurado para associar intervalos de endereços IP a zonas específicas. A identidade da zona detectada deve ser passada para o Citrix DaaS através do StoreFront.

Embora tenha sido escrito para uso local de zonas, a postagem 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 a 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 usar o Citrix Provisioning: o console Citrix Provisioning atual não reconhece as zonas, portanto, a Citrix recomenda usar a interface **Manage > Full Configuration** para criar os catálogos de máquinas que você deseja colocar em zonas específicas. Depois de criar o catálogo, você pode usar o console Citrix Provisioning para provisionar máquinas no catálogo.

Criação de zona

Quando você cria um local de recursos no Citrix Cloud e adiciona um Cloud Connector a esse local de recursos, o Citrix DaaS cria e nomeia automaticamente uma zona. Opcionalmente, você pode adicionar uma descrição mais tarde.

Depois de criar mais de um local de recursos (e as zonas serem criadas automaticamente), você pode mover os recursos de uma zona para outra.

Os locais de recursos e as zonas são sincronizados periodicamente, normalmente a cada cinco minutos, aproximadamente. Portanto, se você alterar o nome de um local de recursos no Citrix Cloud, essa alteração é propagada para a zona associada em cinco minutos.

Adicionar ou alterar a descrição de uma zona

Embora não seja possível alterar o nome de uma zona, você pode adicionar ou alterar a sua descrição.

1. Em **Manage > Full Configuration**, selecione **Zones** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione **Edit Zone** na barra de ações.
3. Adicione ou altere a descrição da zona.
4. Selecione **OK** ou **Apply.**

Mover recursos de uma zona para outra zona

1. Em **Manage > Full Configuration**, selecione **Zones** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione um ou mais itens.
3. Arraste os itens para a zona de destino ou selecione **Move Items** na barra de ações e 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 a um hipervisor ou serviço de nuvem, confirme que o catálogo e a conexão estão 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 recursos (depois de remover os seus Cloud Connectors). A exclusão do local do recursos 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, ela será excluída automaticamente depois que todos os itens forem removidos.

Adicionar uma zona de origem para um usuário

Configurar a zona de origem de um usuário é o mesmo que *adicionar um usuário a uma zona*.

1. Em **Manage > Full Configuration**, selecione **Zones** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione **Add Users to Zone** na barra de ações.
3. Na caixa de diálogo **Add Users to Zone**, selecione **Add** e selecione os usuários e grupos de usuários a serem adicionados à zona. Se você especificar usuários que já têm uma zona de origem, uma mensagem oferece duas opções: **Yes** = adicionar apenas os usuários que você especificou que não têm uma zona de origem; **No** = retornar à caixa de diálogo de seleção do usuário.
4. Selecione **OK**.

Para usuários com uma zona de origem configurada, você pode exigir que as sessões sejam iniciadas somente a partir de sua zona de origem:

1. Crie ou edite um grupo de entrega.
2. Na página **Users**, marque a caixa de seleção **Sessions must launch in a user's home zone, if configured**.

Todas as sessões iniciadas por um usuário nesse grupo de entrega devem ser iniciadas a partir de máquinas na zona de origem desse usuário. Se um usuário no grupo de entrega não tiver uma zona de origem configurada, esse parâmetro não terá efeito.

Remover uma zona de origem de um usuário

Este procedimento é o mesmo que remover um usuário de uma zona.

1. Em **Manage > Full Configuration**, selecione **Zones** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione **Remove Users from Zone** na barra de ações.
3. Na caixa de diálogo **Add Users to Zone**, selecione **Remove** e selecione os usuários e grupos a serem removidos da zona. Essa ação remove os usuários somente da zona. Esses usuários permanecem nos grupos de entrega aos quais pertencem.
4. Confirme a remoção quando solicitado.

Gerenciar zonas de origem para aplicativos

Configurar a zona de origem de um aplicativo é o mesmo que adicionar um aplicativo a uma zona. Por padrão, em um ambiente de várias zonas, um aplicativo não tem uma zona de origem.

A zona de origem 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 **Properties** na página **Applications** do assistente.
- Para alterar as propriedades de um aplicativo depois que o aplicativo for adicionado, selecione **Zones** no painel esquerdo. Selecione um aplicativo e, em seguida, selecione **Properties** na barra de ações.

Na página **Zones** das propriedades/configurações do aplicativo:

- Se quiser que o aplicativo tenha uma zona de origem:
  - Selecione o botão de opção **Use the selected zone to decide** e selecione a zona.
  - Se quiser que o aplicativo seja iniciado apenas a partir da zona selecionada (e não de outras zonas), marque a caixa de seleção na área de seleção de zona.
- Se não quiser que o aplicativo tenha uma zona de origem:
  - Selecione o botão de opção **Do not configure a home zone**.
  - Se você não quiser que o agente considere nenhuma zona de usuário configurada ao iniciar o aplicativo, marque a caixa de seleção sob o botão de opção. Nesse caso, não serão usadas zonas de origem do aplicativo nem do usuário para determinar onde iniciar o 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 é selecionado alfabeticamente.

Solução de problemas

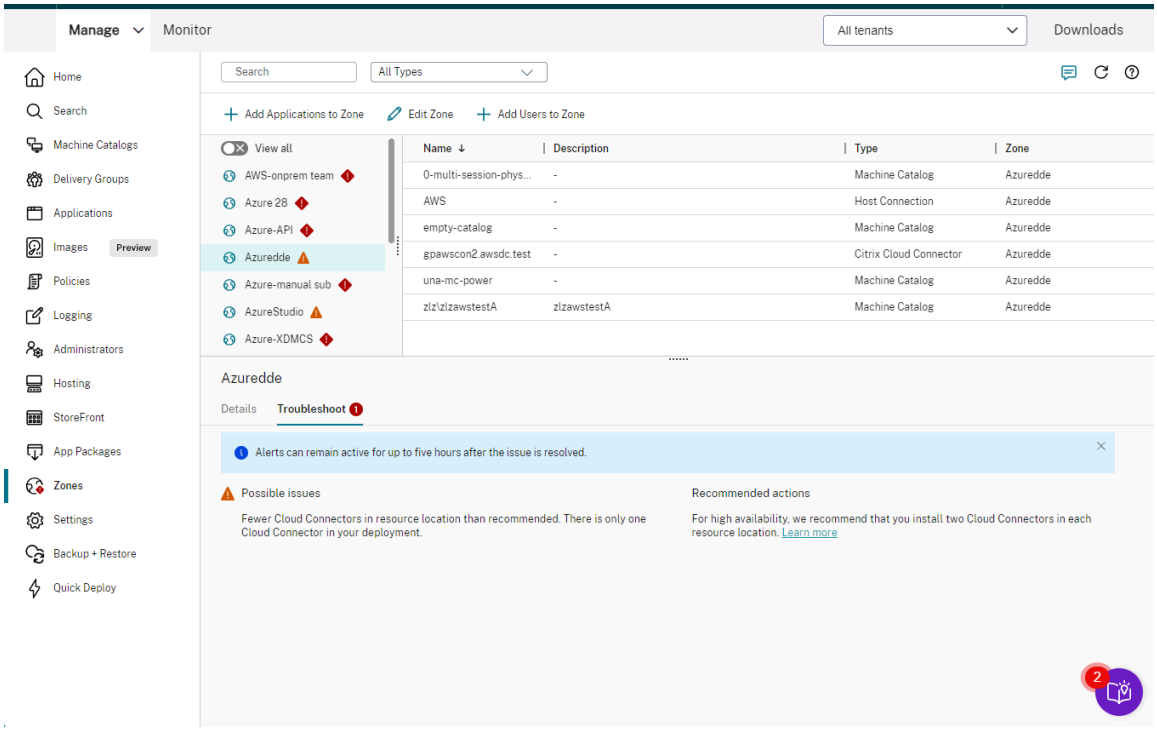
Full Configuration fornece alertas proativos para garantir que o cache do host local e as zonas estejam configurados corretamente para que você possa resolver os problemas a tempo antes que uma interrupção afete seus usuários. Esse recurso ajuda a manter o acesso contínuo do usuário às cargas de trabalho essenciais.

A guia **Troubleshoot** é exibida para cada zona com problemas.

Para verificar problemas relacionados à zona, siga estas etapas:

1. Vá para **Full Configuration > Zones** e clique na zona com o ícone de aviso.
2. Vá para a guia **Troubleshoot** no painel inferior e leia as informações exibidas.

> **Nota:**
>
> Os diagnósticos são atualizados de hora em hora.
>
> Exemplo de informações de solução de problemas:



A tabela a seguir fornece uma lista completa de avisos e erros relacionados à zona:

Gravidade	Título do problema	Descrição do problema	Ação recomendada
Aviso	O local de recursos contém vários domínios	Com vários domínios em um local de recursos, se as relações de confiança não estiverem configuradas corretamente, poderá levar mais tempo para que os VDAs se registrem. Além disso, os VDAs podem não se registrar no modo de alta disponibilidade.	Certifique-se de que as relações de confiança entre domínios nesse local de recursos estejam configuradas corretamente. Consulte os detalhes técnicos do Citrix Cloud Connector.

Gravidade	Título do problema	Descrição do problema	Ação recomendada
Aviso	Mais conexões de host no local de recursos do que o recomendado	Exceder o limite pode resultar na degradação do desempenho, afetando a experiência do usuário.	Reduza o número de conexões de host nesse local de recursos para não mais do que o limite recomendado. Consulte Limites.
Aviso	Menos processadores lógicos de CPU do que o recomendado	No modo de alta disponibilidade, pode haver degradação do desempenho.	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos do processador lógico da CPU. Consulte Cache do host local.
Aviso	Menos Cloud Connectors no local de recursos do que o recomendado	Há apenas um Cloud Connector em sua implantação.	Para alta disponibilidade, recomendamos que você instale dois conectores de nuvem em cada local de recursos. Consulte os detalhes técnicos do Citrix Cloud Connector.
Erro	Mais VDAs no local de recursos do que o recomendado	No modo de alta disponibilidade, o Cache de Host Local permite que somente 10.000 VDAs se registrem. As tentativas de registro por VDAs adicionais falharão.	Reduza o número de VDAs nesse local de recursos para não mais do que o limite recomendado. Consulte Limites.

Gravidade	Título do problema	Descrição do problema	Ação recomendada
Erro	Os Cloud Connectors na zona estão inacessíveis.	Nenhum dos Cloud Connectors na zona pode ser acessado. Os VDAs nesse local de recurso podem não estar disponíveis, a menos que o cache do host local ou a continuidade do serviço estejam configurados para sua implantação.	Analise a conectividade dos Cloud Connectors na zona e verifique o registro para confirmar se o modo LHC é forçado pelo registro ou não. Se o registro não forçar o LHC, considere executar o Cloud Connector Connectivity Check Utility. Se o problema persistir, abra um tíquete de suporte.

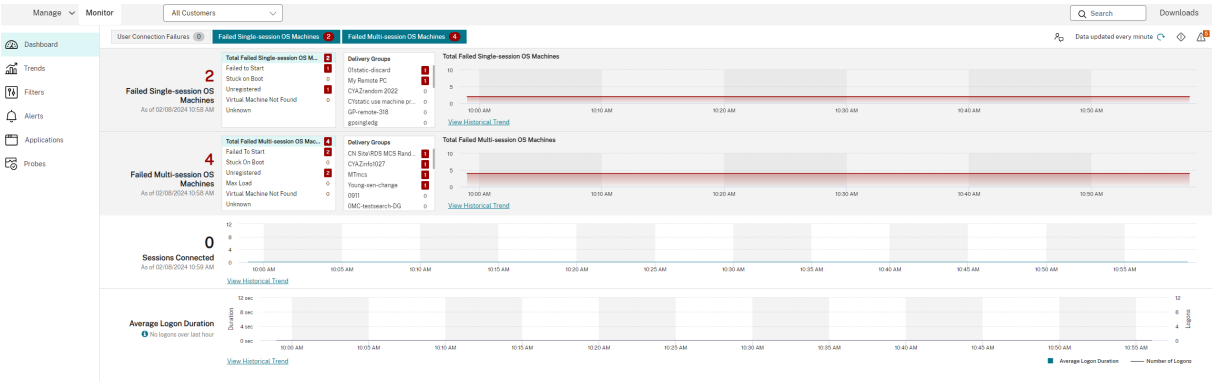
Monitoramento

June 24, 2022

Os administradores e a equipe de suporte técnico podem monitorar o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) a partir do **Monitor**, o console de monitoramento e solução de problemas. A guia **Monitor** exibe 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 da versão atual do Citrix Virtual Apps and Desktops e implantações LTSR.

Para acessar o **Monitor**, faça login no Citrix Cloud. No menu superior esquerdo, selecione **My Services > DaaS**. Clique em **Monitor**.



> **Nota:**
>
> A resolução de tela ideal recomendada para visualização do Monitor é 1366 x 1024.

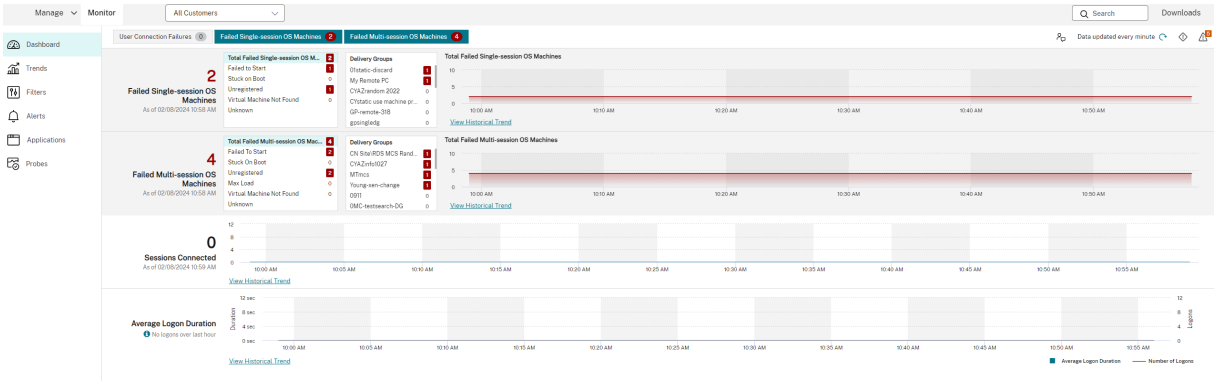
O monitor fornece:

- Dados em tempo real do Broker Agent por meio de um console unificado integrado ao Analytics e Performance Manager.
- O Analytics inclui gerenciamento de desempenho para garantia de integridade e capacidade e tendências históricas para identificar gargalos no seu ambiente Citrix DaaS.
- Dados históricos armazenados no banco de dados do Monitor para acessar o banco de dados de log de configuração.
- Obter visibilidade da experiência do usuário final para aplicativos virtuais, desktops e usuários do Citrix DaaS.
- O Monitor usa um painel de solução de problemas que fornece monitoramento de integridade histórico e em tempo real do Citrix DaaS. Esse recurso permite que você veja falhas em tempo real, dando uma ideia melhor do que os usuários finais estão passando.

Análise do site

January 17, 2023

O painel Monitor fornece um local centralizado para monitorar a integridade e o uso de um site.



Se não houver falhas no momento e não tiver ocorrido nenhuma falha nos últimos 60 minutos, os painéis permanecem recolhidos. Quando há falhas, o painel de falhas específico aparece automaticamente.

Painel	Descrição
Falhas de conexão do usuário, em User Connection Failures	Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para exibir as métricas desse tipo de falha. Na tabela adjacente, esse número é dividido por grupos de entrega. As falhas de conexão incluem falhas causadas por atingir os limites dos aplicativos. Para obter mais informações sobre os limites de aplicativos, consulte Aplicativos.
Máquinas com SO de sessão única com falha, em Failed Single session OS Machines, ou máquinas com SO multissessão com falha, em Failed Multi-session OS Machines	Total de falhas nos últimos 60 minutos divididos por grupos de entrega. Falhas divididas por tipos, incluindo falhas na inicialização em Failed to Start, bloqueios na inicialização, em Stuck on Boot, e cancelamentos de registro, em Unregistered. Para máquinas com SO multissessão, as falhas também incluem máquinas que atingem a carga máxima.
Sessões conectadas, em Sessions Connected	Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.

Duração média de logon, em Average Logon Duration	Dados de logon nos últimos 60 minutos. O número grande à esquerda é a duração média de logons durante o intervalo de hora. Os dados de logon de VDAs anteriores ao XenDesktop 7.0 não estão incluídos nessa média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

> **Nota:**
>
> Se nenhum ícone aparecer para uma métrica específica, isso indica que a métrica não é suportada pelo tipo de host que você está usando. Por exemplo, nenhuma informação de integridade está disponível para hosts do System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

Continue a corrigir os problemas usando estas opções (que estão documentadas abaixo):

- Controlar a energia da máquina do usuário
- Prevenir conexões a máquinas

Monitorar sessões

Se uma sessão for desconectada, ela permanece ativa e seus aplicativos continuam em execução, mas o dispositivo do usuário não se comunica mais com o servidor.

Ação	Descrição
Ver a máquina ou sessão conectada de um usuário no momento	Nas exibições Activity Manager e User Details, veja a máquina ou sessão conectada do usuário no momento e uma lista de todas as máquinas e sessões às quais o usuário tem acesso. Para acessar essa lista, clique no ícone do seletor de sessão na barra de título do usuário. Para obter mais informações, consulte Restaurar sessões.

Ação	Descrição
Ver o número total de sessões conectadas em todos os grupos de entrega	Em Dashboard, no painel **Sessions Connected**, veja o número total de sessões conectadas em todos os grupos de entrega nos últimos 60 minutos. Clique no número total grande, que abre a exibição Filters, onde você pode exibir dados gráficos da sessão baseados em grupos de entrega selecionados e intervalos e uso entre os grupos de entrega.
Encerrar sessões ociosas	A exibição Sessions Filters mostra dados relacionados a todas as sessões ativas. Filtre as sessões por 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 logoff ou desconexão. Para obter mais informações, consulte Solucionar problemas de aplicativos.
Ver dados de um período mais longo	Na exibição Trends, selecione a guia **Sessions** para ver dados de uso detalhados e mais específicos das sessões conectadas e desconectadas durante um período de tempo mais longo (ou seja, totais das sessões anteriores aos últimos 60 minutos). Para ver essas informações, clique em **View historical trends**.

> **Nota:**
>
> Se o dispositivo do usuário estiver executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7 ou um Linux VDA, o Monitor não consegue exibir as informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem informando que as informações não estão disponíveis.

Limitação das regras de atribuição de área de trabalho:
O console Manage permite a atribuição de várias regras de atribuição de área de trabalho (DAR) de diferentes usuários ou grupos de usuários para um único VDA no grupo de entrega. O StoreFront exibe a área de trabalho atribuída com o **nome de exibição** correspondente de acordo com o DAR do usuário conectado. No entanto, o Monitor não oferece suporte a regras DAR e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário conectado. Como resultado, você não pode mapear uma área de trabalho específica a uma máquina no Monitor.

Você pode mapear a área de trabalho atribuída exibida no StoreFront para o nome do grupo de entrega exibido no Monitor usando o seguinte comando do PowerShell. Execute o comando do 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
```

Desativar a visibilidade de aplicativos em execução no Activity Manager

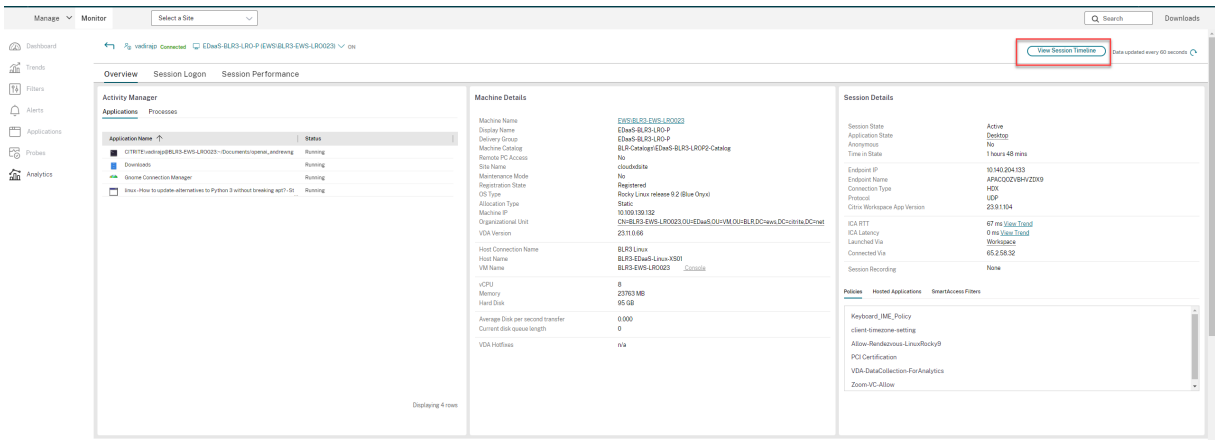
Por padrão, o Activity Manager exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Essas informações podem ser visualizadas por todos os administradores que têm acesso ao recurso Activity Manager. Para funções de administrador delegado, inclui administrador completo, administrador de grupo de entrega e administrador de assistência técnica.

Para proteger a privacidade dos usuários e os aplicativos que estão executando, você pode desativar a guia Applications para listar aplicativos em execução. Para isso, no VDA, modifique a chave de 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 Activity Manager.

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Acesso ao Citrix Analytics for Performance –Detalhes da sessão

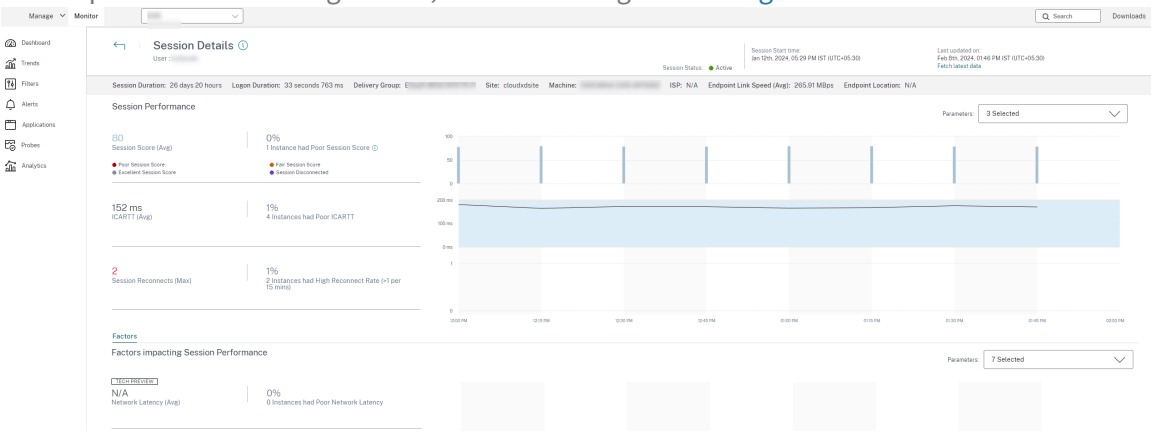
A página Session Details do Citrix Analytics for Performance pode ser acessada em Monitor. Clicar em **View Session Timeline** na seção Sessions Details de Activity Manager abre a página Sessions Details do Citrix Analytics for Performance em Monitor.



Nota:

Esse recurso exige que você tenha um direito válido do Citrix Analytics for Performance.

Session Details está disponível para sessões categorizadas como Excellent, Fair ou Poor no Citrix Analytics for Performance. Para obter mais informações sobre os motivos pelos quais uma sessão pode não estar categorizada, consulte o artigo Não categorizado.

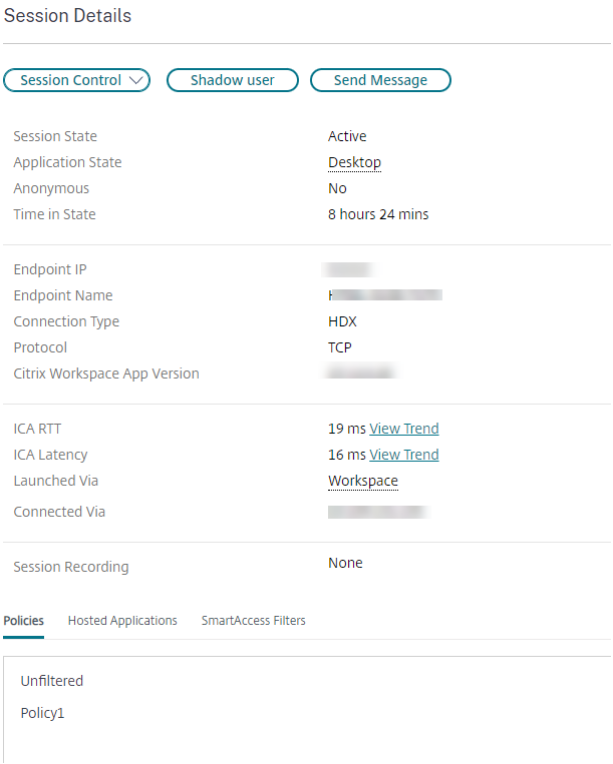


Você pode ver uma tendência da experiência da sessão até os últimos três dias, juntamente com os fatores que contribuem para a experiência da sessão. Essas informações complementam os dados disponíveis em Monitor em tempo real usados pelo administrador do suporte técnico para solucionar problemas relacionados à experiência da sessão.

Para obter mais informações sobre a página Session Details, consulte Detalhes da sessão.

Protocolo de transporte de sessão

Veja o protocolo de transporte em uso para o tipo de conexão HDX da sessão atual no painel **Session Details**. Essas informações estão disponíveis para sessões iniciadas em VDAs versão 7.13 ou posteriores.



Use o menu suspenso Session Control, no painel **Session Details**, para fazer logoff ou desconectar uma sessão.

- Para o tipo de conexão **HDX**:
  - O protocolo é exibido como **UDP**, se EDT for usado para a conexão HDX.
  - O protocolo é exibido como **TCP**, se 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 de sessão se alterna dinamicamente entre EDT (por UDP) e TCP com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ocorre o fallback para o protocolo TCP.

Para obter mais informações sobre a configuração de transporte adaptativo, consulte Transporte adaptativo.

Exportar relatórios

Você pode exportar dados de tendências para gerar relatórios regulares de gerenciamento de capacidade e uso. A exportação oferece suporte aos formatos de relatório PDF, Excel e CSV. Relatórios nos formatos PDF e Excel contêm tendências representadas como gráficos e tabelas. Os relatórios em formato CSV contêm dados tabulares que podem ser processados para gerar exibições ou para arquivamento.

Para exportar um relatório:

1. Vá para a guia **Trends**.
2. Defina os critérios de filtro e o período de tempo e clique em **Apply**. A tabela e o gráfico de tendências são preenchidos com os dados.
3. Clique em **Export** e insira o nome e o formato do relatório.

O Monitor gera o relatório com base nos critérios de filtro selecionados. Se você alterar os critérios de filtro, clique em **Apply** antes de clicar em **Export**.

> **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 em SQL Servers. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados são definidos a limites padrão para alcançar o desempenho de exportação ideal.

Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos dos critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados se ultrapassam os limites padrão de 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 **Sessions**)

Tratamento de erros

Erros que você pode encontrar durante uma operação de exportação:

- **Director has timed out:** esse erro pode ocorrer devido a problemas de rede ou alto uso de recursos do servidor do Director ou Monitor Service.
- **Monitor has timed out:** esse erro pode ocorrer devido a problemas de rede ou alto uso de recursos do Monitor Service ou SQL Server.
- **Max concurrent Export or Preview operations ongoing:** apenas uma instância de Export ou Preview pode ser executada em um momento específico. Se você receber o erro **Max concurrent Export or Preview operations ongoing**, tente refazer a operação seguinte mais tarde.

Monitorar hotfixes

Para ver os hotfixes instalados no VDA de uma máquina específica (física ou VM), escolha a exibição **Machine Details**.

Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas selecionadas no Monitor, use as opções de controle de energia. Essas opções estão disponíveis para máquinas com SO de sessão única, mas podem não estar disponíveis para máquinas com SO multissessão.

> **Nota:**
>
> Essa funcionalidade não está disponível para máquinas físicas ou máquinas que usam o Remote PC Access.

Comando	Função
Restart	Executa o desligamento ordenado (suave) da máquina virtual, e todos os processos em execução são interrompidos individualmente antes de reiniciar a máquina virtual. Por exemplo, selecione máquinas que aparecem no Monitor com o erro “failed to start”e use esse comando para reiniciá-las.
Force Restart	Reinicia a máquina virtual sem executar nenhum procedimento de desligamento primeiro. Esse comando funciona da mesma forma que desconectar o cabo de um servidor físico, reconectá-lo em seguida e ligar o servidor novamente.
Shut Down	Executa o desligamento ordenado (suave) da máquina virtual. Todos os processos em execução são interrompidos individualmente.

Comando	Função
Force Shutdown	Desliga a máquina virtual sem executar nenhum procedimento de desligamento primeiro. Esse comando funciona da mesma forma que desconectar o cabo de um servidor físico. Porém, nem sempre os processos em execução são encerrados e você corre o risco de perder dados se encerrar uma máquina virtual dessa maneira.
Suspend	Suspende uma máquina virtual em execução em seu estado atual e armazena o estado em um arquivo no repositório de armazenamento padrão. Essa opção permite que você desligue o servidor host da máquina virtual e, posteriormente, após reinicializá-lo, retome a máquina virtual, retornando-a ao seu estado de execução original.
Resume	Retoma uma máquina virtual suspensa e restaura seu estado de execução original.
Start	Inicia uma máquina virtual quando ela está desligada (também chamada de inicialização a frio).

Se as ações de controle de energia falharem, passe o mouse sobre o alerta e uma mensagem pop-up aparece com detalhes sobre a falha.

Prevenir conexões a máquinas

Use o modo de manutenção para evitar novas conexões temporariamente enquanto o administrador apropriado executa tarefas de manutenção na imagem.

Quando você ativa o modo de manutenção em máquinas, nenhuma nova conexão é permitida até você desativá-lo. Se os usuários estiverem conectados no momento, o modo de manutenção entrará em vigor assim que todos os usuários estiverem desconectados. Para usuários que não fizerem logoff, envie uma mensagem informando que as máquinas serão desligadas em um determinado momento e use os controles de energia para forçar as máquinas a desligarem.

1. Selecione a máquina, como, por exemplo, na exibição User Details, ou um grupo de máquinas na exibição Filters.
2. Selecione **Maintenance Mode** e ative a opção.

Se um usuário tentar se conectar a uma área de trabalho atribuída enquanto estiver no modo de manutenção, será exibida uma mensagem indicando que a área de trabalho não está disponível no momento. Nenhuma nova conexão pode ser feita até que você desative o modo de manutenção.

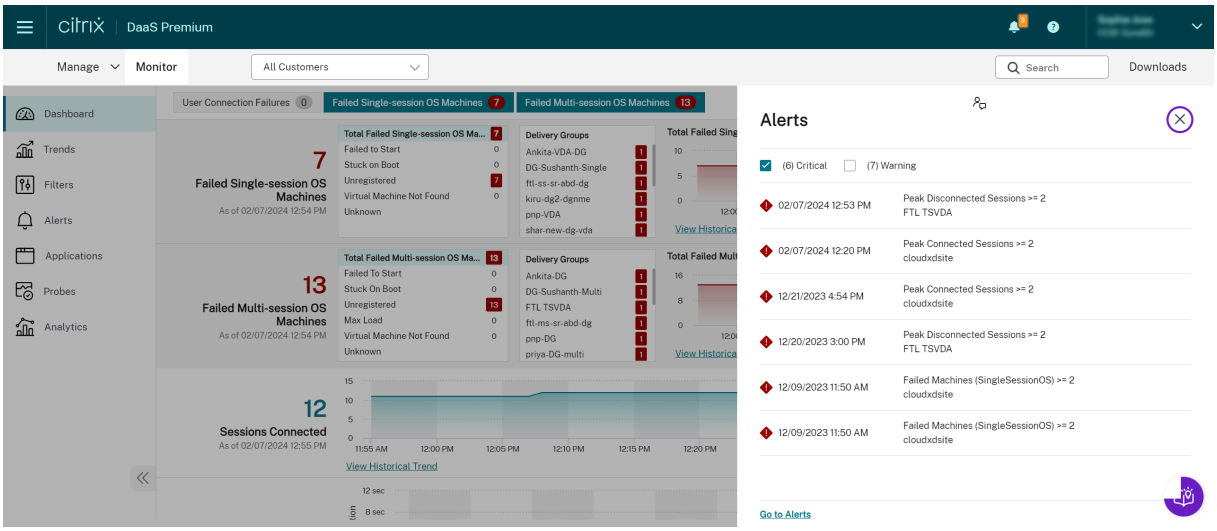
Análise de aplicativos

A guia **Applications** exibe análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos com eficiência. Você pode obter informações valiosas sobre a integridade e uso de todos os aplicativos publicados no site. Ela mostra métricas, tais como, os resultados de investigações, o número de instâncias por aplicativo e falhas e erros associados aos aplicativos publicados. Para obter mais informações, consulte a seção Análise de aplicativos em **Solucionar problemas de aplicativos**.

Alertas e notificações

November 21, 2023

Os alertas são exibidos no Monitor, no painel e em outras visualizações de alto nível, com símbolos de alerta crítico e de aviso. Os alertas são atualizados automaticamente a cada minuto, mas você também pode atualizar os alertas sob demanda.

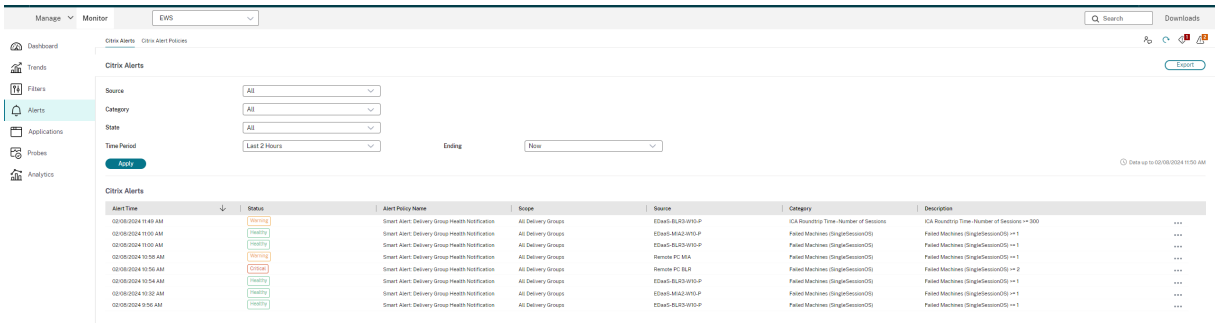


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre alertas selecionando um alerta na barra lateral, clicando no link **Go to Alerts**, na parte inferior da barra lateral, ou selecionando **Alerts** na parte superior da página do Monitor.

Na exibição Alerts, você pode filtrar e exportar os alertas. Por exemplo, para ver as máquinas com SO multissessão em um grupo de entrega específico que apresentaram falha no último mês ou todos os alertas a um usuário específico. Para obter mais informações, consulte Exportar relatórios.



Alertas Citrix

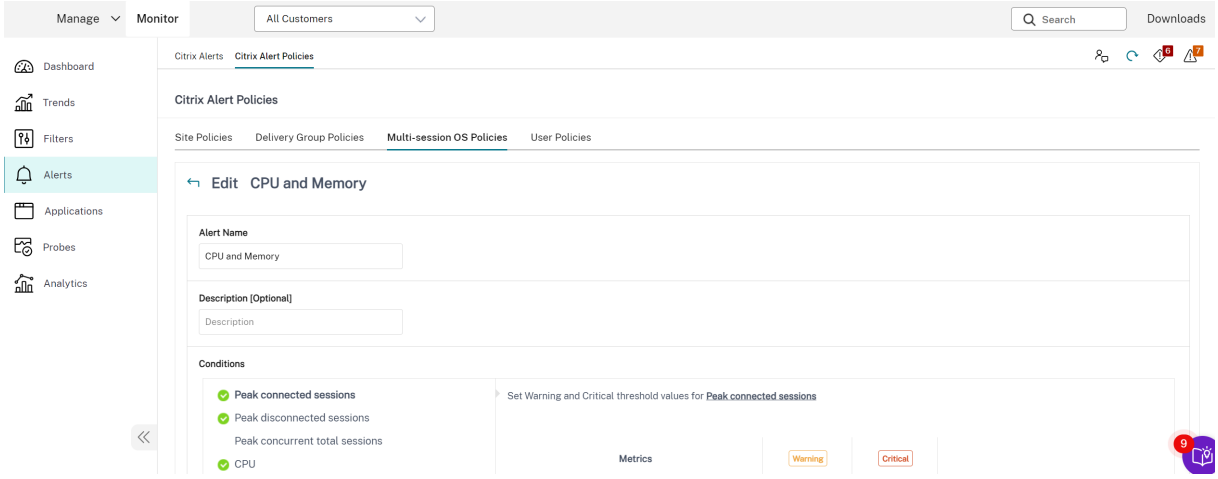
Os alertas Citrix são os que se originam de componentes Citrix. Você pode configurar alertas Citrix no Monitor em **Alerts** > **Citrix Alerts Policy**. Como parte da configuração, você pode definir notificações para serem enviadas por e-mail para indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar alertas Citrix, consulte Criar políticas de alertas.

Políticas de alertas inteligentes

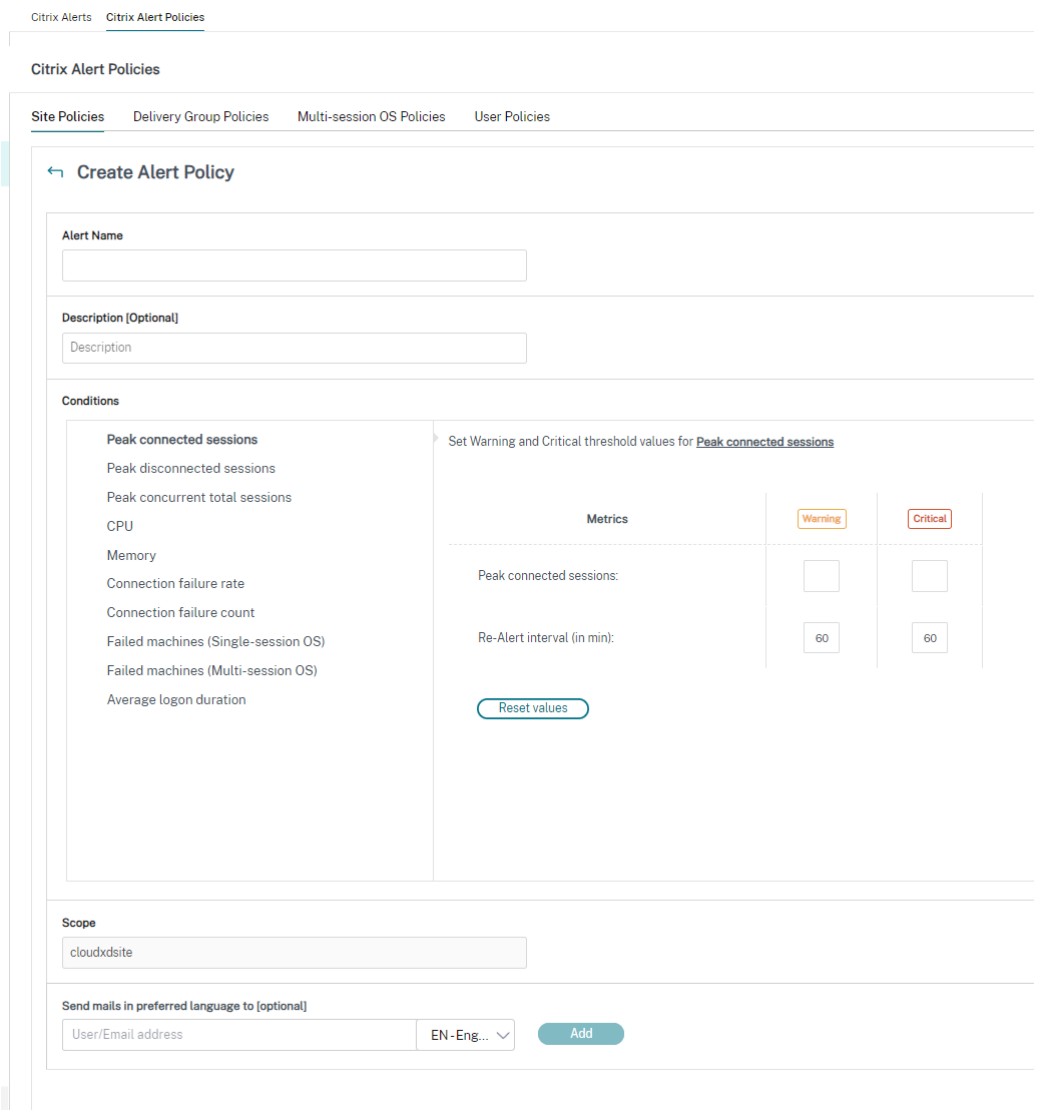
Um conjunto de políticas de alertas internos com valores limite predefinidos está disponível para o escopo de VDAs com SO multissessão e grupos de entrega. Você pode modificar os parâmetros de limite das políticas de alertas internos em **Alerts** > **Citrix Alerts Policy**.
Essas políticas são criadas quando há pelo menos um alvo de alerta: um grupo de entrega ou um VDA com SO multissessão definido em seu site. Além disso, esses alertas internos são adicionados automaticamente a um novo grupo de entrega ou a um VDA com SO multissessão.

As políticas de alertas internos são criadas somente se não houver regras de alertas correspondentes no banco de dados de monitoramento.

Para obter os valores limite das políticas de alertas internos, consulte a seção Condições das políticas de alertas.



Criar políticas de alertas



Para criar uma nova política de alertas, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alerts** > **Citrix Alerts Policy** e selecione, por exemplo, a política de SO multissessão.
2. Clique em **Create**.
3. Dê um nome e uma descrição para política e defina as condições que precisam ser atendidas para que o alerta seja disparado. Por exemplo, especifique os valores de pico de avisos e alertas críticos em Peak Connected Sessions, Peak Disconnected Sessions e Peak Concurrent Total Sessions. Os valores em Warning não devem ser maiores que os valores em Critical. Para obter mais informações, consulte Condições das políticas de alertas.
4. Defina o intervalo de repetição de alerta em Re-alert interval. Se as condições para o alerta continuarem a ser atendidas, o alerta será disparado novamente nesse intervalo de tempo e, se

configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta descartado não gera uma notificação por e-mail no intervalo de repetição do alerta.

5. Defina o escopo em Scope. Por exemplo, defina para um grupo de entrega específico.
6. Em Notification preferences, especifique quem deve ser notificado por e-mail quando o alerta for disparado. E-mails de notificações são enviados via SendGrid. Certifique-se de que o endereço de e-mail "donotreplynotifications@citrix.com"esteja na lista branca 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 controle giratório é exibido durante esse período.

A criação de mais de 50 políticas para até 20 grupos de entrega exclusivos (1000 alvos do 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 disparar alertas incorretamente do grupo de entrega que são definidos usando parâmetros da máquina.

> **Observação:**
> Depois de excluir uma política de alerta, pode levar até 30 minutos para que as notificações de alerta geradas pela política parem.

Condições das políticas de alertas

Veja abaixo as categorias de alertas, as ações recomendadas para mitigar o alerta e as condições de políticas internas, se definidas. As políticas de alertas internos são definidas para alertar repetidamente a intervalos de 60 minutos.

Pico de sessões conectadas, em Peak Connected Sessions

- No Monitor, verifique a exibição Session Trends para ver o pico de sessões conectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.

Pico de sessões desconectadas, em Peak Disconnected Sessions

- No Monitor, verifique a exibição Session Trends para ver o pico de sessões desconectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

Pico total de sessões simultâneas, em Peak Concurrent Total Sessions

- No Monitor, verifique a exibição Session Trends ver o pico de sessões simultâneas.
- 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 do uso da CPU indica o consumo geral da CPU no VDA, incluindo os processos. Você pode obter mais informações sobre a utilização da CPU por processos individuais na página **Machine details** do VDA correspondente.

- Vá para **Machine Details > View Historical Utilization > Top 10 Processes** e identifique os processos que consomem a CPU. Certifique-se de que a política de monitoramento de processos esteja ativada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Com o término do processo, os dados não salvos são perdidos.
- Se tudo estiver funcionando conforme o esperado, adicione recursos extras de CPU no futuro.

  > **Nota:**
  >
  > A configuração de política **Enable resource monitoring** é permitida por padrão para o monitoramento de contadores de desempenho de memória e CPU em máquinas com VDAs. Se essa configuração de política estiver desativada, os alertas com condições de CPU e memória não são disparados. Para obter mais informações, consulte Configurações da política de monitoramento.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 80%, Critical - 90%

Memória

A porcentagem de uso de memória indica o consumo geral de memória no VDA, incluindo os processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Machine details** do VDA correspondente.

- Vá para **Machine Details > View Historical Utilization > Top 10 Processes** e identifique os processos que consomem a memória. Certifique-se de que a política de monitoramento de

processos esteja ativada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.

- Encerre o processo, se necessário.
- Com o término do processo, os dados não salvos são perdidos.
- Se tudo estiver funcionando conforme o esperado, adicione memória extra no futuro.

> **Nota:**
>
> A configuração de política **Enable resource monitoring** é permitida por padrão para o monitoramento de contadores de desempenho de memória e CPU em máquinas com VDAs. Se essa configuração de política estiver desativada, os alertas com condições de CPU e memória não são disparados. Para obter mais informações, consulte Configurações da política de monitoramento.

Condições de políticas inteligentes:

- **Escopo:** scope de Delivery Group, Multi-session OS
- **Valores limite:** Warning - 80%, Critical - 90%

Taxa de falha na conexão, em Connection Failure Rate

Porcentagem de falhas de conexão na última hora.

- Calculado com base no total de falhas das tentativas totais de conexões.
- No Monitor, verifique a exibição Connection Failures Trends para ver os eventos registrados no log de configuração.
- Determine se os aplicativos ou as áreas de trabalho são acessíveis.

Contagem de falhas de conexão, em Connection Failure Count

Número de falhas de conexão na última hora.

- No Monitor, verifique a exibição Connection Failures Trends para ver os eventos registrados no log de configuração.
- Determine se os aplicativos ou as áreas de trabalho são acessíveis.

Média, em ICA RTT (Average)

Tempo médio de resposta do ICA (Independent Computing Architecture).

- Verifique o Citrix ADM para obter uma análise do ICA RTT para determinar a causa raiz. Para obter mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, verifique a exibição User Details no Monitor para saber o ICA RTT e Latência e determinar se é um problema de rede ou um problema com aplicativos ou áreas de trabalho.

Valor, em ICA RTT (No. of Sessions)

Número de sessões que excedem o limite de tempo de resposta do ICA.

- Verifique o Citrix ADM para saber o número de sessões com alto ICA RTT. Para obter 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 de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 300 ms por 5 ou mais sessões, Critical - 400 ms por 10 ou mais sessões

Valor, em ICA RTT (% of Sessions)

Porcentagem de sessões que excedem o tempo médio de resposta do ICA.

- Verifique o Citrix ADM para saber o número de sessões com alto ICA RTT. Para obter 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.

Valor, em ICA RTT (User)

Tempo de resposta do ICA que é aplicado às sessões iniciadas pelo usuário especificado. O alerta é acionado se o ICA RTT for maior que o limite em pelo menos uma sessão.

Máquinas com falha em sistemas de sessão única, em Failed Machines (Single session OS)

Número de máquinas com SO de sessão única com falhas. As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Monitor em Dashboard e Filters.

- Execute o diagnóstico do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Resolução de problemas de usuário.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group
  - **Valores limite:** Warning - 1, Critical - 2

Máquinas com falha em sistemas multissessão, em Failed Machines (Multi-session OS)

Número de máquinas com SO multissessão com falhas. As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Monitor em Dashboard e Filters.

- Execute o diagnóstico do Citrix Scout para determinar a causa raiz.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 1, Critical - 2

Máquinas com falha (em %)

Porcentagem de máquinas com SO de sessão única e multissessão com falha em um grupo de entrega calculada com base no número de máquinas com falha. Essa condição de alerta permite que você configure limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega, calculada a cada 30 segundos.
As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Director em Dashboard e Filters. Execute o diagnóstico do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Resolução de problemas de usuário.

Duração média de logon, em Average Logon Duration

Duração média dos logons ocorridos na última hora.

- Verifique o Dashboard do Monitor para obter métricas atualizadas em relação à duração do logon. Um grande número de usuários fazendo login em um curto período de tempo pode aumentar a duração do logon.
- Verifique a linha de base e a análise detalhada dos logons para determinar a causa. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 45 segundos, Critical - 60 segundos

Duração do logon (usuário), em Logon Duration (User)

Duração dos logons de um usuário especificado que ocorreu na última hora.

Índice do avaliador de carga, em Load Evaluator Index

Valor do índice do avaliador de carga nos últimos 5 minutos.

- No Monitor, verifique os computadores em Multi-session OS Machines que possam ter um pico de carga (carga máxima). Analise as falhas no Dashboard e o relatório de tendências do índice do avaliador de carga.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 80%, Critical - 90%

Monitoramento de alertas do Hypervisor

O Monitor exibe alertas para monitorar a integridade do Hypervisor. Alertas do Citrix Hypervisor e do 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 reinicializado ou não estiver disponível.

Para receber alertas do Hypervisor, certifique-se de que uma conexão de hospedagem seja criada na guia Manage. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas quanto a alertas do Hypervisor. A tabela a seguir descreve os vários parâmetros e estados dos alertas do Hypervisor.

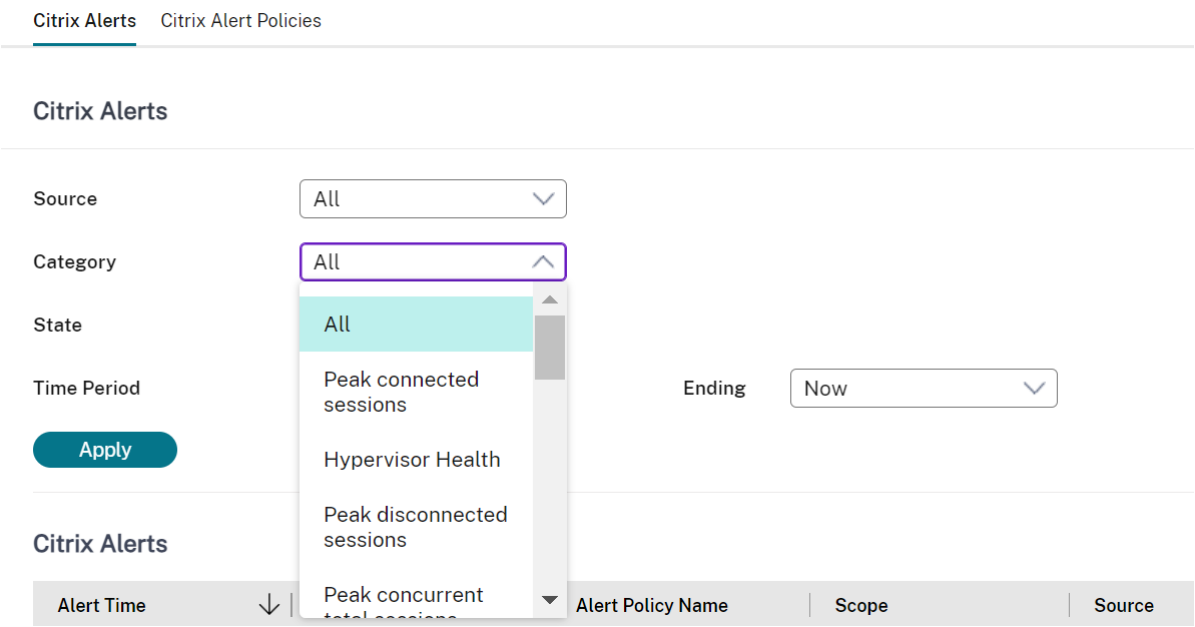
Alerta	Hypervisors compatíveis	Disparado por	Condição	Configuração
Uso de CPU	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da CPU é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Uso de memória	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de memória é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.

Alerta	Hypervisors compatíveis	Disparado por	Condição	Configuração
Uso de rede	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da rede é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Disk usage	VMware vSphere	Hypervisor	O limite de alerta de uso do disco é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Conexão do host ou estado de energia	VMware vSphere	Hypervisor	O host do Hypervisor foi reinicializado ou não está disponível	Os alertas estão integrados ao VMware vSphere. Não são necessárias configurações adicionais.
Conexão com o Hypervisor não disponível	Citrix Hypervisor, VMware vSphere	Delivery Controller	A conexão com o Hypervisor (pool ou cluster) é perdida ou desligada ou reinicializada. Esse alerta é gerado a cada hora, enquanto a conexão não estiver disponível.	Os alertas estão integrados ao Delivery Controller. Não são necessárias configurações adicionais.

> **Nota:**
>
> Para obter mais informações sobre como configurar alertas, consulte Citrix XenCenter Alerts ou a documentação de VMware vCenter Alerts.

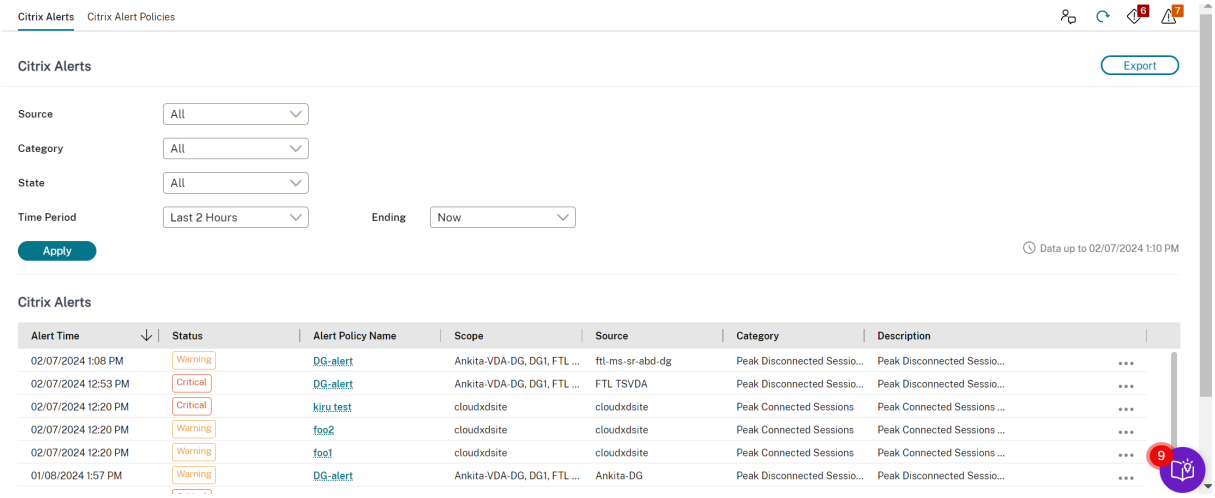
A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > Site Policy > Hypervisor Health**. As condições de limite para as políticas de alerta do Hypervisor podem ser configuradas, editadas, desativadas ou excluídas somente no Hypervisor, não no Monitor. No entanto, modificar as preferências de e-mail e descartar um alerta pode ser feito no Monitor.

> **Importante:**
>
> - Todos os alertas do Hypervisor com mais de um dia são descartados automaticamente.
> - Os alertas disparados pelo Hypervisor são obtidos e exibidos no Monitor. No entanto, as mudanças no ciclo de vida/estado dos alertas do Hypervisor não são refletidas no Monitor.
> - Alertas de boa integridade, ou que são descartados ou desativados no console do Hypervisor, continuarão a aparecer no Monitor e precisam ser descartados explicitamente.
> - Os alertas que são descartados no Monitor não são descartados automaticamente no console do Hypervisor.



Uma nova categoria de alerta chamada **Hypervisor Health** foi adicionada para permitir a filtragem somente dos alertas do Hypervisor. Esses alertas são exibidos quando os limites são atingidos ou excedidos. Alertas do Hypervisor podem ser:

- Critical —limite crítico da política de alarme do Hypervisor atingido ou excedido
- Warning —limite de aviso da política de alarme do Hypervisor atingido ou excedido
- Dismissed —o alerta não aparece mais como um alerta ativo

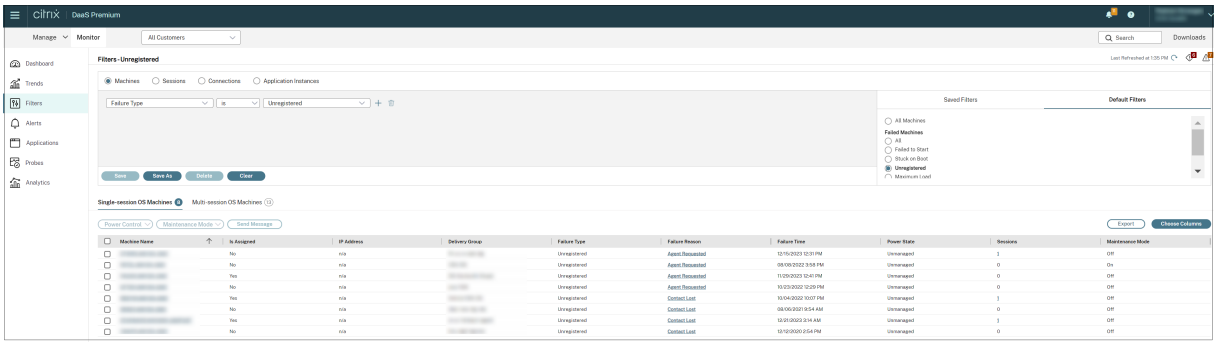


Filtrar dados para solucionar problemas de falhas

August 17, 2023

Quando você clica em números no painel Dashboard ou seleciona um filtro Default predefinido na guia **Filters**, a exibição Filters é aberta para exibir os dados com base na máquina selecionada ou no tipo de falha.

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 Saved filter.



1. Selecione uma exibição:

   - **Machines**. Selecione Single session OS Machines ou Multi-session OS Machines. Essas exibições mostram o número de máquinas configuradas. A guia Multi-session OS Machines também inclui o índice do avaliador de carga, que indica a distribuição dos contadores de desempenho e exibe dicas de ferramentas de contagem de sessões se você passar o mouse sobre o link.

- **Sessions**. Você também pode ver a contagem de sessões na exibição Sessions. Use as medições de tempo ocioso para identificar sessões que estão ociosas além de um período de tempo limite. Clique no **usuário associado** para abrir o gerenciador de atividades do usuário. Clicar no nome do **ponto de extremidade** abre o gerenciador de atividades do ponto de extremidade. Clicar em **View Details** abre as páginas **User Details** ou **Endpoint Details** respectivamente. Para obter mais informações, consulte Detalhes do usuário.
- **Connections**. Filtre conexões por diferentes períodos de tempo, incluindo últimos 60 minutos, últimas 24 horas ou últimos 7 dias.
- **Application Instances**. Essa exibição mostra as propriedades de todas as instâncias de aplicativos em VDAs com SO multissessão e de sessão única. As medições de tempo ocioso da sessão estão disponíveis para instâncias de aplicativos em VDAs com SO multissessão.

2. Selecione um filtro na lista de filtros Saved ou Default.
3. Use as listas suspensas para selecionar outros critérios de filtro.
4. Selecione colunas extras, conforme necessário, para solucionar problemas mais complexos.
5. Salve e dê um nome ao seu filtro.
6. Para abrir o filtro posteriormente, na exibição Filters, selecione View (Machines, Sessions, Connections ou Application Instances) e selecione o filtro salvo.
7. Clique em **Export** 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 **Machines** ou **Connections**, use os controles de energia para todas as máquinas selecionadas na lista filtrada. Para a exibição Sessions, use os controles de sessão ou a opção para enviar mensagens.
9. Nas exibições **Machines** e **Connections**, clique em **Failure Reason** em uma máquina ou conexão com falha para obter uma descrição detalhada da falha e das ações recomendadas para solucionar o problema da falha. Os motivos de falha e as ações recomendadas para falhas de máquina e na conexão estão disponíveis em Citrix Director Failure Reasons Troubleshooting Guide.
10. Na exibição **Machines**, clique no link do nome de uma máquina para ir para a página **Machine Details** correspondente. A página exibe os detalhes da máquina, fornece controles de energia, mostra os dados de monitoramento de CPU, memória e disco, além do gráfico de monitoramento da GPU. Clique também em **View Historical Utilization** para ver as tendências de utilização dos recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
11. Na exibição **Application Instances**, classifique ou filtre com base no **Idle Time** maior que um período de tempo limite. Selecione as instâncias do aplicativo ociosas para encerrá-las. O logoff ou a desconexão de uma instância de aplicativo encerra todas as instâncias de aplicativo

ativas em uma mesma sessão. Para obter mais informações, consulte Solucionar problemas de aplicativos. A página de filtro Application Instances e as medições de tempo ocioso nas páginas de filtro Sessions ficam disponíveis se os VDAs forem da versão 7.13 ou posterior.

> **Nota:**
>
> O console do Manage permite atribuir várias regras de atribuição de área de trabalho (DAR) de diferentes usuários ou grupos de usuários para um único VDA no grupo de entrega. O StoreFront exibe a área de trabalho atribuída com o nome de exibição correspondente de acordo com o DAR do usuário conectado. No entanto, o Monitor não oferece suporte a regras DAR e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário conectado. Como resultado, você não pode mapear uma área de trabalho específica a uma máquina no Monitor. Para mapear a área de trabalho atribuída exibida no StoreFront para o nome do grupo de entrega exibido no Monitor, use o seguinte comando do PowerShell. Execute o comando do 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
<!--NeedCopy-->
```

Monitorar tendências históricas em um site

August 17, 2023

A exibição Trends acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas na máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos

Para localizar essas informações, clique no menu **Trends**.

O recurso de zoom na análise detalhada permite navegar pelos gráficos de tendências, destacando um período de tempo (clicando em um ponto de dados no gráfico) para ver os pormenores associados

à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que foi afetado pelas tendências que estão sendo exibidas.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

> **Nota:**
>
> - As informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Last month (**Ending now**) ou mais curto. Quando você escolhe Last Month, com uma data de término personalizada, ou Last Year, as informações de tendência ficam disponíveis como gráficos, não como tabelas.
> - O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) oferece suporte à retenção de dados históricos apenas por 90 dias. Portanto, tendências e relatórios de um ano no Monitor mostram os últimos 90 dias de dados.

Tendências disponíveis

Exibir tendências para sessões: na guia Sessions, selecione o grupo de entrega e o período de tempo para exibir informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Session Auto Reconnect** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas Session Reliability ou Auto Client Reconnect estão em vigor. Quando há uma interrupção de rede no ponto de extremidade, as seguintes políticas entram em vigor:

- A confiabilidade da sessão, em Session Reliability, entra em vigor (por padrão, por 3 minutos) quando o Citrix Receiver ou o aplicativo Citrix Workspace tenta se conectar com o VDA.
- A reconexão automática de cliente, em Auto Client Reconnect, entra em vigor entre 3 e 5 minutos, quando o cliente tenta se conectar com o VDA.

Essas duas reconexões são capturadas e exibidas para o usuário. Essas informações podem levar um tempo máximo de 5 minutos para aparecer na interface do usuário do Director após ocorrer a reconexão.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções e a analisar redes com facilidade. Você pode exibir o número de reconexões para um grupo de entrega específico ou período de tempo selecionado nos filtros.

Uma análise detalhada fornece informações adicionais, como dados de confiabilidade da sessão ou reconexão automática de cliente, carimbos de hora, IP do ponto de extremidade e nome do ponto de extremidade da máquina em que o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de hora do evento em ordem decrescente. Esse recurso está disponível para o aplicativo Citrix Workspace para Windows, aplicativo Citrix Workspace

para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Esse 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 de 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 envia os dados de reconexão automática para o VDA.
- O VDA não envia os dados para o serviço Monitor.

> **Nota:**
>
> Às vezes, o endereço IP do cliente não é obtido corretamente se determinadas políticas do Citrix Gateway estiverem definidas.

Exibir tendências de falhas de conexão: na guia Failures, selecione a conexão, o tipo de máquina, o tipo de falha, o grupo de entrega e o período de tempo para exibir um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em todo o site.

Exibir tendências de falhas de máquinas: na guia Single session OS Machine Failures ou Multi-session OS Machines, selecione o tipo de falha, grupo de entrega e período de tempo para exibir um gráfico contendo informações mais detalhadas sobre as falhas da máquina em todo o site.

Exibir tendências de desempenho de logon: na guia Logon Performance, selecione o grupo de entrega e o período de tempo para exibir um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em todo o site e se o número de logons afeta o desempenho. Essa exibição também mostra a duração média das fases de logon, como a duração de intermediação do agente e a hora de início da máquina virtual.
Esses dados são especificamente para logons de usuários e não incluem usuários que tentam se reconectar em sessões desconectadas.
A tabela abaixo do gráfico mostra a duração do logon por sessão de usuário. Você pode escolher as colunas para exibir e classificar o relatório por qualquer uma das colunas.
Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Exibir tendências de avaliação de carga: na guia Load Evaluator Index, veja um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas com SO multissessão. As opções de filtro do gráfico incluem: grupo de entrega ou máquina com SO multissessão em um grupo de entrega, máquina com SO multissessão (disponível somente se a máquina com SO multissessão em um grupo de entrega tiver sido selecionada) e um intervalo. O índice do avaliador de carga é exibido em porcentagens do total de CPU, memória, disco ou sessões e comparado com o número de usuários conectados no último intervalo.

Exibir o uso de aplicativos hospedados: na guia Capacity Management, selecione a guia Hosted Applications Usage, selecione o grupo de entrega e o período de tempo para exibir um gráfico que mostra o pico no uso simultâneo e uma tabela que mostra o uso baseado em aplicativos. Na tabela Application Based Usage, você pode escolher um aplicativo específico para ver seus detalhes e uma lista dos usuários que estão usando ou usaram o aplicativo. Você pode ver os valores de pico previstos escolhidos para as instâncias simultâneas de aplicativos no período de tempo futuro usando a previsão da instância em Application. Para obter mais informações, consulte a seção Previsão de instâncias de aplicativo.

Exibir uso de SO de sessão única e multissessão: a exibição Trends mostra o uso do sistema operacional 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 Trends também mostra o uso do sistema operacional 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 você seleciona Machine, o uso é mostrado por usuário.

Exibir o uso da máquina virtual: na guia Machine Usage, selecione Single session OS Machines ou Multi-session OS Machines para ver uma exibição em tempo real do uso da sua máquina virtual. A página exibe o número de máquinas com SO multissessão e de sessão única habilitadas para AutoScale que estão ativadas para um grupo de entrega e período de tempo selecionados. Ao ativar AutoScale no grupo de entrega selecionado, você também terá disponível a economia estimada obtida; 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.

- Single session OS availability –exibe o estado atual das máquinas com SO de sessão única (VDIs) por disponibilidade de todo o site ou de um grupo de entrega específico.
- Multi-session OS availability - exibe o estado atual das máquinas com SO multissessão por disponibilidade de todo o site ou de um grupo de entrega específico.

> **Nota:**
>
> A grade abaixo do gráfico exibe os dados de uso da máquina com base no grupo de entrega em tempo real. Os dados incluem a disponibilidade de todas as máquinas, independentemente da ativação de AutoScale. O número de máquinas que aparece na coluna Available Counter da grade inclui máquinas no modo de manutenção.

A consolidação de dados de monitoramento depende do período de tempo selecionado.

- 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 são desconsideradas. Para ver o período de consolidação, consulte a documentação da API Monitor.

Para obter mais informações sobre como monitorar máquinas habilitadas para AutoScale, consulte o artigo AutoScale.

Exibir utilização de recursos: na guia Resource Utilization, selecione Single session OS Machines ou Multi-session OS Machines para ver informações sobre os dados de tendências históricas de uso de CPU e memória, além de IOPS e latência de disco de cada máquina VDI para poder planejar melhor a sua capacidade.
Esse recurso requer VDAs **versão 7.11** ou posterior.
Os gráficos mostram dados médios de CPU, memória e IOPS, latência do disco e pico de sessões simultâneas. Você pode fazer o detalhamento dos dados por máquina e visualizar dados e gráficos dos 10 principais processos que consomem a CPU. Filtre por grupo de entrega e período de tempo. Os gráficos de CPU, uso de memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, últimas 24 horas, últimos 7 dias, último mês e último ano. Os gráficos de médias de latência de disco e IOPS estão disponíveis para as últimas 24 horas, o último mês e o último ano.

> **Nota:**
>
> - A configuração da política Monitoring, Enable Process Monitoring, deve ser definida como "Allowed"para coletar e exibir dados na tabela Top 10 Processes na página Historic Machine Utilization. A política é definida como "Prohibited"por padrão. Por padrão, todos os dados de utilização de recursos são coletados. Isso pode ser desativado usando a configuração de política Enable Resource Monitoring. A tabela abaixo dos gráficos mostra os dados de utilização dos recursos por máquina.
> - O IOPS médio mostra as médias diárias. O pico de IOPS é calculado como a maior das médias de IOPS para o intervalo de tempo selecionado. (O IOPS médio é a média de IOPS por hora coletada durante a hora no VDA.)
> - O detalhamento da máquina lista processos com uso médio de CPU ou memória de mais de 1%. Isso pode significar que, às vezes, menos de 10 processos são listados.

Exibir falhas de aplicativos: a guia Application Failures exibe falhas associadas aos aplicativos publicados nos VDAs.

Esse recurso requer VDAs **versão 7.15** ou posterior. VDAs com SO de sessão única executando Windows Vista, e posterior, e VDAs com SO multissessão executando Windows Server 2008, e posterior, são suportados.
Para obter mais informações, consulte Monitoramento de falhas de aplicativos históricas.

Por padrão, somente falhas de aplicativos de VDAs com SO multissessão são exibidas. Você pode definir o monitoramento de falhas de aplicativos usando as políticas Monitoring. Para obter mais informações, consulte Configurações da política de monitoramento.

Exibir resultados do probe do aplicativo: a guia **Probe Results** exibe os resultados do probe dos aplicativos e áreas de trabalho que foram configurados para investigação na página Configuration. Nela, é registrado o estágio da inicialização durante o qual ocorreu a falha do início do aplicativo.

Para obter mais informações, consulte Investigação de aplicativo e área de trabalho.

Criar relatórios personalizados: a guia Custom Reports fornece uma interface de usuário para gerar relatórios personalizados contendo dados históricos e em tempo real do banco de dados de monitoramento em formato tabular.

Na lista de consultas ao relatório personalizado salvas anteriormente, você pode clicar em **Run and download**, para exportar o relatório em formato CSV, clicar em **Copy OData**, para copiar e compartilhar a consulta OData correspondente, ou clicar em **Edit**, para editar a consulta.
Você pode criar uma consulta ao relatório personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativos. Especifique as condições de filtro com base em máquina, grupo de entrega ou período de tempo. Especifique as colunas extras necessárias no seu relatório personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta ao relatório personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta ao relatório personalizado com base em uma consulta OData copiada. Para isso, selecione a opção OData Query e cole a consulta OData copiada. Você pode salvar a consulta resultante para executar posteriormente.

> **Nota:**
>
> Os nomes das colunas no relatório de visualização e exportação gerados usando consultas OData não são traduzidos (aparecem em inglês).

Os ícones dos sinalizadores no gráfico indicam eventos ou ações significativos para o intervalo de tempo específico. Passe o mouse sobre o sinalizador e clique para listar eventos ou ações.

> **Nota:**
>
> - Os dados de logon da 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 console Manage estão disponíveis para seleção nos filtros Trends até que os dados relacionados a eles sejam eliminados. Selecionar um grupo de entrega excluído exibe gráficos com os dados disponíveis até a retenção. No entanto, as tabelas não mostram nenhum dado.
> - Mover uma máquina contendo sessões ativas de um grupo de entrega para outro faz com que as tabelas **Resource Utilization e Load Evaluator Index** do novo grupo de entrega exibam métricas consolidadas dos grupos de entrega antigo e novo.

Previsão de instâncias de aplicativo

A análise preditiva oferece a capacidade de prever o uso futuro de recursos. Esse recurso é especialmente útil para os administradores organizarem os recursos e as licenças necessários em cada recurso.

O primeiro recurso de análise preditiva, a previsão de instância de aplicativo, prevê o número de instâncias de aplicativos hospedadas que provavelmente serão executadas por site ou grupo de entrega ao longo do tempo.

A previsão da instância do aplicativo está disponível na guia **Trends > Capacity Management**, que exibe o uso do aplicativo hospedado para o período escolhido. O gráfico histórico contém os valores de pico para as instâncias simultâneas de aplicativos plotadas para o período escolhido.

Para obter o gráfico previsto, marque a caixa de seleção Predict. Um gráfico de previsão em linha pontilhada é exibido como uma extensão do gráfico histórico. Os valores de pico previstos paras as instâncias simultâneas de aplicativos são plotados com a linha do tempo estendida ao futuro para o período escolhido.

Você pode prever as instâncias do aplicativo para os próximos 7 dias, 1 mês ou 1 ano. Datas de término personalizadas não são aceitas.

A previsão é feita usando algoritmos de aprendizado de máquina baseados em modelos de dados criados com dados históricos existentes. As previsões são, portanto, tão precisas quanto a qualidade dos dados existentes.

A precisão da previsão é indicada pelo nível de tolerância exibido como uma dica de ferramenta sobre o gráfico previsto. Ele indica a quantidade de variação possível entre os valores reais e os valores previstos.

O nível de tolerância pode ser alto se os dados disponíveis não seguirem um padrão regular ou estiverem ausentes por determinados períodos ou forem insuficientes.

A previsão para um ano captura os padrões mensais e trimestrais, juntamente com a tendência geral do ano. Da mesma forma, a previsão mensal captura os padrões diários e semanais, juntamente com tendências semanais, como atividade reduzida nos fins de semana.

Dados históricos suficientes devem estar disponíveis para previsão da seguinte forma:

- Dados de 14 dias para previsão de 7 dias
- Dados de 35 dias para previsão de 1 mês
- Dados de 84 dias para previsão de 1 ano

> **Nota:**
>
> Você pode exportar somente o gráfico histórico, não o gráfico previsto.

Monitorar máquinas gerenciadas por AutoScale

June 24, 2022

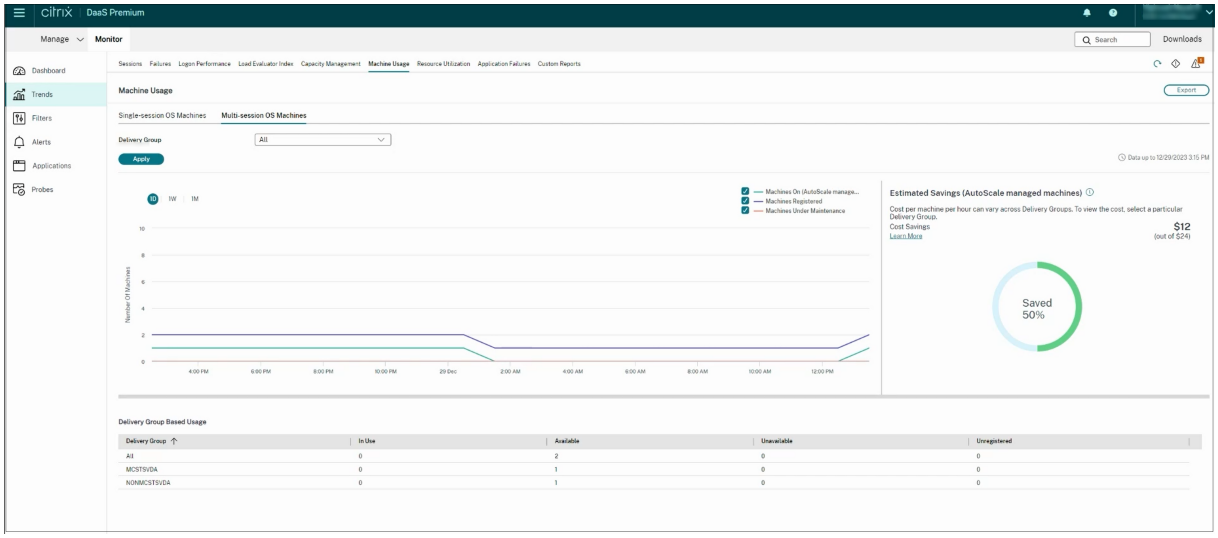
AutoScale é um recurso de gerenciamento de energia que permite o gerenciamento proativo de energia de todas as máquinas registradas com SO multissessão e de sessão única em um grupo de entrega. Você pode configurar o AutoScale para um grupo de entrega selecionado na guia **Manage**. Para obter mais informações, consulte AutoScale.

Você pode monitorar as principais métricas das máquinas habilitadas para AutoScale na guia **Monitor**.

Uso da máquina

A página **Monitor** > **Trends** > **Machine Usage** exibe o número total de máquinas com SO miltissessão e de sessão única habilitadas para AutoScale que estão ativadas para um grupo de entrega e período de tempo selecionados. Essa métrica indica o uso real de máquinas no grupo de entrega.

Na guia **Single session OS Machines** ou **Multi-session OS Machines**, selecione o grupo de entrega e o período de tempo.

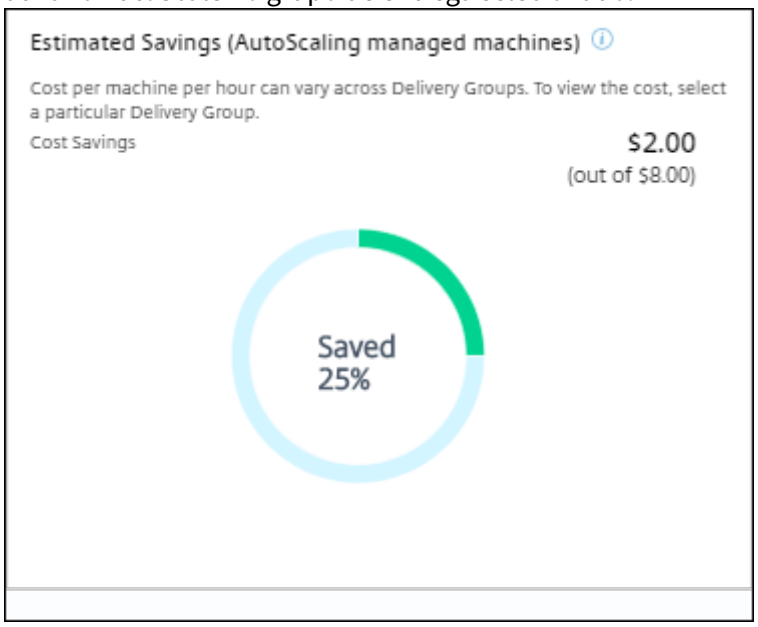


O gráfico representa as seguintes métricas:

- **Machines On** - o número de máquinas habilitadas para AutoScale que estão ligadas
- **Machines Registered** - o número de máquinas registradas com SO multissessão ou de sessão única
- **Machines under Maintenance** - o número de máquinas de SO multissessão ou de sessão única com o modo de manutenção ativado

Economia estimada

A página **Monitor** > **Trends** > **Machine Usage** também exibe a economia de custo estimada obtida ao ativar 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 **Manage** > **Edit Delivery Group** > **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 de economia estimada em todos os grupos de entrega é exibido.
A economia estimada ajuda os administradores a consolidar a infraestrutura existente e a planejar a capacidade para obter o máximo de economia e utilização.

Notificações de alerta de máquinas e sessões

O painel Monitor exibe notificações de alerta que podem ser detalhadas. Os detalhes do alerta são exibidos na página **Monitor** > **Alerts**.

- Para criar uma política de alerta em um grupo de entrega, vá para **Monitor** > **Alerts** > **Citrix Alerts Policy** > **Delivery Group Policy**.
- Você poderá definir os seguintes limites para Warning e Critical:
  - Failed Machines (SO de sessão única) e Failed Machines (SO multissessão)
  - Peak Connected Sessions, Peak Disconnected Sessions e Peak Concurrent Total Sessions no grupo de entrega
- Os alertas são gerados quando a métrica correspondente no grupo de entrega atinge o limite.

Para obter mais detalhes sobre as condições da política de alertas e a criação de novas políticas de alertas, consulte Alertas e notificações.

Status da máquina

- **Monitor** > **Filters** > **Machines** exibe o estado de energia de todas as máquinas em formato tabular. Você pode filtrar por grupo de entrega específico.
- **Monitor** > **Filters** > **Sessions** exibe o filtro pelo nome da máquina para mostrar as sessões associadas e seu status em tempo real.
- Em **Monitor** > **Trends** > **Sessions**, selecione o grupo de entrega e o período de tempo para ver a tendência das sessões e suas métricas associadas.

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

Tendências de avaliação de carga

A página **Monitor** > **Trends** > **Load Evaluator Index** exibe um gráfico com informações detalhadas sobre a carga que é distribuída entre as máquinas com SO multissessão. As opções de filtro do gráfico incluem: grupo de entrega ou máquina com SO multissessão em um grupo de entrega, máquina com SO multissessão (disponível somente se a máquina com SO multissessão em um grupo de entrega tiver sido selecionada) e um intervalo. O índice do avaliador de carga é exibido em porcentagens do total de CPU, memória, disco ou sessões e comparado com o número de usuários conectados no último intervalo.

Solucionar problemas de implantações

May 3, 2022

Como administrador do suporte técnico, você pode pesquisar o usuário que relatou um problema e exibir detalhes de sessões ou aplicativos associados a esse usuário.

Da mesma forma, você pode procurar máquinas ou pontos de extremidade onde os problemas são relatados. Os problemas podem ser resolvidos rapidamente 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 no modo de manutenção
- redefinir um perfil de usuário

Solucionar problemas de aplicativos

July 28, 2023

Análise de aplicativos

A exibição **Applications** mostra análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos com eficiência. Você pode obter informações valiosas sobre a integridade e uso de todos os aplicativos publicados no site. A exibição padrão ajuda a identificar os aplicativos em execução mais frequentemente.
Esse recurso requer VDAs versão 7.15 ou posterior.

A coluna **Probe Result** exibe o resultado da execução da investigação do aplicativo nas últimas 24 horas. Clique no link do resultado da investigação na página **Trends** > **Probe Results**. Para obter mais detalhes sobre como configurar probes de aplicativos, consulte Investigação de aplicativo e área de trabalho.

A coluna **Instances** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativos em execução no momento (instâncias conectadas e desconectadas). Para solucionar problemas, clique no campo **Instances** para ver a página de filtros **Application Instances** correspondente. Nela você pode selecionar instâncias de aplicativos para fazer logoff ou desconectar.

> **Nota:**
>
> Para administradores de escopo personalizados, o Monitor não exibe instâncias de aplicativos criadas em grupos de aplicativos. Para exibir todas as instâncias do aplicativo, você deve ser um administrador completo. Para obter mais informações, consulte o artigo do Knowledge Center CTX256001.

Monitore a integridade dos aplicativos publicados em seu site com as colunas **Application Faults** e **Application Errors**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao

iniciar o aplicativo correspondente na última hora. Clique no campo **Application Faults** ou **Application Errors** para ver os detalhes da falha na página **Trends** > **Application Failures** correspondente ao aplicativo selecionado.

As configurações da política de falha do aplicativo regem a disponibilidade e a exibição de falhas e erros. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da política Monitoring.

Monitoramento de aplicativos em tempo real

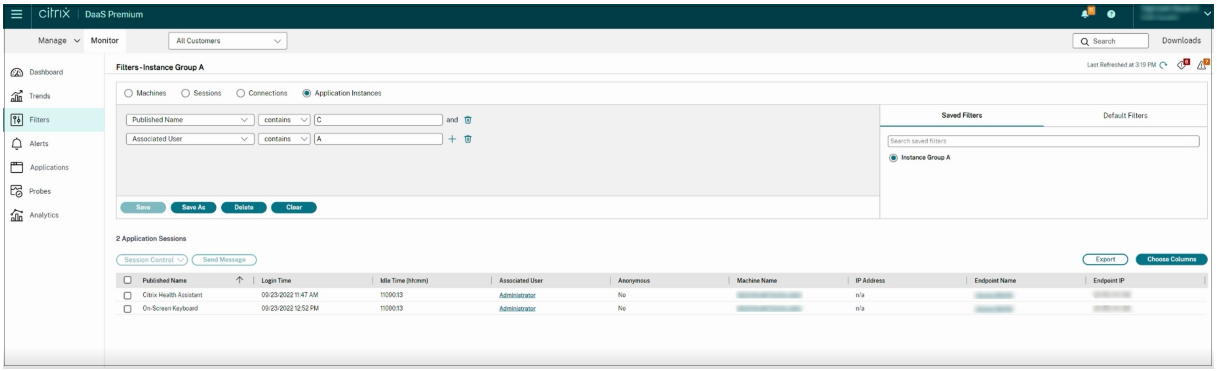
Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas com base em aplicativos são do setor de saúde, onde os funcionários compartilham licenças de aplicativos. Nesses casos, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente do Citrix Virtual Apps and Desktops, para reconfigurar servidores com baixo desempenho ou para manter e atualizar aplicativos.

A página de filtro **Application Instances** lista todas as instâncias de aplicativos em VDAs de SO multissessão e de sessão única. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativos em VDAs com SO multissessão que ficaram ociosas por pelo menos 10 minutos

> **Nota:**
>
> As métricas de instâncias de aplicativos estão disponíveis nos sites de todas as edições de licença.

Use essas informações para identificar as instâncias do aplicativo que estão ociosas além de um período de tempo específico e faça logoff ou desconecte-as conforme apropriado. Para isso, selecione **Filters > Application Instances** e selecione um filtro pré-salvo ou escolha **All Application Instances** e crie o seu próprio filtro.

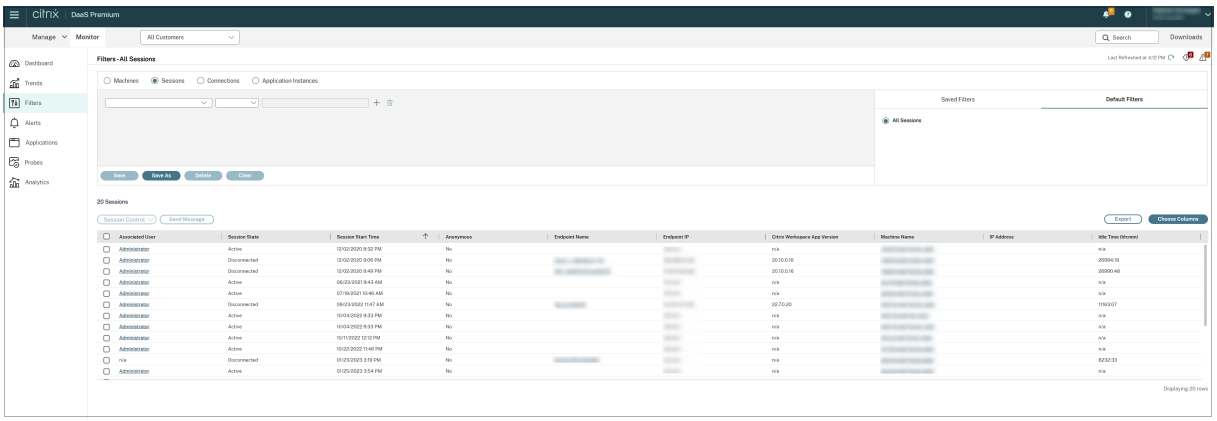


Um exemplo de filtro seria o que se segue. Como critério, em **Filter by**, escolha **Published Name** (do aplicativo) e **Idle Time**. Depois defina **Idle Time** como **greater than or equal to**, especifique um

limite de tempo e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias do aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Session Control**, escolha **Logoff** ou **Disconnect** para encerrar as instâncias.

> **Nota:**
>
> Fazer logoff ou desconectar uma instância do aplicativo encerra ou desconecta a sessão atual, dessa forma, terminando todas as instâncias do aplicativo que pertencem à mesma sessão.

Você pode identificar sessões ociosas na página de filtro **Sessions** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Idle Time** 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 com SO multissessão que ficaram ociosas por pelo menos 10 minutos.



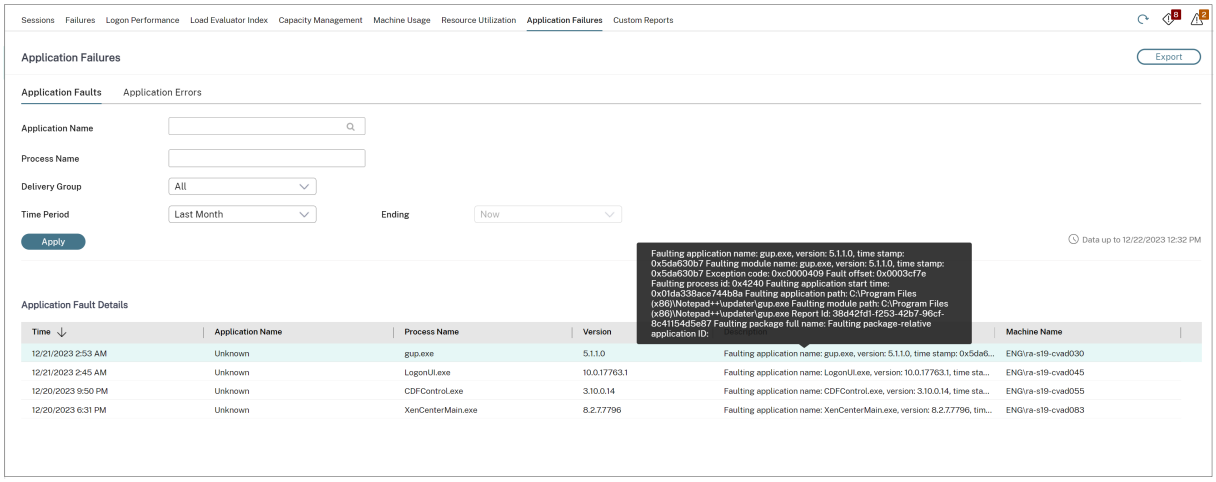
Idle time aparece como **N/A** quando a instância do aplicativo ou sessão

- não ficou ociosa por mais de 10 minutos,
- é iniciada em um VDA com SO de sessão única ou
- é iniciada em um VDA executando a versão 7.12 ou anterior.

Monitoramento de falhas de aplicativos históricas

A guia **Trends** -> **Application Failures** exibe falhas associadas aos aplicativos publicados nos VDAs.

Para obter mais informações sobre a disponibilidade das tendências de falha do aplicativo, consulte o artigo Granularidade e retenção de dados. As falhas de aplicativo registradas no log do Event Viewer com “Application Errors”na origem são monitoradas. Clique em **Export** para gerar relatórios em formatos CSV, Excel ou PDF.



As falhas são exibidas como **Application Faults** ou **Application Errors** com base em sua gravidade. A guia Application Faults exibe falhas associadas à perda de funcionalidade ou dados. Application Errors indica problemas que não são imediatamente relevantes, mas que significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Published Application Name**, **Process Name** ou **Delivery Group**, e **Time Period.** A tabela exibe o código de falha ou erro e uma breve descrição da falha. A descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:**
>
> O nome de Published Application é exibido como "Unknown"quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de área de trabalho ou quando falha devido a uma exceção não tratada causada por um executável dependente.

Por padrão, somente falhas de aplicativos hospedados em VDAs com SO multissessão são monitoradas. Você pode modificar as configurações de monitoramento por meio das políticas de grupo Monitoring: Enable monitoring of application failures, Enable monitoring of application failures on Single session OS VDAs e List of applications excluded from failure monitoring. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da política Monitoring.

A página **Trends > Application Probe Results** exibe os resultados da investigação de aplicativos executada no site nas últimas 24 horas e 7 dias. Para obter mais detalhes sobre como configurar probes de aplicativos, consulte Investigação de aplicativo.

Investigação de aplicativo

January 17, 2023

A investigação de aplicativos automatiza o processo de verificação da integridade do Citrix Virtual Apps que é publicado em um site. Os resultados da investigação do aplicativo estão disponíveis na guia **Monitor** do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). O Citrix Probe Agent é compatível com sites hospedados nos planos de controle do Citrix Cloud Japan e Citrix Cloud Government.

Assegure que as máquinas de ponto de extremidade executando Probe Agents sejam máquinas Windows com Citrix Receiver para Windows versão 4.8 ou posterior, ou aplicativo Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versão 1808 ou posterior. Aplicativo Workspace para UWP (Plataforma Universal do Windows) não é suportado.

Requisitos:

- Máquinas de ponto de extremidade executando probe agents são máquinas Windows com Citrix Receiver para Windows versão 4.8 ou posterior, ou aplicativo Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versão 1906 ou posterior. Aplicativo Workspace para UWP (Plataforma Universal do Windows) não é suportado.
- O Citrix Probe Agent suporta a autenticação padrão baseada em formulários, conforme suportada pelo Citrix WorkSpace. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como logon único (SSO) ou autenticação multifator (MFA). Da mesma forma, o Citrix Probe Agent funciona somente quando não há servidor proxy ou balanceador de carga, como o Citrix Gateway ou o Citrix ADC, implantado.
- Verifique se o Microsoft .NET Framework versão 4.7.2 ou posterior está instalado na máquina de ponto de extremidade em que você deseja instalar o Probe Agent.
- Para usar o agente de investigação no plano de controle do Citrix Cloud Japan, defina o valor do registro no caminho, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regic como 2. Para usar o agente de investigação no plano de controle do Citrix Cloud Government, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAge como 3.

As permissões/contas de usuário necessárias para executar a investigação do aplicativo são:

- Um usuário exclusivo do Workspace para investigar cada máquina de ponto de extremidade. O usuário do Workspace não precisa ser um administrador; os probes podem ser executados 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 ponto de extremidade.

- Uma conta de usuário de administrador completo com as seguintes permissões. A reutilização de contas de usuário existentes para investigação de aplicativos pode encerrar as sessões ativas dos usuários.
  - Permissões do grupo de entrega:
    * Somente leitura
  - Permissões do Director:
    * Criar\editar\remover configurações de investigação
    * Exibir a página de configurações
    * Exibir a página de tendências

Configurar a investigação de aplicativos

Configure as investigações do seu aplicativo para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes da investigação podem ajudar a solucionar problemas relacionados a aplicativos, máquina de hospedagem ou conexão antes que os usuários enfrentem esses problemas.

O Citrix Probe Agent versão 2103 suporta a agregação de sites. Aplicativos e áreas de trabalho podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o probe agent, selecione a opção **Workspace (StoreFront) Site Aggregation Enabled** para ativar a enumeração de aplicativos e áreas de trabalho a partir de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com um URL do StoreFront.
- Sites locais e na nuvem com um URL do StoreFront ou do Workspace.
- Vários sites na nuvem com um URL do Workspace.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar probes que tenham acesso a apenas um site.

Etapa 1: Instalar e configurar o Citrix Probe Agent

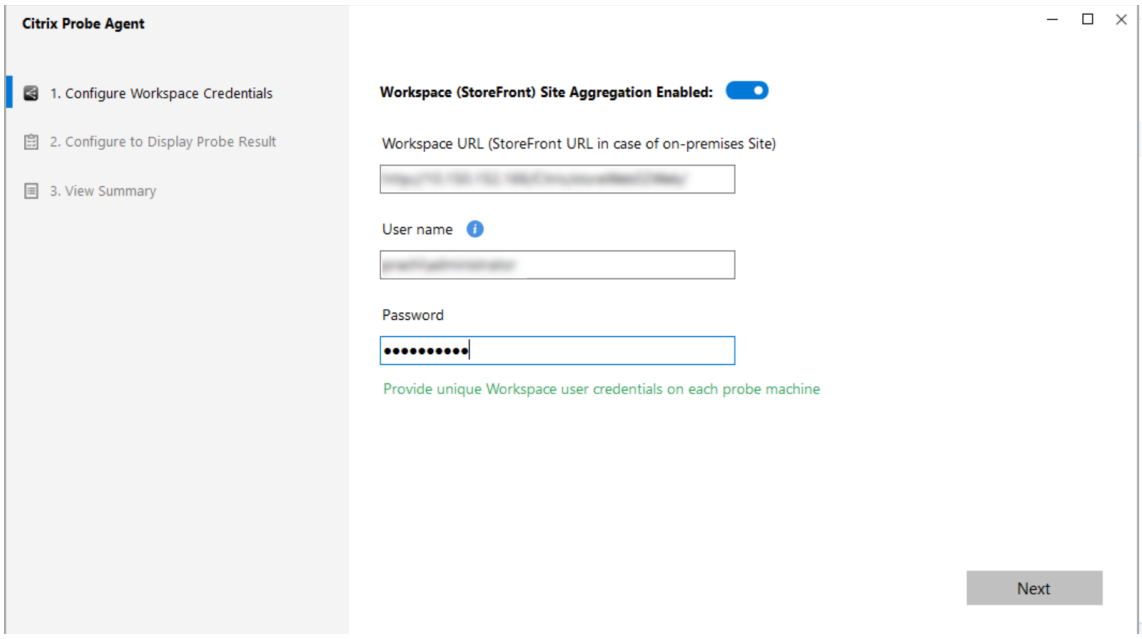
O Citrix Probe Agent é um executável do Windows que simula o início real do aplicativo pelo usuário por meio do Citrix Workspace. Ele testa a inicialização de aplicativos conforme configurada no Monitor e informa os resultados ao Monitor.

1. Identifique as máquinas de ponto de extremidade de onde você deseja executar a investigação do aplicativo.

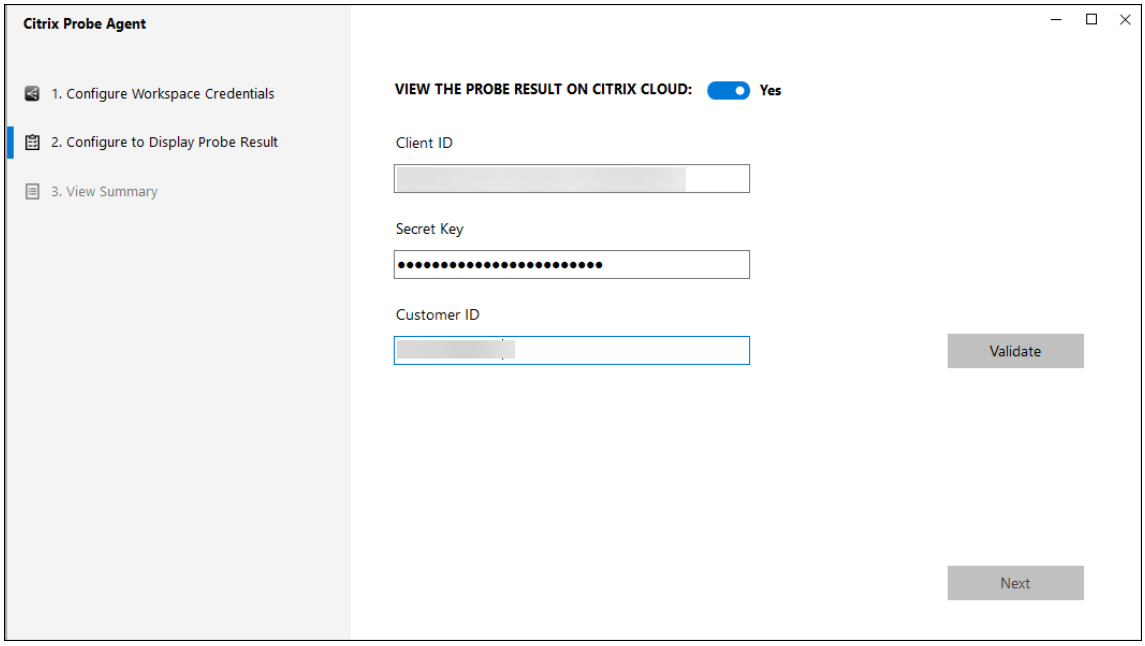
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de ponto de extremidade. Baixe o executável Citrix Probe Agent disponível em https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie o agente e configure suas credenciais do Citrix Workspace. Configure um usuário exclusivo do Workspace em cada máquina de ponto de extremidade. As credenciais são criptografadas e armazenadas com segurança.

   Observações:

   - Para acessar o site a ser investigado de fora da rede, digite o URL de login do Citrix Gateway no campo **URL do Workspace**. O Citrix Gateway roteia automaticamente a solicitação para o URL do Workspace do site correspondente.
   - Use NetBIOS como o nome de domínio no campo de nome de usuário. Por exemplo, NetBIOS/nome de usuário.
   - A investigação de aplicativos é compatível com o serviço Citrix Content Collaboration usando a autenticação do Workspace (somente AD).



4. Na guia **Configure To Display Probe Result**, insira as credenciais para acessar o Citrix DaaS. No console do Citrix Cloud, na página API Access, você encontra Customer Name ou Customer ID, Client ID e Secret Key.



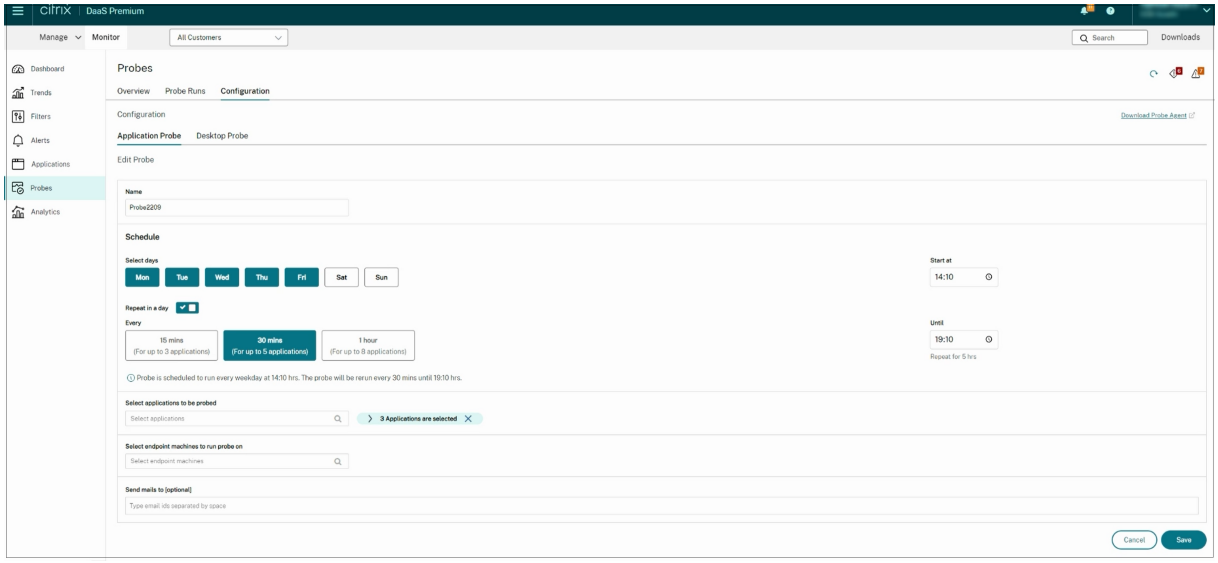
Etapa 2: Configurar a investigação de aplicativos na guia Monitor

1. No Citrix DaaS, vá para **Configuration** > **Probe Configuration** > **Application Probe** e clique em **Create Probe**:
2. Na página **Create Probe**, insira o nome da investigação.
3. Selecione a programação:

   a) Escolha os dias da semana em que você deseja que a investigação seja executada.
   b) Insira a hora de início na qual você deseja que a investigação seja executada.
   c) Além disso, você pode escolher a opção **Repeat in a day**. Insira a hora de término e o intervalo que deseja que a investigação seja repetida no dia. Por exemplo, a configuração abaixo ajuda a executar investigações de aplicativos das 12h08 até as 16h34, repetindo-as a cada 30 minutos todas as segundas, quartas, quintas e domingos.

4. Selecione o número recomendado de aplicativos a serem investigados, de acordo com o intervalo.
5. Selecione as máquinas de ponto de extremidade nas quais a investigação deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da investigação da falha são enviados e clique em **Save**.

Nessa configuração, as sessões do aplicativo são iniciadas às 12h08, 12h38, 13h08 e assim por diante até as 16h08 todas as segundas, quartas, quintas e domingos.



> **Nota:**
>
> - Configure seu servidor de e-mail em **Alerts** > **Email Server Configuration**.
> - Após a configuração na guia **Monitor**, o agente executa as investigações configuradas começando na próxima hora.
> - As investigações, ou sondagens, que foram configuradas antes da introdução da opção **Repeat in a day** continuam sendo executadas no horário programado. Elas têm a opção **Repeat in a day** desativada por padrão.

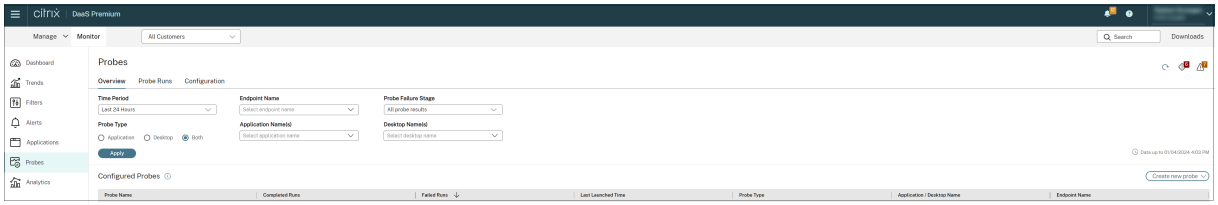
Etapa 3: Execução da investigação

O agente executa a investigação do aplicativo de acordo com a configuração do probe que ele obtém do Monitor a cada hora. Ele inicia aplicativos selecionados em série usando o Workspace. O agente relata os resultados para o Monitor através do banco de dados de monitoramento. As falhas são relatadas em cinco estágios específicos:

- **Workspace Reachability** - o URL do Workspace configurado não pode ser acessado.
- **Workspace Authentication** - as credenciais do Workspace configuradas são inválidas.
- **Workspace Enumeration** - a lista de aplicativos Workspace Enumerate não contém o aplicativo a ser investigado.
- **ICA download** –o arquivo ICA não está disponível.
- **Application launch** –o aplicativo não pode ser iniciado.

Etapa 4: Exibir resultados da investigação

Você pode ver os resultados da investigação mais recente em Citrix DaaS > página **Applications**.



Para ver mais detalhes para a solução de problemas, clique no link do resultado da investigação na página **Trends** > **Application Probe Results**.

Os dados dos resultados da investigação consolidados estão disponíveis para as últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a investigação falhou. Você pode filtrar a tabela para um aplicativo específico, estágio de falha da investigação ou máquina de ponto de extremidade.

Investigação da área de trabalho

February 16, 2023

A investigação de área de trabalho automatiza o processo de verificação da integridade do Citrix Virtual Desktops que é publicado em um site. Os resultados da investigação da área de trabalho estão disponíveis no Monitor. Agora, o Citrix Probe Agent é compatível com sites hospedados nos planos de controle do Citrix Cloud Japan e Citrix Cloud Government.

Na página Configuration do Monitor, configure as áreas de trabalho a serem investigadas, as máquinas de ponto de extremidade para executar a investigação e o tempo da investigação. O agente testa o início de áreas de trabalho selecionadas usando o Workspace e informa os resultados de volta ao Monitor. Os resultados da investigação são exibidos na interface do usuário do Monitor —os dados das últimas 24 horas na página Applications e os dados do histórico de investigação na página **Trends > Probe Results > Desktop Probe Results**.

Aqui, você pode ver o estágio em que a falha de investigação ocorreu –Workspace Reachability, Workspace Authentication, Workspace Enumeration, ICA Download ou Desktop Launch. O relatório de falhas é enviado para os endereços de e-mail configurados.

Você pode agendar as investigações da sua área de trabalho para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes podem ajudar a solucionar problemas proativamente relacionados a áreas de trabalho provisionadas, máquinas de hospedagem ou conexões antes que os usuários enfrentem esses problemas.

Esse recurso requer o Probe Agent 1903 ou posterior.

Requisitos:

- Máquinas de ponto de extremidade executando probe agents são máquinas Windows com Citrix Receiver para Windows versão 4.8 ou posterior, ou aplicativo Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versão 1906 ou posterior. Aplicativo Workspace para UWP (Plataforma Universal do Windows) não é suportado.
- O Citrix Probe Agent suporta a autenticação padrão baseada em formulários, conforme suportada pelo StoreFront e pelo Citrix WorkSpace. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como logon único (SSO) ou autenticação multifator (MFA). Da mesma forma, o Citrix Probe Agent funciona somente quando não há servidor proxy ou balanceador de carga, como o Citrix Gateway ou o Citrix ADC, implantado.
- Verifique se o Microsoft .NET Framework versão 4.7.2 ou posterior está instalado na máquina de ponto de extremidade em que você deseja instalar o Probe Agent.
- Para usar o agente de investigação no plano de controle do Citrix Cloud Japan, defina o valor do registro no caminho, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regic como 2. Para usar o agente de investigação no plano de controle do Citrix Cloud Government, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAge como 3.

Permissões ou contas de usuário necessárias para executar a investigação da área de trabalho:

- Um usuário exclusivo do Workspace para investigar cada máquina de ponto de extremidade. O usuário do Workspace não precisa ser um administrador; os probes podem ser executados 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 ponto de extremidade.
- Uma conta de usuário de administrador completa ou uma função personalizada com as seguintes permissões. A reutilização de contas de usuário normais para investigação de áreas de trabalho pode desconectar os usuários de suas 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 investigação
    - Exibir a página de configurações
    - Exibir a página de tendências

Configurar a investigação de área de trabalho

Você pode agendar as investigações da sua área de trabalho para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes da investigação podem ajudar

a solucionar problemas relacionados a áreas de trabalho, máquina de hospedagem ou conexão antes que os usuários enfrentem esses problemas.

O Citrix Probe Agent versão 2103 suporta a agregação de sites. Aplicativos e áreas de trabalho podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o probe agent, selecione a opção **Workspace (StoreFront) Site Aggregation Enabled** para ativar a enumeração de aplicativos e áreas de trabalho a partir de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com um URL do StoreFront.
- Sites locais e na nuvem com um URL do StoreFront ou do Workspace.
- Vários sites na nuvem com um URL do Workspace.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar probes 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 início real da área de trabalho pelo usuário por meio do Workspace. Ele testa a inicialização da área de trabalho conforme configurada no Monitor e informa os resultados ao Monitor.

1. Identifique as máquinas de ponto de extremidade de onde você deseja executar a investigação da área de trabalho.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de ponto de extremidade. Baixe o executável Citrix Probe Agent disponível em https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie o agente e configure suas credenciais do Workspace Receiver para Web. Configure um usuário exclusivo do Workspace em cada máquina de ponto de extremidade. As credenciais são criptografadas e armazenadas com segurança.

   > **Observações:**
   >
   > - Para acessar o site a ser investigado de fora da rede, digite o URL da página de login do Citrix Gateway no campo URL do Workspace. O Citrix Gateway roteia automaticamente a solicitação para o URL do Workspace do site correspondente. Esse 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 investigação de áreas de trabalho é compatível com o serviço Citrix Content Collab-

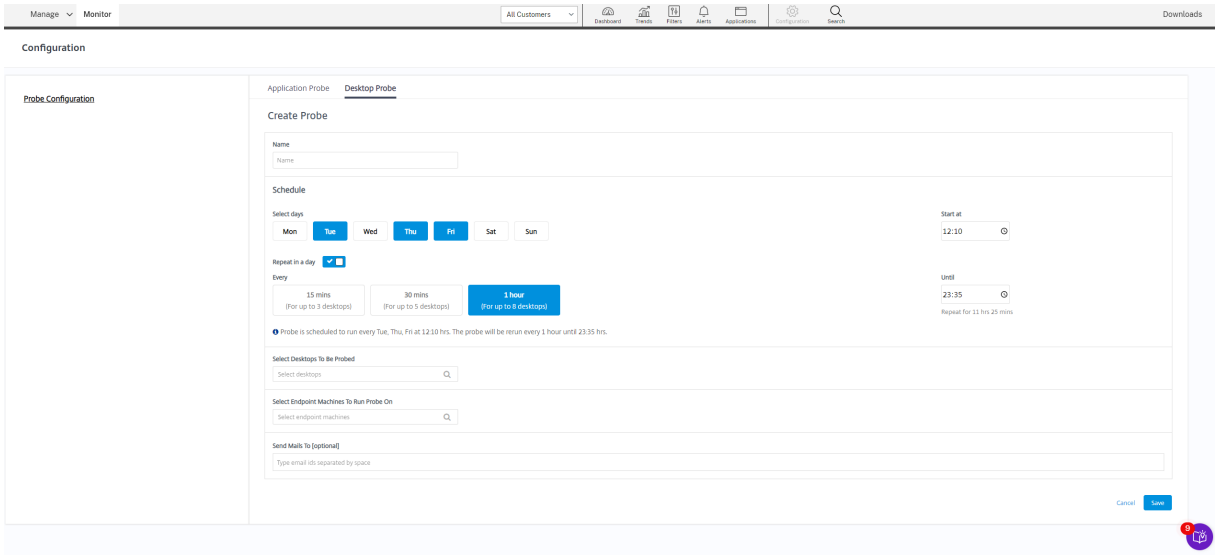
> oration usando a autenticação do Workspace (somente AD).
> - Você deve habilitar o logon interativo para o usuário exclusivo configurado do StoreFront.

4. Na guia **Configure To Display Probe Result**, insira suas credenciais do Monitor. No console do Citrix Cloud, na página API Access, você encontra Customer Name ou Customer ID, Client ID e Secret Key.

Etapa 2: Configurar a investigação de área de trabalho no Monitor

1. No Citrix DaaS, vá para **Configuration** > **Probe Configuration** > **Application Probe** e clique em **Create Probe**.
2. Na página **Create Probe**, insira o nome da investigação.
3. Selecione a programação:
   a) Escolha os dias da semana em que você deseja que a investigação seja executada.
   b) Insira a hora de início na qual você deseja que a investigação seja executada.
   c) Além disso, você pode escolher a opção **Repeat in a day**. Insira a hora de término e o intervalo que deseja que a investigação seja repetida no dia. Por exemplo, a configuração abaixo ajuda a executar investigações de áreas de trabalho das 12h10 às 23h35, repetindo-as a cada hora todas as terças, quintas e sextas-feiras.
4. Selecione o número recomendado de áres de trabalho a serem investigadas, de acordo com o intervalo.
5. Selecione as máquinas de ponto de extremidade nas quais a investigação deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da investigação da falha são enviados e clique em **Save**.

Nessa configuração, as sessões de áreas de trabalho são iniciadas às 12h10, 13h10, 14h10 e assim por diante até as 23h10 todas as terças, quintas e sextas-feiras.



> **Nota:**
>
> - Configure seu servidor de e-mail em **Alerts** > **Email Server Configuration**.
> - Após concluir a configuração da investigação da área de trabalho, o agente executa as investigações configuradas começando na próxima hora.
> - As investigações, ou sondagens, que foram configuradas antes da introdução da opção **Repeat in a day** continuam sendo executadas no horário programado. Elas têm a opção **Repeat in a day** desativada por padrão.

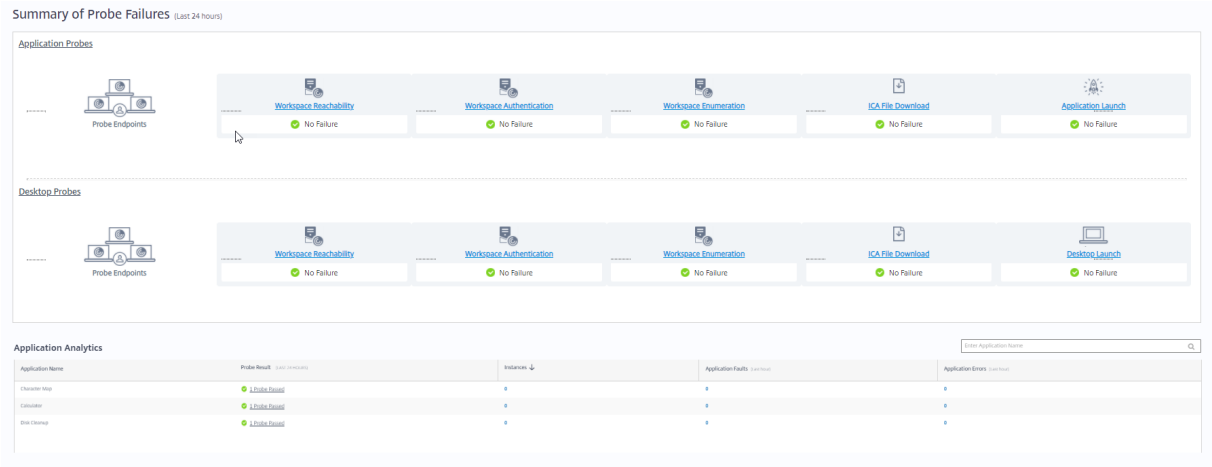
Etapa 3: Execução da investigação

O agente executa a investigação da área de trabalho de acordo com a configuração do probe que ele busca no Monitor periodicamente. Ele inicia áreas de trabalho selecionadas em série usando o Workspace. O agente relata os resultados para o Monitor através do banco de dados de monitoramento. As falhas são relatadas em cinco estágios específicos:

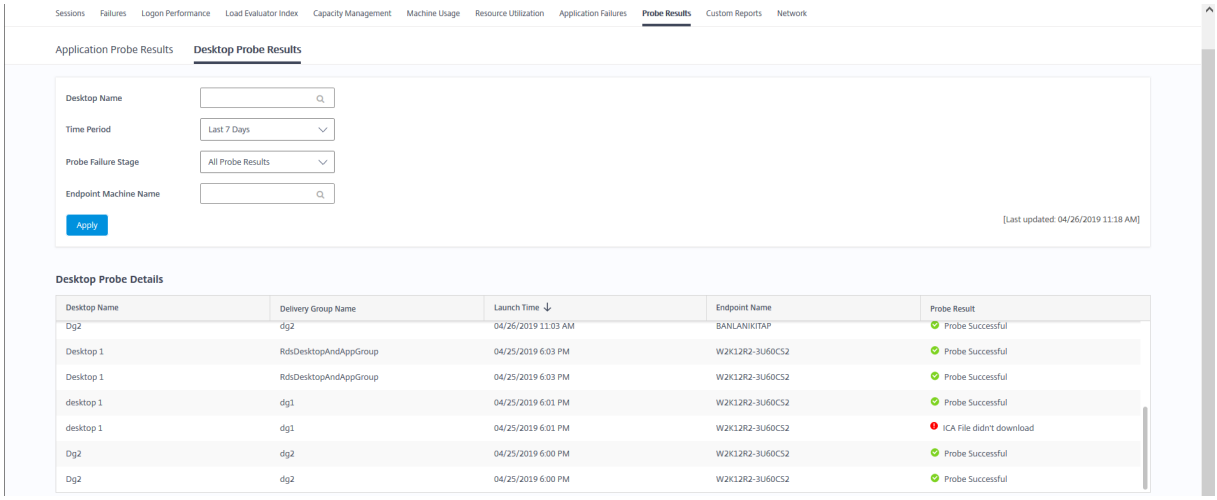
- **Workspace Reachability** - o URL do Workspace configurado não pode ser acessado.
- **Workspace Authentication** - as credenciais do Workspace configuradas são inválidas.
- **Workspace Enumeration** –a lista de áreas de trabalho do Workspace Enumerate não contém a área de trabalho a ser investigada.
- **ICA download** –o arquivo ICA não está disponível.
- **Desktop launch** –a área de trabalho não pode ser iniciada.

Etapa 4: Exibir resultados da investigação

Você pode ver os resultados da investigação mais recente na página **Desktops**.



Para ver mais detalhes para a solução de problemas, clique no link do resultado da investigação na página **Trends** >**Probe Results** > **Desktop Probe Results**.



Os dados dos resultados da investigação consolidados estão disponíveis para as últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a investigação falhou. Você pode filtrar a tabela para uma área de trabalho específica, estágio de falha da investigação ou máquina de ponto de extremidade.

Solucionar problemas de máquinas

December 20, 2023

> **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 identi-

> ficar possíveis causas de falhas de registro do VDA e problemas na configuração de redirecionamento de fuso horário e início de sessão. O artigo do Knowledge Center Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém as instruções de download e uso da ferramenta **Citrix Health Assistant**.

A exibição **Filters > Machines** na guia Monitor mostra as máquinas configuradas no site. A guia Multi-session OS Machines inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessão quando você passa o mouse sobre o link.

Clique na coluna **Failure Reason** de uma máquina com falha para obter uma descrição detalhada da falha e das ações recomendadas para solucionar o problema. Os motivos de falha e as ações recomendadas para falhas de máquina e na conexão estão disponíveis em Citrix Director Failure Reasons Troubleshooting Guide.

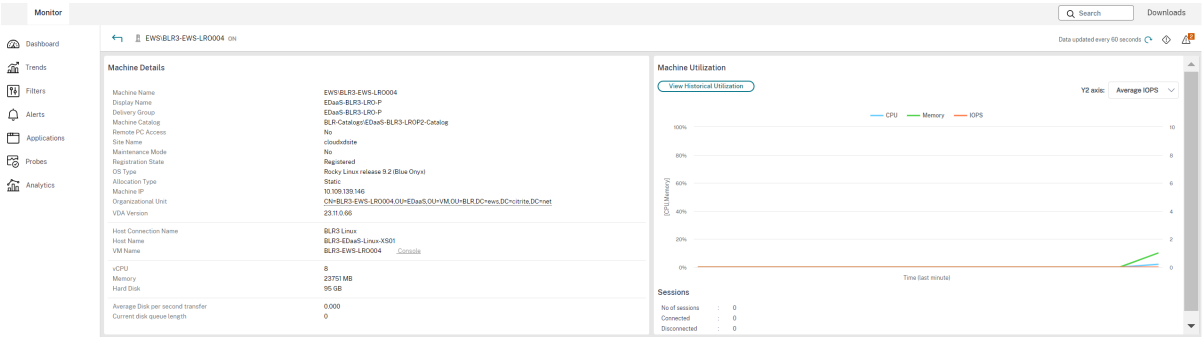
Clique no link do nome da máquina para ir para a página **Machine Details**.

A página Machine Details lista os detalhes da máquina, os detalhes da infraestrutura e os detalhes dos hotfixes aplicados na máquina.

Utilização em tempo real de recursos baseada em máquina

O painel **Machine Utilization** exibe gráficos que mostram a utilização em tempo real da CPU e da memória. Além disso, gráficos de monitoramento de disco e GPU estão disponíveis para sites com VDA 7.14 e versões posteriores.

Gráficos de monitoramento de disco, média de IOPS e latência de disco são medições de desempenho importantes que ajudam a monitorar e solucionar problemas relacionados aos discos VDA. O gráfico Average IOPS exibe o número médio de leituras e gravações em um disco. Selecione **Disk Latency** para ver um gráfico do atraso entre uma solicitação de dados e o seu retorno do disco, medido em milissegundos.



Utilização de GPU

Selecione **Utilização de GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do codificador e do decodificador para solucionar problemas relacionados à GPU em VDAs com SO multissessão ou de sessão única.

Versões de GPU suportadas:

- GPUs NVIDIA Tesla M60 executando o Display Driver versão 369.17 ou posterior. Para obter mais informações, consulte Software NVIDIA vGPU.
- GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12(Rome). Para obter mais informações, consulte Suporte e Drivers AMD.

Drivers:

Os drivers ou extensões apropriados devem ser instalados nos VDAs.

- Para GPUs NVIDIA, instale os drivers GRID manualmente ou por meio de extensões. Para obter mais informações, consulte Software NVIDIA vGPU.
  - Observe que, para NVIDIA, somente os drivers GRID são suportados. Os drivers CUDA não funcionam com a série NVadsA10 v5 e não são suportados.
  - Para ver um exemplo do processo de instalação de drivers da GPU Nvidia Grid por meio de extensões em máquinas baseadas no Azure, consulte Drivers NVIDIA GRID. Extensão de driver de GPU NVIDIA - VMs do Azure Windows - Máquinas virtuais do Azure.
  - Para ver um exemplo do processo para instalar manualmente os drivers da GPU Nvidia Grid, consulte Configuração de driver de GPU NVIDIA da série N do Azure para Windows - Máquinas virtuais do Azure.
- Para GPUs AMD, instale os drivers gráficos AMD manualmente ou por meio de extensões. Para obter mais informações, consulte Suporte e Drivers AMD.
  - Para ver um exemplo do processo de instalação de drivers de GPU AMD por meio de extensões em máquinas baseadas no Azure, consulte Extensão do Driver GPU AMD - VMs do Azure Windows - Máquinas virtuais do Azure.
  - Para ver um exemplo do processo de instalação manual de drivers de GPU AMD em máquinas do Azure, consulte Instalação de drivers de GPU AMD em VMs da série N executando Windows.

Notas de uso:

- Os gráficos de utilização de GPU estão disponíveis somente para VDAs que executam o Windows de 64 bits.
- Os gráficos de utilização da GPU AMD estão disponíveis somente para VDAs que executam o Citrix Virtual Apps and Desktops 7 2212 ou posterior.

- Os VDAs devem ter o HDX 3D Pro habilitado para fornecer aceleração de GPU. Para obter mais informações, consulte Aceleração da GPU para SO Windows de sessão única e Aceleração da GPU para SO multissessão Windows.
- Quando um VDA acessa mais de uma GPU, o gráfico de utilização exibe a média das métricas da GPU coletadas das GPUs individuais. As métricas da GPU são coletadas para todo o VDA e não para processos individuais.
- Para AMD, o uso do codificador e o uso do decodificador não são suportados separadamente. Qualquer carga de trabalho de codificação/decodificação usando a GPU será relatada como a carga geral 3D no uso da GPU.
- Certifique-se de instalar o NVIDIA WMI durante a instalação. Essa janela está disponível somente 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 nenhuma atividade no Director, verifique se a carga de trabalho que você está executando está usando a GPU. Para cargas de trabalho gráficas, isso pode ser ativado em Configurações > Sistema > Tela > Configurações de elementos gráficos > Escolha um aplicativo para definir a preferência. Certifique-se de ativar Alto desempenho. Às vezes, o Windows usa a CPU como padrão para cargas de trabalho gráficas quando ela é definida 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 um minuto após selecionar **Utilização de GPU**.

Utilização histórica de recursos baseada em máquina

No painel **Machine Utilization**, clique em **View Historical Utilization** para exibir o uso histórico de recursos na máquina selecionada.
Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, pico de sessões simultâneas, média de IOPS e latência de disco.

> **Nota:**
>
> A configuração de política de monitoramento **Enable Process Monitoring** deve ser definida como Allowed para coletar e exibir dados na tabela Top 10 Processes na página Historic Machine Utilization. A coleção é proibida por padrão.

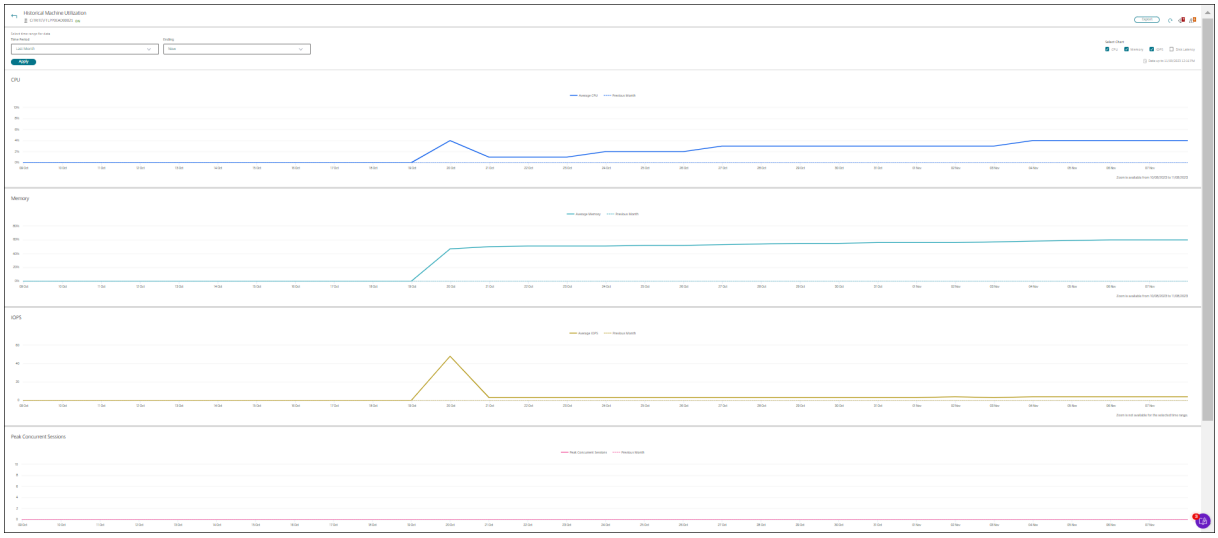
Os dados de utilização da CPU e da memória, média de IOPS e latência de disco são coletados por

padrão. Você pode desativar a coleta usando a configuração de política **Enable Resource Monitoring**.

1. No painel **Machine Utilization**, na exibição **Machine Details**, selecione **View Historical Utilization**.
2. Na página **Historical Machine Utilization**, defina **Time Period** para ver o uso nas últimas 2 horas, 24 horas, 7 dias, mês ou ano.

   > **Nota:**
   >
   > Os dados de uso médio de IOPS e latência de disco estão disponíveis somente para as últimas 24 horas, para o último mês e para o último ano até agora, onde Ending é definido como “now”. A hora de término personalizada não é suportada.

3. Clique em **Apply** e selecione os gráficos necessários.
4. Passe o mouse sobre diferentes seções do gráfico para exibir mais informações para o período selecionado.



Por exemplo, se você selecionar **Last 2 hours**, o período da linha de base será as 2 horas antes do intervalo de tempo selecionado. Exiba a tendência de CPU, memória e sessão nas últimas 2 horas e no horário da linha de base. Se você selecionar **Last month**, o período da linha de base será o mês anterior. Selecione para exibir a IOPS média e a latência do disco entre o último mês e o período da linha de base.

1. Clique em **Export** para exportar os dados de utilização do recurso 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: Application Name, User Name, Session ID, Average CPU, Peak CPU, Average Memory e Peak Memory para o período de tempo selecionado. As colunas IOPS e Disk Latency não podem ser ordenadas.

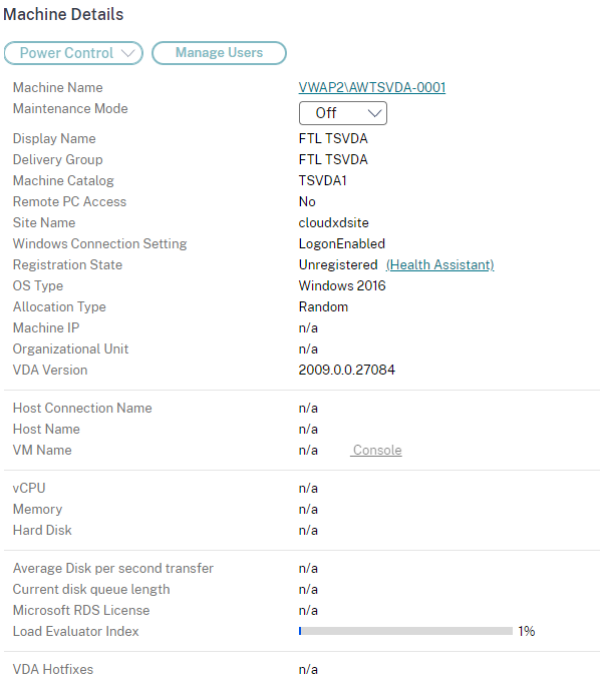
   > **Nota:**
   >
   > - O ID da sessão para processos do sistema é exibido como “0000”.
   > - Se um site pertencente ao plano Citrix Cloud Japan ou ao plano Citrix Cloud Government contiver mais de 5.000 máquinas, os dados do processo estarão disponíveis somente para até 2.000 máquinas. A política de monitoramento de processos Process Monitoring deve estar ativada nessas máquinas.

3. Para exibir a tendência histórica de consumo de recursos de um processo específico, aprofunde-se nos detalhes de qualquer um dos 10 principais processos.

Acesso ao console da máquina

Você pode acessar os consoles de máquinas com SO de sessão única e áreas de trabalho hospedadas no XenServer versão 7.3 e posterior diretamente do Monitor. Dessa forma, você não precisa do Xen-

Center 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.

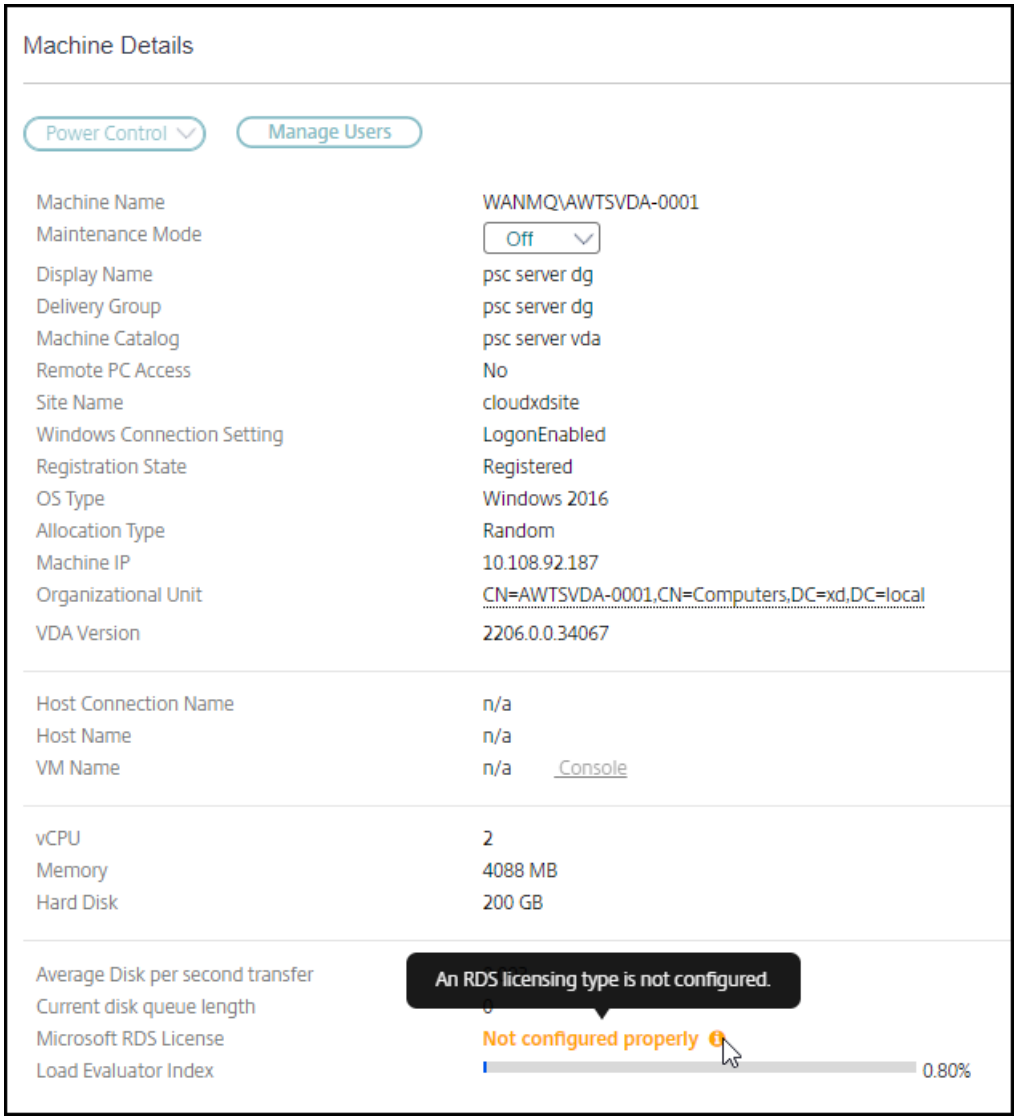


Para solucionar problemas de uma máquina, clique no link **Console** no painel Machine Details correspondente. Após a autenticação das credenciais de host fornecidas, o console da máquina é aberto em uma guia separada usando noVNC, um cliente VNC baseado na Web. Agora você tem acesso ao console pelo teclado e mouse.

> **Nota:**
>
> - Esse recurso não é suportado no Internet Explorer 11.
> - Se o ponteiro do mouse no console da máquina estiver desalinhado, consulte CTX230727 para ver as etapas para corrigir o problema.
> - O acesso ao console é iniciado em uma nova guia, portanto, certifique-se de que as configurações do navegador permitam pop-ups.
> - Por motivos de segurança, a Citrix recomenda que você instale certificados SSL em seu navegador.

Integridade da licença do Microsoft RDS

Você pode exibir o status da licença do Microsoft RDS no painel Machine Details na página **Machine Details** e **User Details** para máquinas com SO multissessão.



Uma das seguintes mensagens é exibida:

- License available
- Not configured properly (aviso)
- License error (erro)
- Incompatible VDA version (erro)

> **Nota:**
>
> O status de integridade da licença do RDS para máquinas em período de tolerância com licença válida exibe a mensagem **License available** em verde. Renove sua licença antes que ela expire.

Nas mensagens de aviso e erro, passe o mouse sobre o ícone de informações para exibir informações adicionais conforme indicado na tabela a seguir.

Tipo da mensagem	Mensagens no Monitor
Erro	Disponível para VDAs versão 7.16 e posterior.
Erro	Novas conexões RDS não são permitidas.
Erro	O licenciamento do RDS excedeu seu período de tolerância.
Erro	Não há nenhum servidor de licenças configurado para o nível de SO necessário com o tipo de licenciamento Per Device Client Access.
Erro	O servidor de licenças configurado não é compatível com o nível RDS Host OS com o tipo de licenciamento Per Device Client Access.
Aviso	Personal Terminal Server não é um tipo de licenciamento RDS válido em uma implantação do Citrix Virtual Apps and Desktops.
Aviso	Remote Desktop for Administration não é um tipo de licenciamento válido em uma implantação do Citrix Virtual Apps and Desktops.
Aviso	Nenhum tipo de licenciamento RDS não está configurado.
Aviso	O controlador de domínio ou o servidor de licenças não pode ser acessado com o tipo de licenciamento RDS Per User Client Access.
Aviso	Com o tipo de licenciamento Per Device Client Access, a licença Client Device não poderia ser determinada, pois o servidor de licenças para o nível de SO necessário não está acessível.

> **Nota:**
>
> Esse recurso é aplicável somente para Microsoft RDS CAL (Client Access License).

Métricas do dispositivo de destino PVS

Você pode exibir o status dos dispositivos de destino PVS para máquinas de SO de sessão única e multissessão na página **Machine Details** no Director. Várias métricas de **Network**, **Boot** e **Cache** estão disponíveis nesse painel. Essas métricas ajudam você a monitorar e solucionar problemas de dispositivos de destino PVS para garantir que estejam em condições de funcionamento adequadas.

PVS Target Device Metrics

Network		Boot		Cache	
NIC Bandwidth Utilization (%)	12	Boot Bytes Read MB	231	Write Cache Type	Device RAM with overflow on local har...
Server Reconnect Count	5	Boot Bytes Written MB	0	Write Cache Volume Drive Letter	D:
Total UDP Retry Count	7	Boot From	vDisk	Write Cache Volume Size MB	6142
		Boot Retry Count	0	Cache File Size MB	1058
		Boot Time (sec)	31	Ram Cache Usage MB	62.3125
		Target Software Version	7.23.0		
		VDisk Name	v10VDisk.vhdx		

Network:

- Network Bandwidth Utilization: utilização média da largura de banda em todas as NICs.
- Server Reconnect Count: número de vezes que o servidor se reconectou devido a problemas de rede ou rebalanceamento do servidor ou desligamentos e reinicializações do Citrix Provisioning Stream Service.
- Total UDP Retry Count: número de vezes que o dispositivo de destino do Provisioning tentou se reconectar ao servidor do Provisioning usando UDP. Essa métrica ajuda você a saber se há algum problema de rede no Citrix Provisioning Stream Service (por exemplo, configurações de comutador incorretas).

Boot:

- Boot Bytes Read MB: bytes lidos durante a inicialização.
- Boot Byes Written MB: bytes escritos durante a inicialização.
- Boot From: meio de inicialização (vDisk, disco local e assim por diante).
- Boot Retry Count: número de novas tentativas para inicializar a máquina.
- Boot Time: tempo necessário para inicializar a máquina, em segundos. Por padrão, há um atraso de 5 segundos entre as novas tentativas. Se esse atraso aumentar para dois dígitos, haverá um aumento significativo no tempo de inicialização. Verifique a configuração do Provisioning para resolver esse problema.
- Target Software Version: versão do software do dispositivo de destino do Provisioning.
- vDisk Name: o vDisk a partir do qual o dispositivo de destino do Provisioning está inicializando.

Cache:

- Write Cache Type: o vDisk pode ser definido para diferentes tipos de cache. Para obter mais informações, consulte o artigo do Knowledge Center CTX119469.
- Write Cache Volume Drive Letter: letra da unidade para tipos de cache de gravação envolvendo unidades.
- Write Cache Volume Size MB: tamanho total do volume configurado para cache de gravação.
- Cache File Size MB: tamanho do arquivo de cache atual (cache na RAM do dispositivo com estouro no disco rígido).

- Ram Cache Usage MB: tamanho atual do cache de RAM (cache na RAM do dispositivo com estouro no disco rígido). Use Overflow to disk somente se necessário. Essa métrica é útil ao configurar ou otimizar o tamanho adequado do cache de RAM.

Para obter mais informações, consulte Usando Status Tray em um dispositivo de destino.

As métricas do dispositivo de destino do Provisioning estão disponíveis somente em:

- Máquinas do Provisioning.
- Dispositivo de destino do Provisioning versão 7.19 e posterior.
- VDA versão 2003 e posterior.

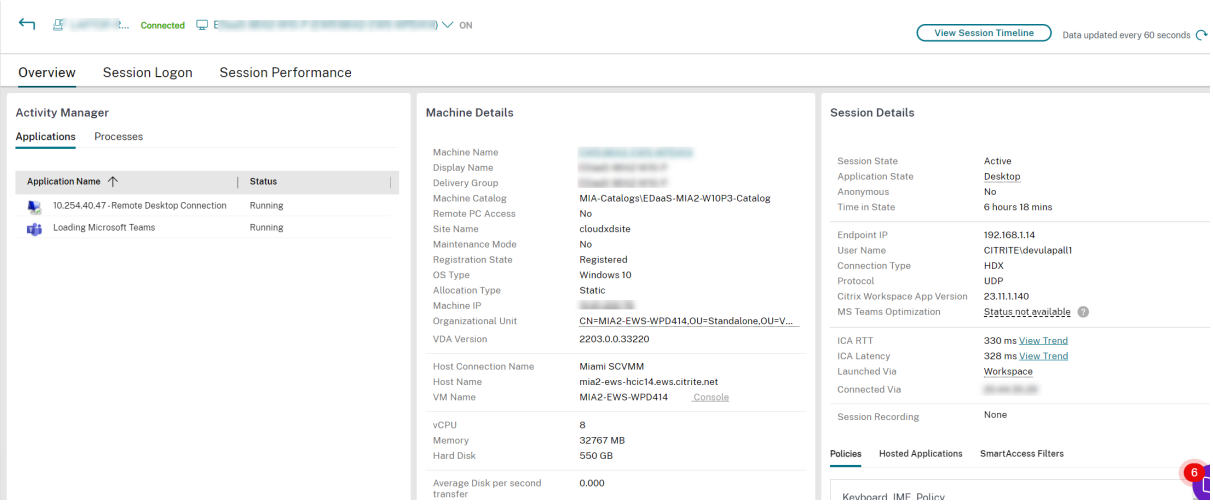
> **Nota:**
>
> As métricas de Server Reconnect Count e UDP Retry Count estão disponíveis apenas para a versão de destino do Provisioning 1912 CU2 e posterior.

Resolução de problemas de usuário

November 21, 2023

No Monitor, use a exibição **Help Desk** (página **Activity Manager**) para ver as informações sobre o usuário ou ponto de extremidade.

Clicar em **View Details** a partir do Activity Manager for User abre a página **User Details**.
Clicar em **View Details** a partir do Activity Manager for Endpoint abre a página **Endpoint Details**.



Se o usuário tiver iniciado mais de uma sessão, o seletor de sessão será exibido.

Escolha uma sessão para ver seus detalhes.

- Verificar os detalhes sobre a sessão, a experiência de login do usuário, a inicialização da sessão, a conexão e os aplicativos.
- Fazer a sombra da máquina do usuário.
- Solucionar problemas com as ações recomendadas na tabela a seguir e, se necessário, encaminhar um problema para o administrador apropriado.

Dicas de solução de problemas

Problema de usuário	Sugestões
O logon leva muito tempo ou falha intermitente ou repetidamente	Diagnosticar problemas de logon do usuário
A inicialização da sessão leva muito tempo ou falha intermitente ou repetidamente	Diagnosticar problemas de início da sessão
Identificar os componentes envolvidos no estabelecimento da sessão	Exibição da análise da topologia da sessão
A resposta da sessão é lenta ou não responde	Diagnosticar problemas de desempenho da sessão
O aplicativo está lento ou não responde	Resolver falhas de aplicativos
Falha na conexão	Restaurar conexões de área de trabalho
A sessão está lenta ou não está respondendo	Restaurar sessões
O vídeo está lento ou com baixa qualidade	Executar relatórios do sistema de canais HDX

> **Nota:**
>
> Para garantir que a máquina não esteja no modo de manutenção, na exibição User Details, revise os dados no painel Machine Details.

Desempenho da sessão

A guia **Session Performance** teve seus fluxos de trabalho aprimorados para a solução de problemas, começando com a capacidade de correlacionar métricas em tempo real para identificar problemas nas sessões do usuário. O painel **Session Topology** fornece uma representação visual do caminho da sessão de sessões HDX conectadas. O painel **Performance Metrics** fornece tendências das métricas da sessão, como ICARTT, latência ICA, quadros por segundo, largura de banda de saída disponível e largura de banda de saída consumida, ajudando a indicar o desempenho dessas métricas 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 conduzida em todos os Active Directories configurados.

Quando você digita um nome de máquina multiusuário em um campo de pesquisa, os detalhes da máquina da máquina especificada são exibidos em Machine Details.

Quando você digita um nome de ponto de extremidade em um campo de pesquisa, são listadas as sessões não autenticadas (anônimas) e as sessões autenticadas que estão conectadas a um

ponto de extremidade específico. Isso permite a solução de problemas de sessões não autenticadas. Certifique-se de que os nomes dos pontos de extremidade sejam exclusivos para habilitar a solução de problemas de sessões não autenticadas.

Os resultados da pesquisa também incluem usuários que não estão usando uma máquina no momento ou que não atribuídos a nenhuma máquina.

- As pesquisas não fazem distinção entre maiúsculas e minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome com duas partes (nome de usuário, nome de família ou nome de exibição), separadas por um espaço, os resultados incluem correspondências para as duas cadeias de caracteres. Por exemplo, se você digitar "jo rob", os resultados podem incluir cadeias de caracteres como "Joao Roberto"ou Roberta, Joana.

Para retornar à página inicial, clique na guia Monitor.

Diagnosticar problemas de inicialização de sessão

June 24, 2022

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 na duração de Workspace App Session Startup e na duração de VDA Session Startup nas páginas **User Details** e **Endpoint Details**. Essas duas durações contêm outras fases individuais cujas durações de inicialização também são exibidas. Esses dados ajudam você a entender e solucionar problemas de alta duração na inicialização da sessão. Além disso, a duração de tempo de cada fase envolvida na inicialização da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de mapeamento da unidade for alto, você poderá verificar se todas as unidades válidas estão mapeadas corretamente no GPO ou no 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:

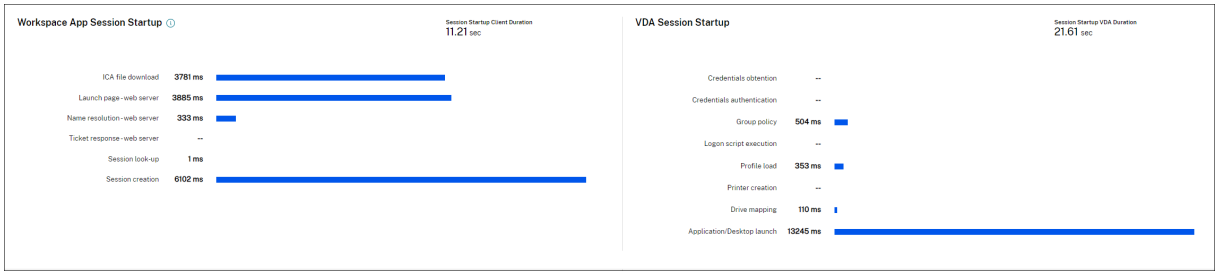
- VDA 1903 ou posterior.
- O serviço de monitoramento da experiência do usuário final da Citrix (EUEM) deve estar em execução no VDA.

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 somente para sessões HDX.
- Para inicializações de sessão a partir do iOS e do SO Android, somente a duração de inicialização do VDA está disponível.
- O IFDCD está disponível apenas quando o aplicativo Workspace é detectado durante a inicialização a partir de um navegador.
- Nas inicializações de sessão no macOS, o IFDCD está disponível apenas para o aplicativo Workspace 1902 e posterior.
- Nas inicializações de sessão em SO Windows, o IFDCD está disponível para o aplicativo Workspace 1902 e posterior. Para versões anteriores, o IFDCD é exibido apenas para inicializações de aplicativos no navegador com o aplicativo Workspace detectado.

> **Notas:**
>
> - Se você tiver problemas na exibição da duração da inicialização das sessões depois que os pré-requisitos forem atendidos, consulte os logs do VDA e do servidor do Monitor conforme descrito em CTX130320.
> Para sessões compartilhadas (vários aplicativos iniciados na mesma sessão), as métricas de inicialização do aplicativo Workspace são exibidas para a conexão mais recente ou a inicialização mais recente do aplicativo.
> - Algumas métricas na inicialização da sessão do VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.



Fases de inicialização da sessão do aplicativo Workspace

Session Startup Client Duration (SSCD)

Quando esta métrica é alta, ela indica um problema do lado do cliente que está causando tempos de inicialização prolongados. Revise as métricas subsequentes para determinar a provável causa raiz do

problema. SSCD inicia o mais próximo possível da hora da solicitação (clique do mouse) e termina quando a conexão ICA entre o dispositivo cliente e o VDA foi estabelecida. Em uma sessão compartilhada, essa duração é muito menor, já que muitos dos custos de configuração associados à criação de uma nova conexão com o servidor não são incorridos. No próximo nível abaixo, existem várias métricas detalhadas disponíveis.

ICA File Download Duration (IFDCD)

IFDCD é o tempo necessário para o cliente baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou área de trabalho) no aplicativo Workspace.
2. Uma solicitação do usuário é enviada para o StoreFront por meio do Citrix Gateway (se configurado), que envia a solicitação para o 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 ticket 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 necessário para o processo completo (etapas 1 a 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 estiver normal), o processamento da inicialização 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 potenciais de rede primeiro.

Launch Page Web Server Duration (LPWD)

Este é o tempo necessário para processar a página de inicialização (launch.aspx) no StoreFront. Se o LPWD estiver alto, pode haver um gargalo de informações no StoreFront.

As possíveis causas incluem:

- Alta carga no StoreFront. Tente identificar a causa da lentidão: verifique os logs e ferramentas de monitoramento dos Serviços de Informações da Internet (IIS), o Gerenciador de Tarefas, Monitor de Desempenho e outros.
- O StoreFront está tendo 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 há Delivery Controllers inativos ou sobrecarregados.

Name Resolution Web Server Duration (NRWD)

Este é o tempo gasto pelo Delivery Controller para resolver o nome de um aplicativo/área de trabalho publicado para um endereço IP de uma máquina VDA.

Quando essa métrica está alta, isso 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; por exemplo, o Delivery Controller está sobrecarregado ou há um problema no link de rede entre eles

Ticket Response Web Server Duration (TRWD)

Esta duração indica o tempo que leva para obter um tíquete (se necessário) do servidor do Secure Ticket Authority (STA) ou do Delivery Controller. Quando essa duração é alta, o servidor STA ou o Delivery Controller estão sobrecarregados.

Session Look-up Client Duration (SLCD)

Esta duração representa o tempo necessário para consultar todas as sessões para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode lidar com a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

Session Creation Client Duration (SCCD)

Esta duração representa o tempo necessário para criar uma sessão, do momento em que o wfica32.exe (ou um arquivo equivalente) é iniciado até o momento em que a conexão é estabelecida.

Fases de inicialização da sessão VDA

Session Startup VDA Duration (SSVD)

Esta duração é a métrica de inicialização de conexão do lado do servidor de alto nível que indica o tempo que o VDA leva para executar toda a operação de inicialização. Quando essa métrica é alta, isso indica que há um problema com o VDA que aumenta os tempos de inicialização da sessão. Isso inclui o tempo gasto no VDA executando toda a operação de inicialização.

Credentials Obtention VDA Duration (COVD)

O tempo necessário para que o VDA obtenha as credenciais do usuário.

Essa duração pode ser inflada artificialmente se um usuário não fornecer credenciais em tempo hábil, portanto, ela não é incluída na VDA Startup Duration. Esse tempo provavelmente será significativo somente 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).

Credentials Authentication VDA Duration (CAVD)

Este é o tempo gasto pelo VDA para autenticar as credenciais do usuário no provedor de autenticação, que pode ser Kerberos, Active Directory ou SSPI (Security Support Provider Interface).

Group Policy VDA Duration (GPVD)

Esta duração é o tempo necessário para aplicar objetos de política de grupo durante o logon.

Login Script Execution VDA Duration (LSVD)

Este é o tempo gasto pelo VDA para executar os scripts de login do usuário.

Você pode tornar os scripts de login do usuário ou do grupo assíncronos. Otimize os scripts de compatibilidade de aplicativos ou use variáveis de ambiente em seu lugar.

Profile Load VDA Duration (PLVD)

Este é o tempo gasto pelo VDA para carregar o perfil do usuário.

Se essa duração for alta, verifique a configuração do seu perfil de usuário. O tamanho e a localização do perfil de roaming contribuem para o início lento da sessão. Quando um usuário faz logon em uma sessão em que os perfis de roaming e as pastas iniciais do Terminal Services estão habilitados, o conteúdo do perfil de roaming e o acesso à pasta são mapeados durante o logon, o que exige recursos extras. Às vezes, isso pode consumir uma quantidade significativa do uso da CPU. Use as pastas **base do Terminal Services** com pastas pessoais redirecionadas para mitigar o 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 os tempos de logon estiverem lentos, verifique se o software antivírus está bloqueando a ferramenta Citrix Profile Management.

Printer Creation VDA Duration (PCVD)

Este é o tempo necessário para que o VDA mapeie as impressoras cliente do usuário de forma síncrona. Se a configuração estiver definida para que a criação da impressora seja executada de forma assíncrona, nenhum valor é registrado em PCVD, pois isso não afeta a conclusão da inicialização da sessão.

O tempo excessivo gasto em impressoras de mapeamento geralmente resulta das configurações da política de criação automática da impressora. O número de impressoras adicionadas localmente aos 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 todas as impressoras mapeadas localmente no dispositivo cliente. Reconfigure suas políticas de impressão para reduzir o número de impressoras criadas, especificamente quando os usuários tiverem muitas impressoras locais. Para isso, edite a política de criação automática da impressora no Delivery Controller e no Citrix Virtual Apps and Desktops.

Drive Mapping VDA Duration (DMVD)

Este é o tempo gasto pelo VDA para mapear as unidades, dispositivos e portas do cliente do usuário.

Certifique-se de que suas políticas básicas incluam configurações para desativar canais virtuais não utilizados, como mapeamento de porta de áudio ou COM, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

Application/Desktop Launch VDA Duration (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 o userinit.exe. O usernit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o explorer.exe, a interface de usuário do Windows. O userinit representa a duração entre o início do userinit.exe e o início da interface do usuário para o aplicativo ou área de trabalho virtual. A duração do Shell é o tempo entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

Session Creation VDA Duration (SCVD)

Este tempo inclui atrasos diversos na criação da sessão no VDA.

Diagnosticar problemas de logon do usuário

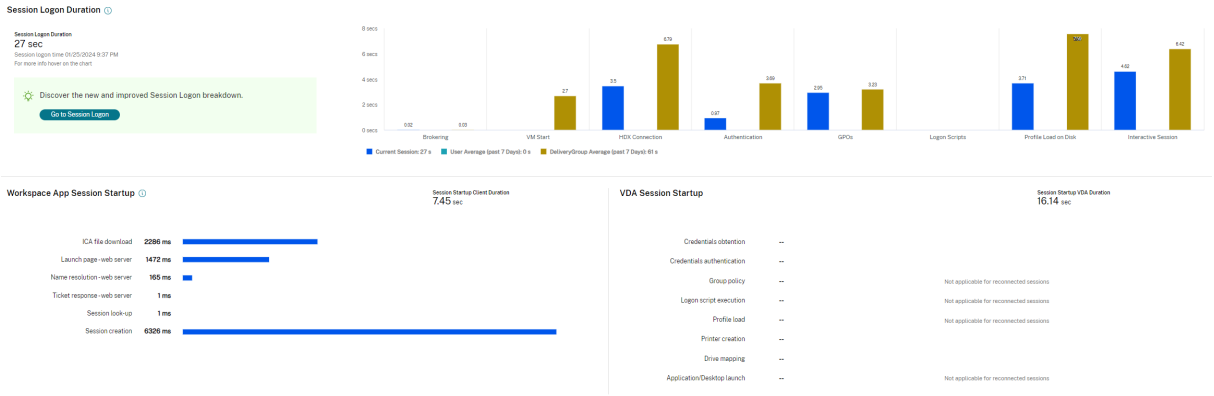
November 21, 2023

Use os dados em Logon Duration para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a uma área de trabalho ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o protocolo RDP 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.

Na exibição User Details, a duração é exibida como um valor numérico, abaixo do qual é exibido o horário em que o logon ocorreu e um gráfico das fases do processo de logon.

À medida que os usuários fazem logon no Citrix Virtual Apps and Desktops, o Monitor Service acompanha as fases do processo de logon desde o momento em que o usuário se conecta no aplicativo Citrix Workspace até o momento em que a área de trabalho está pronta para uso.



O número grande à esquerda é o tempo total de logon e é calculado combinando o tempo gasto estabelecendo a conexão e obtendo uma área de trabalho do Delivery Controller com o tempo gasto para autenticar e fazer logon em uma área de trabalho virtual. As informações de duração são apresentadas em segundos (ou frações de segundo).

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que sejam exibidos os dados de duração de logon e os detalhes:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Citrix Profile Management Service esteja em execução.

3. Para os sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Do not process the legacy run list**.
4. O acompanhamento do processo de auditoria deve estar ativado para o detalhamento em Interactive Session.
5. Para o detalhamento do GPO, aumente o tamanho dos logs operacionais da política de grupo.

> **Nota:**
>
> A duração do logon é suportada somente no shell padrão do Windows (explorer.exe) e não em shells personalizados.

Etapas para solucionar problemas de logon do usuário

1. Na exibição **User Details**, solucione os problemas de estado do logon usando o painel Logon Duration.
   - Se o usuário estiver fazendo logon, a exibição refletirá o processo de logon.
   - Se o usuário estiver conectado, o painel Logon Duration exibirá o tempo que foi necessário para o usuário fazer logon na sessão atual.
2. Examine as fases do processo de logon.

Fases do processo de logon

Brokering

Tempo que foi necessário para decidir qual área de trabalho atribuir ao usuário.

VM Start

Se a sessão exigiu um início da máquina, este é o tempo que foi necessário para iniciar a máquina virtual.

HDX Connection

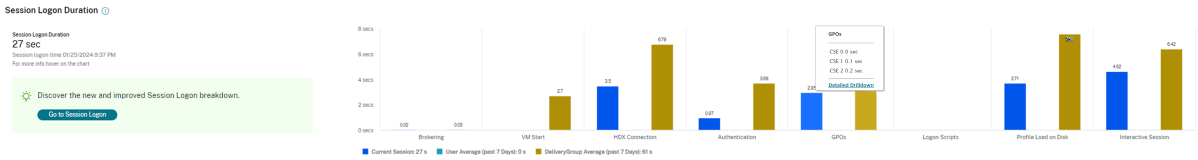
Tempo que foi necessário para concluir as etapas necessárias na configuração da conexão HDX do cliente com a máquina virtual.

Autenticação

Tempo que foi necessário para concluir a autenticação com a sessão remota.

GPOs

Se as configurações da política e grupo estiverem ativadas nas máquinas virtuais, esse é o tempo que foi necessário para aplicar objetos da política de grupo durante o logon. O detalhamento do tempo que foi necessário para aplicar cada política de acordo com os CSEs (extensão do lado do cliente) está disponível como dica de ferramenta quando você passa o mouse sobre a barra de GPO.



Clique em **Detailed Drilldown** para ver uma tabela com o status da política e o nome do objeto de política de grupo 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 a solução de problemas ou para usar em relatórios. O tempo de GPO para as políticas é recuperado dos logs no visualizador de eventos. Os logs podem ser substituídos dependendo da memória alocada para os logs operacionais (o tamanho padrão é de 4 MB). Para obter mais informações sobre como aumentar o tamanho de log para os logs operacionais, consulte o artigo do Microsoft TechNet https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

Logon Scripts

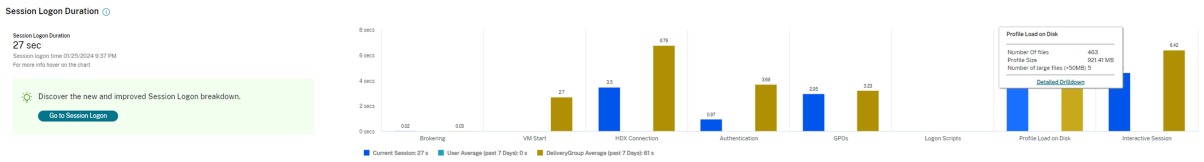
Se os scripts de logon estiverem configurados para a sessão, esse é o tempo que foi necessário para que os scripts de logon fossem executados.

Profile Load

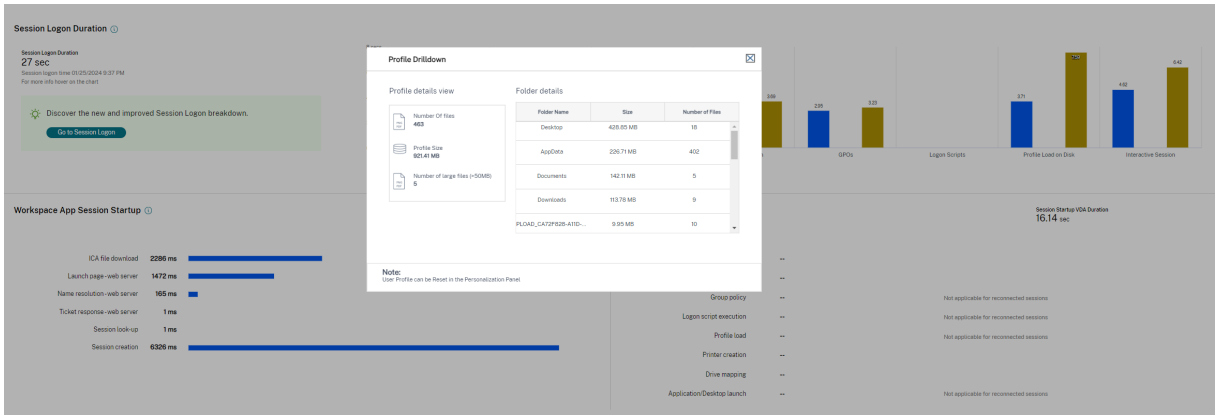
Se as configurações de perfil estiverem definidas para o usuário ou a máquina virtual, esse é o tempo que foi necessário para o perfil carregar.

Se o Citrix Profile Management estiver configurado, a barra de carregamento do perfil inclui o tempo gasto pelo Citrix Profile Management para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management é configurado, a barra de carregamento de perfil exibe uma duração maior. Esse aumento é causado por esse aprimoramento e não reflete degradação do desempenho. Esse aprimoramento está disponível em VDAs 1903 e posteriores.

Passe o mouse sobre a barra Profile Load para ver uma dica de ferramenta mostrando os detalhes do perfil do usuário da sessão atual. Essa informação adicional pode ajudar a solucionar problemas de carga de alto perfil.



Clique em **Detailed Drilldown** para se aprofundar mais em cada pasta individual na pasta raiz do perfil (por exemplo, C:/Users/nome_de_usuário), ver seu tamanho e o número de arquivos (incluindo arquivos dentro das pastas aninhadas).



O detalhamento do perfil está disponível no VDAs 1811 e posteriores. Usando as informações de detalhamento do perfil, você pode resolver problemas que envolvem um tempo longo de carregamento de perfil. Você pode:

- Redefinir o perfil do usuário
- Otimizar o perfil removendo arquivos grandes desnecessários
- Reduzir o número de arquivos para reduzir a carga da rede
- Usar streaming de perfil

Por padrão, todos os nomes de pastas ficam visíveis. Para ocultar o nome das pastas, edite o valor dos registros na máquina VDA seguindo estas etapas:

> **Aviso:**
>
> Adicionar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale 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 conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

1. No VDA, adicione um novo valor de registro **ProfileFoldersNameHidden** HKEY_LOCAL_MACHINE\Software\C
2. Defina o valor como 1. Esse valor deve ser um valor DWORD (32 bits). A visibilidade do nome das pastas agora está desativada.
3. Para deixar o nome das pastas visível novamente, defina o valor como 0.

> **Nota:**
>
> Você pode usar GPO ou PowerShell para aplicar a alteração de valor do registro em várias máquinas. Para obter mais informações sobre como usar o objeto de política de grupo para implantar alterações no registro, consulte o blog.

Informações adicionais

- O detalhamento de perfil não considera as pastas redirecionadas.
- Os arquivos NTUser.dat na pasta raiz podem não estar visíveis para os usuários finais. No entanto, eles são incluídos no detalhamento do perfil e exibidos na lista de arquivos em **Root Folder**.
- Existem alguns arquivos ocultos na pasta AppData que não estão incluídos no detalhamento do perfil.
- O número de arquivos e dados do tamanho do perfil talvez não correspondam aos dados no painel Personalization devido a certas limitações do Windows.

Interactive Session

Este é o tempo que foi necessário para "entregar"o controle do teclado e do mouse para o usuário após o carregamento do perfil do usuário. Normalmente, esta 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 de Desktop Ready Event (EventId 1000 no VDA) - carimbo de data/hora de User Profile Loaded Event (EventId 2 no VDA)**. Interactive Session tem três subfases: Pre-userinit, Userinit e Shell. Passe o mouse sobre Interactive Session para ver uma dica de ferramenta mostrando o seguinte:

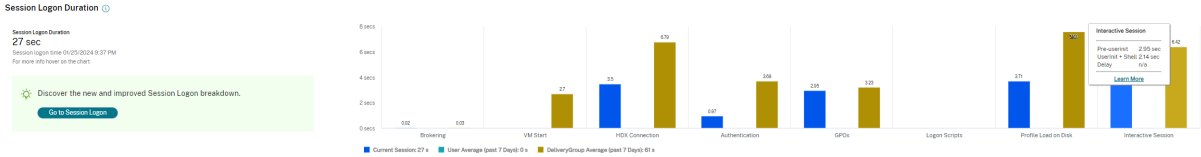
- subfases
- o tempo que foi necessário para cada subfase
- o tempo total de atraso acumulado entre essas subfases

> **Nota:**
>
> Esse recurso está disponível nos VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores a 7.18 e depois atualizou para a versão 7.18, é exibida a mensagem "Drilldown unavailable due to server error". No entanto, se você iniciou as sessões após uma atualização, nenhuma mensagem de erro é exibida.

Para exibir a duração do tempo de cada subfase, ative o acompanhamento do processo Audit na máquina virtual (VDA). Quando o acompanhamento do processo de auditoria está desativado (padrão), a duração de Pre-userinit e a duração combinada de Userinit e Shell são exibidas. Você pode ativar o acompanhamento do processo de auditoria através de um objeto de política de grupo (GPO) da seguinte forma:

1. Crie um objeto de política de grupo 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 **Auditoria de acompanhamento de processos**.
4. Selecione **Sucesso** e clique em OK.
5. Aplique este objeto de política de grupo aos VDAs ou grupo necessários.

Para obter mais informações sobre a auditoria de acompanhamento de processos e ativá-la ou desativá-la, consulte https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) na documentação da Microsoft.



Painel Logon Duration na exibição User Details.

- **Interactive Session –Pre-userinit:** este é o segmento de Interactive Session que se sobrepõe a objetos de política de grupo e scripts. Essa subfase pode ser reduzida otimizando os GPOs e os scripts.
- **Interactive Session –Userinit:** quando um usuário faz logon em uma máquina Windows, o Winlogon executa o userinit.exe. O userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface de usuário do Windows. Essa subfase do Interactive Session representa a duração entre o início do userinit.exe e o início da interface do usuário da área de trabalho ou aplicativo virtual.
- **Interactive Session –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.
- **Delay:** este é o atraso de tempo cumulativo entre as subfases **Pre-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 somatória.
O tempo total de logon não inclui o tempo ocioso do ICA, que é o tempo entre o download do arquivo ICA e o início do arquivo ICA para um aplicativo.
Para habilitar a abertura automática do arquivo ICA no momento da inicialização do aplicativo, configure seu navegador para iniciar o arquivo ICA automaticamente após o download de um arquivo ICA. Para obter mais informações, consulte CTX804493.

> **Nota:**

> O gráfico Logon Duration mostra as fases de logon em segundos. Os 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 maior valor do eixo y em 200 segundos. Qualquer valor maior que 200 segundos é mostrado com o valor real exibido acima da barra.

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 do usuário nos últimos sete dias e a duração média de todos os usuários no grupo de entrega nos últimos sete dias.

Encaminhe a outros colegas conforme necessário. Por exemplo, se a inicialização da máquina virtual estiver lenta, o problema pode estar no Hypervisor, portanto, você pode encaminhá-lo para o administrador do Hypervisor. Ou, se o tempo de intermediação do agente for lento, você pode encaminhar o problema para o administrador do site para verificar o balanceamento de carga no Delivery Controller.

Examine diferenças incomuns, incluindo:

- Barras de logon ausentes (atuais)
- Grande discrepância entre a duração atual e a duração média do usuário. As causas incluem:
  - Um novo aplicativo foi instalado.
  - Ocorreu uma atualização do sistema operacional.
  - Foram feitas mudanças de configuração.
  - O tamanho do perfil do usuário é alto. Nesse caso, a carga do perfil em Profile Load está alta.
- Grandes discrepâncias entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

Se necessário, clique em **Restart** para observar o processo de logon do usuário para solucionar os problemas, por exemplo, em VM Start ou Brokering.

Sombrear usuários

November 17, 2022

Use o recurso de sombreamento de usuário 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, verifique o nome da máquina listado na barra de título do usuário.

O sombreamento é iniciado em uma nova guia; atualize as configurações do navegador para permitir pop-ups do URL do Citrix Cloud.

Acesse o recurso de sombreamento na exibição **User Details**. Selecione a sessão do usuário e clique em **Shadow** na exibição do Activity Manager ou no painel Session Details.

Sombreamento de Linux VDAs

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

> **Nota:**
>
> - 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 x11vnc instalados.
> - A conexão do 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 do Monitor e Linux VDA.

Siga as instruções em Session Shadowing para configurar seu VDA para sombreamento.

1. Depois que você clicar em **Shadow**, 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.

Sombreamento de Windows VDAs

As sessões do Windows VDA são sombreadas usando a Assistência Remota do Windows. Ative o recurso User Windows Remote Assistance durante a instalação do VDA. Para obter mais informações, consulte Ativar ou desativar recursos.

1. Depois de clicar em **Shadow**, a conexão de sombreamento 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 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.

Agilizar os navegadores Microsoft Internet Explorer para o sombreamento

Configure o navegador Microsoft Internet Explorer para abrir automaticamente o arquivo Microsoft Remote Assistance (.msra) baixado com o cliente de Assistência Remota.

Para isso, você deve ativar a configuração de aviso automático para o download 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 > Aviso automático para downloads de arquivo.

Enviar mensagens para usuários

May 3, 2022

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 reinicializações de máquinas e redefinições de perfis.

Para enviar uma mensagem para um usuário, siga estas etapas:

1. Vá para **Monitor** > **Filters** > **Machines** > **All Machines**.
2. Selecione uma máquina para a qual deseja enviar uma mensagem e clique em **Send Message**.
3. Digite sua mensagem e clique em **Send**.

Se a mensagem for enviada com sucesso, uma mensagem de confirmação é exibida. Se a máquina do usuário estiver conectada, a mensagem aparecerá nela.

Se a mensagem não for enviada com sucesso, uma mensagem de erro aparece. Solucione o problema de acordo com a mensagem de erro. Quando terminar, digite o assunto e o texto da mensagem novamente e clique em Try novamente.

Resolver falhas de aplicativos

February 16, 2023

Na exibição **Activity Manager**, clique na guia **Applications**. Você pode visualizar todos os aplicativos em todas as máquinas às quais o usuário tem acesso, incluindo aplicativos locais e hospedados para a máquina conectada atualmente e o status de cada um.

A lista inclui apenas os aplicativos que foram iniciados dentro da sessão.

Para máquinas com SO multissessão 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 **End Application**. Depois 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 **Processes**. Selecione um processo relacionado ao aplicativo ou usando uma grande quantidade de recursos da CPU ou memória e clique em **End Process**. 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 em máquinas com SO de sessão única, na sessão selecionada, clique em **Restart**. Como alternativa, na exibição Machine Details, use os controles de energia para reiniciar ou desligar a máquina. Instrua o usuário a fazer logon novamente para que você possa verificar novamente o aplicativo. Para máquinas com SO multissessão, a opção de reinicialização não está disponível. Em vez disso, faça logoff do usuário e deixe que o usuário faça logon novamente.
Colocar a máquina no modo de manutenção	Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina no modo de manutenção. Na exibição Machine Details, clique em **Details** e ative a opção de modo de manutenção. Encaminhe para o administrador apropriado.

Desativar a visibilidade de aplicativos em execução

Por padrão, o Activity Manager 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 Activity Manager. Para funções de administrador delegado, inclui administrador completo, administrador de grupo de entrega e administrador de assistência técnica.

Para proteger a privacidade dos usuários e os aplicativos que estão executando, você pode desativar a guia Applications para listar aplicativos em execução. Para isso, no VDA, modifique a chave de 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 Activity Manager.

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do 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. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Restaurar conexões da área de trabalho

July 1, 2022

No Monitor, verifique o status da conexão do usuário da máquina atual na barra de título do usuário.

Se a conexão da área de trabalho falhar, o erro que causou a falha é exibido e pode ajudá-lo a decidir como solucionar o problema.

Ação	Descrição
Assegurar que a máquina não está no modo de manutenção	Na página User Details, verifique se o modo de manutenção está desativado.
Reiniciar a máquina do usuário	Selecione a máquina e clique em **Restart**. Use essa opção se a máquina do usuário não responder ou não conseguir se conectar, como quando a máquina está usando uma quantidade excepcionalmente alta de recursos da CPU, o que pode tornar a CPU inutilizável.

Restaurar sessões

July 1, 2022

Se uma sessão for desconectada, ela permanece ativa e seus aplicativos continuam em execução, mas o dispositivo do usuário não se comunica mais com o servidor.

Na exibição User Details, solucione problemas de falhas de sessão no painel **Session Details**. Você pode exibir os detalhes da sessão atual, indicados pelo ID da sessão.

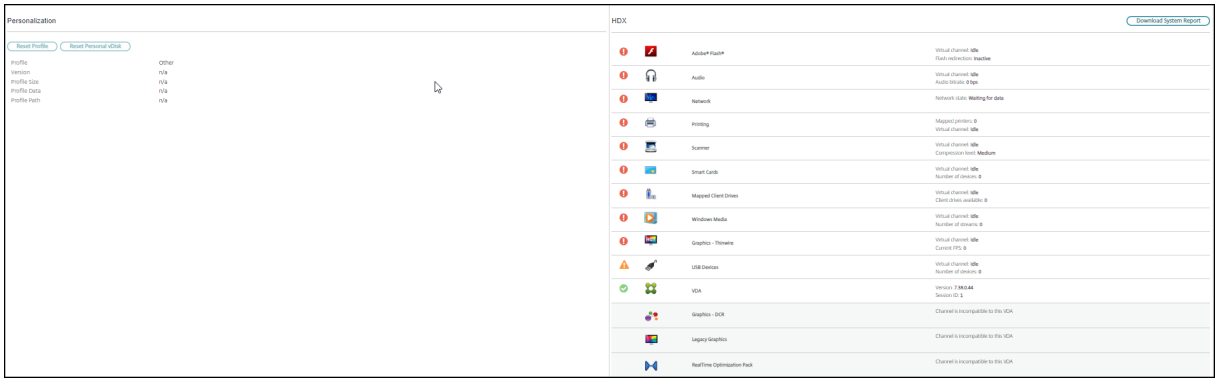
Ação	Descrição
Encerrar aplicativos e processos que não estão respondendo	Clique na guia **Applications**. Selecione o aplicativo que não está respondendo e clique em **End Application**. Da mesma forma, selecione um processo correspondente que não esteja respondendo e clique em **End Process**. Além disso, encerre os processos que estão consumindo uma quantidade excepcionalmente alta de memória ou recursos de CPU, o que pode tornar a CPU inutilizável.
Desconectar a sessão do Windows	Clique em **Session Control** e selecione **Disconnect**. Essa opção está disponível somente para máquinas com SO multissessão intermediado pelo agente. Para sessões não intermediadas, a opção está desativada.
Faça o logoff do usuário da sessão	Clique em **Session Control** e selecione **Log Off**.

Para testar a sessão, o usuário pode tentar fazer logon novamente. Você também pode sombrear o usuário para monitorar a sessão mais de perto.

Executar relatórios do sistema de canais HDX

November 21, 2023

Na exibição **User Details**, verifique o status dos canais HDX na máquina do usuário no painel HDX. Esse painel só estará disponível se a máquina do usuário estiver conectada usando HDX.



Se aparecer uma mensagem indicando que as informações não estão disponíveis no momento, aguarde um minuto até que a página seja recarregada 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 exibir 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 canal HDX são usados principalmente pelo suporte Citrix para solucionar problemas. Para isso, no painel HDX, clique em **Download System Report**.

Redefinir um perfil de usuário

May 3, 2022

> **Cuidado:**
>
> Quando um perfil é redefinido, embora as pastas e os 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 **Reset Profile**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente. As pastas e os 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 usuário a fazer logon novamente na mesma área de trabalho ou aplicativo que o usuário informou como um problema. Isso garante que o perfil correto seja redefinido. Para um perfil de usuário da Citrix, o perfil já estará redefinido no momento em que a área de trabalho do usuário for exibida. Para um perfil de roaming da Microsoft, a restauração da pasta poderá continuar em andamento por um breve período. O usuário deve permanecer conectado até que a restauração esteja concluída.

As etapas anteriores pressupõem que você esteja usando o Citrix Virtual Desktops (VDA de área de trabalho). Se você estiver usando o Citrix Virtual Desktops (VDA de servidor), deverá estar conectado para executar a redefinição do perfil. O usuário precisa fazer logoff e logon novamente para concluir a redefinição do perfil.

Se o perfil não for redefinido com êxito (por exemplo, o usuário não puder efetuar logon novamente na máquina ou alguns dos arquivos estiverem ausentes), você deverá restaurar manualmente o perfil original.

As pastas (e seus arquivos) do perfil do usuário são salvas e copiadas para o novo perfil. Eles são copiados na ordem listada:

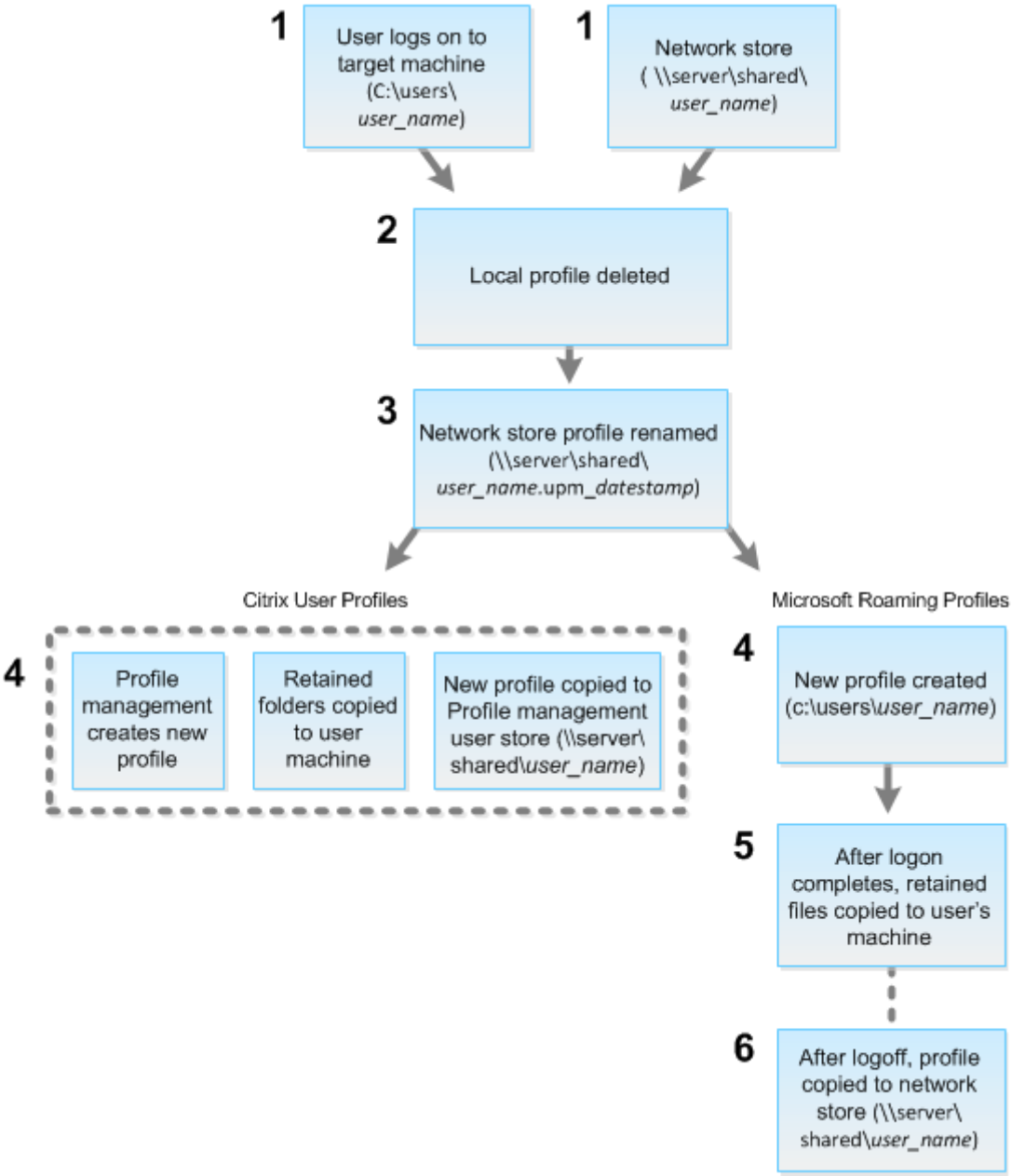
- Área de Trabalho
- Cookies
- Favoritos
- Documentos
- Imagens
- Música
- Vídeos

> **Nota:**
>
> No Windows 8 e posterior, os cookies não são copiados quando os perfis são redefinidos.

Como os perfis de redefinição são processados

Qualquer perfil de usuário da Citrix ou perfil de roaming da Microsoft pode ser redefinido. Depois que o usuário fizer logoff e você selecionar o comando reset (no Monitor ou usando o PowerShell SDK), o Monitor primeiro identifica o perfil do usuário em uso e emite um comando de redefinição apropriado. O Monitor recebe as informações através do Profile Management, incluindo informações sobre o tamanho do perfil, o tipo e os horários de logon.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.



O comando reset emitido pelo Monitor especifica o tipo de perfil. Depois, o serviço Profile Management tenta redefinir um perfil desse tipo e procura o compartilhamento de rede apropriado (armazenamento do usuário). Se o Profile Management processar o usuário, mas receber um comando de perfil de roaming, ele será rejeitado (ou vice-versa).

1. Se um perfil local estiver presente, ele será 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 da Citrix ou um perfil de roaming 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 de roaming for usado para a redefinição, todas as configurações do registro no perfil de roaming serão preservadas no perfil redefinido. Você pode configurar o Profile Management de modo que um perfil de modelo substitua o perfil de roaming, se necessário.

Para perfis de roaming 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 houver um.
3. Localize a pasta arquivada no compartilhamento de rede que contém a data e a hora anexadas ao nome da pasta, a pasta com a extensão .upm_datahora.
4. Exclua o nome de perfil atual. Ou seja, aquele sem a extensão .upm_datahora.
5. Renomeie a pasta arquivada usando o nome de perfil original. Ou seja, remova a extensão de data e hora. Você retornou o perfil ao estado original de pré-redefinição.

Matriz de compatibilidade de recursos

September 5, 2023

O Citrix Monitor oferece suporte a três edições do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). São elas, **Premium**, **Citrix DaaS Advanced** e **Citrix DaaS Advanced Plus**. Recursos específicos do Citrix Monitor, versões do VDA, componentes dependentes e suas respectivas edições de licença estão listados na tabela a seguir.

Recurso	Dependências – versão mínima necessária	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Utilização de GPU em tempo real disponível para GPUs AMD	VDA 7 2212 executando Windows 64 bits	Sim	Sim	Sim

Recurso	Dependências – versão mínima necessária	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Acesso aos detalhes da sessão do Citrix Analytics for Performance	Direito ao Citrix Analytics for Performance	Sim	Sim	Sim
Reconexão automática de sessão	VDA 1906	Sim	Sim	Sim
Duração do início da sessão	VDA 1903	Sim	Sim	Sim
Investigação da área de trabalho	Citrix Probe Agent 1903	Sim	Não	Não
Duração do Citrix Profile Management no carregamento do perfil	VDA 1903	Sim	Sim	Sim
Análise detalhada de perfil	VDA 1811	Sim	Sim	Sim
Monitoramento de alertas do Hypervisor	Nenhuma	Sim	Não	Não
Investigação de aplicativo	Citrix Application Probe Agent 1811	Sim	Não	Não
Integridade da licença do Microsoft RDS	VDA 7.16	Sim	Sim	Sim
Acesso ao console da máquina a partir do Monitor	XenServer Hypervisor 7.3	Sim	Sim	Sim
Exportação de dados de filtros	Nenhuma	Sim	Sim	Sim

Recurso	Dependências – versão mínima necessária	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Análise detalhada da sessão interativa	VDA 1808	Sim	Sim	Sim
Análise detalhada de GPO	VDA 1808	Sim	Sim	Sim
Dados históricos da máquina disponíveis usando a API OData	Nenhuma	Sim	Sim	Sim
Políticas de alertas inteligentes	Nenhuma	Sim	Não	Não
Link do Health Assistant	Nenhuma	Sim	Sim	Sim
Análise detalhada da sessão interativa	Nenhuma	Sim	Sim	Sim
Análise de aplicativos	VDA 7.15	Sim	Sim	Sim
OData API V.4	Nenhuma	Sim	Sim	Sim
Sombrear usuários Linux VDA	VDA 7.16	Sim	Sim	Sim
Acesso ao console da máquina	Nenhuma	Sim	Sim	Sim
Monitoramento de falhas de aplicativo	VDA 7.15	Sim	Sim	Sim

Recurso	Dependências – versão mínima necessária	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Solução de problemas centrada no aplicativo	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 claras de falhas de máquina e conexão	VDA 7.x	Sim	Sim	Sim
Retenção de dados históricos	VDA 7.x	Sim	Não	Não
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 ICA RTT	VDA 7.11	Sim	Não	Não
Melhorias de exportação de relatórios	VDA 7.x	Sim	Sim	Sim

Recurso	Dependências – versão mínima necessária	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Detalhamento da duração do logon	VDA 7.x	Sim	Sim	Sim
Monitoramento e alertas proativos	VDA 7.x	Sim	Não	Não
Uso de aplicativos hospedados	VDA 7.x	Sim	Não	Não
Uso de SO de sessão única e multissessão	VDA 7.x	Sim	Não	Não
Suporte para canal virtual Framehawk	VDA 7.6	Sim	Sim	Sim

Administração delegada e monitoramento

June 24, 2022

A administração delegada usa três conceitos: administradores, funções e escopos. As permissões são baseadas em uma função de administrador e no escopo dessa função. Por exemplo, um administrador pode receber uma função de administrador de assistência técnica em que o escopo envolve a responsabilidade pelos 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 chamadas de exibição.
- As áreas de trabalho, máquinas e sessões as quais o administrador pode visualizar e com elas interagir.
- Os comandos que o administrador pode executar, como sombrear a sessão de um usuário ou ativar o modo de manutenção.

O monitoramento agora oferece suporte a funções de administrador delegadas que permitem que você atribua aos administradores funções personalizadas definidas ou integradas. A função deter-

mina 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 aos quais a função é aplicável.

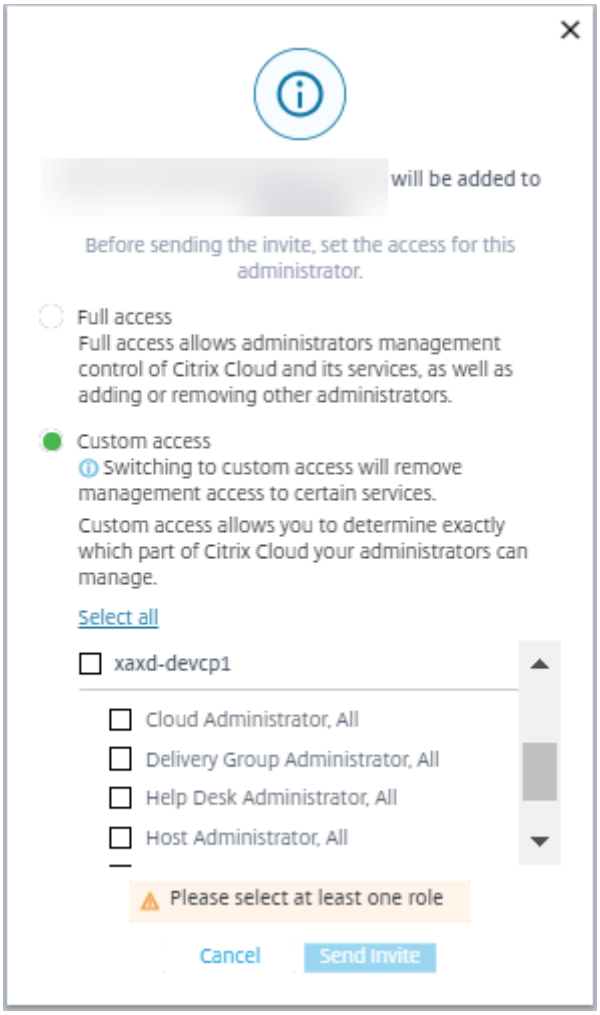
Para obter informações sobre a criação de administradores delegados, consulte o artigo principal Administração delegada.

As permissões e funções internas determinam como os administradores usam o **Monitor**:

Função do administrador	Permissões no Monitor
Full Administrator	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, ativar o modo de manutenção e exportar dados de tendências.
Delivery group Administrator	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, ativar o modo de manutenção e exportar dados de tendências.
Read Only Administrator	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 Export na exibição Trends. Não é possível executar nenhum outro comando nem alterar nada nas exibições.
Help Desk Administrator	Pode acessar somente as exibições Help Desk e User Details e pode exibir somente objetos que o administrador foi delegado para gerenciar. Pode sombrear a sessão de um usuário e executar comandos para esse usuário. Pode realizar operações no modo de manutenção. Pode usar opções de controle de energia para máquinas com SO de sessão única. Não pode acessar as exibições Dashboard, Trends, Alerts ou Filters. Não pode usar opções de controle de energia para máquinas com SO multissessão.
Machine catalog Administrator	Pode acessar somente a página Machine Details (pesquisa baseada em máquina).

Função do administrador	Permissões no Monitor
Host Administrator	Nenhum acesso. Este administrador não é compatível com o Monitor e não pode exibir dados.
Probe Agent Administrator	Acesso somente leitura à página Applications, não pode acessar nenhuma outra exibição. Destinado a executar o Citrix Probe Agent em máquinas de ponto de extremidade.
Monitoring Full Administrator	Tem acesso total a todas as exibições e comandos na guia **Monitor**.
Session Administrator	Pode exibir grupos de entrega e gerenciar suas sessões e máquinas associadas na página **Filters** da guia **Monitor**.

Para atribuir uma função (integrada ou personalizada) a um usuário, no menu Citrix Cloud, vá para **Identity and Access Management** > **Administrators**. Quando adicionar ou editar o acesso de um administrador, você pode selecionar **Custom Access** e uma das funções listadas.



Você pode definir funções e escopos personalizados em **Full Configuration > Administrators > Administrators**.

As funções internas e as funções personalizadas são listadas para seleção com escopo personalizado.

- [ ] [illegible]
  - [ ] 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

Granularidade e retenção de dados

January 17, 2023

Agregação de valores de dados

O Monitor Service coleta vários dados, incluindo uso de sessão do usuário, detalhes do desempenho de logon do usuário, detalhes do balanceamento de carga da sessão e informações de falha de máquina e conexão. Os dados são agregados de forma diferente, dependendo de sua categoria. Compreender a agregação de valores dos dados apresentados usando as APIs do método OData é fundamental para interpretar os dados. Por exemplo:

- Connected Sessions e Machine Failures ocorrem ao longo de um período. Portanto, são exibidas como máximos ao longo de um período de tempo.
- Logon Duration é uma medida de tempo, portanto, é exibida como uma média ao longo de um período de tempo.
- Logon Count e Connection Failures são contagens de ocorrências ao longo de um período, portanto, são exibidas como somas ao longo de um período de tempo.

Avaliação simultânea de dados

Suas sessões devem se sobrepor para serem consideradas simultâneas. No entanto, quando o intervalo de tempo é 1 minuto, todas as sessões nesse minuto (caso se sobreponham) são consideradas simultâneas. O tamanho do intervalo é tão pequeno que a sobrecarga de desempenho envolvida no cálculo da precisão não vale 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 as métricas de duas maneiras diferentes:

- As tabelas de resumo representam exibições agregadas das métricas granulares 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:

- **Não há dados resumidos para intervalos parciais.** Os resumos de métricas são projetados para atender às necessidades de tendências históricas por longos períodos. Essas métricas são agregadas na tabela de resumo para intervalos completos. Não há dados resumidos para um intervalo parcial no início (dados disponíveis mais antigos) da coleta de dados nem no final. Ao visualizar agregações de um dia (Interval=1440), isso significa que o primeiro dia e os dias incompletos mais recentes não têm dados. Embora possam existir dados brutos para esses intervalos parciais, eles nunca são resumidos. Extraia o SummaryDate mínimo e máximo 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 o comprimento 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 eventos brutos podem ser mais atuais no estado do que o que foi resumido para a análise de tendências. Qualquer comparação baseada em tempo entre dados de resumo e 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.** Métricas que são agregadas na tabela de resumo podem ser um pouco imprecisas se houver eventos perdidos ou latentes no período de agregação. Embora o Monitor Service tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo dos eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a HA de conexão, ocorrem lacunas nas contagens de dados resumidas das conexões atuais, mas as instâncias da sessão continuam em execução nos dados brutos.
- **Períodos de retenção de dados.** Os dados nas tabelas de resumo são retidos em uma programação de limpeza diferente da programação para dados brutos do evento. Os dados podem estar ausentes porque foram eliminados das tabelas de resumo ou de dados brutos. Os períodos de retenção também podem diferir para diferentes granularidades de dados de resumo. Dados de granularidade mais baixa (minutos) são eliminados mais rapidamente do que os dados de granularidade mais alta (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles podem ser encontrados em uma granularidade maior. 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 maior para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não caem em limites por hora, pode haver alguma discrepância quanto ao local em que 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 de uso, granularidade por hora
- T > 31 dias de uso, 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 somente dados relevantes sejam mantidos a longo prazo. Isso garante melhor desempenho, mantendo a granularidade necessária para a emissão de relatórios.

	Nome do parâmetro	Limpeza afetada	Dias de retenção para Premium	Dias de retenção para Advanced
1	GroomSessionsRetentionDays	Retenção dos registros de sessão e conexão após o encerramento da sessão	90	31
2	GroomFailuresRetentionDays	Registros de MachineFailureLog e ConnectionFailureLog	90	31
3	GroomLoadIndexRetentionDays	Registros LoadIndex	90	31

	Nome do parâmetro	Limpeza afetada	Dias de retenção para Premium	Dias de retenção para Advanced
4	GroomDeletedRetentionDays	Entidades de máquina, catálogo, grupo de áreas de trabalho e Hypervisor que têm LifecycleState como “"Deleted”. Isso também exclui todos os registros relacionados a Session, SessionDetail, Summary, Failure ou LoadIndex.	90	31
5	GroomSummariesRetentionDays	Registros DesktopGroupSummary, FailureLogSummary e LoadIndexSummary. Dados agregados - granularidade diária.	365	31
6	GroomMachineHotfixesRetentionDays	Hotfixes aplicados às máquinas VDA e Controller	90	31

	Nome do parâmetro	Limpeza afetada	Dias de retenção para Premium	Dias de retenção para Advanced
7	GroomHourlyRetentionDays	Dados agregados - granularidade por hora	32	31
8	GroomApplicationInstanceRetentionDays	Histórico de instância do aplicativo	90	Não aplicável
9	GroomNotificationLogRetentionDays	Registro de log de notificação	90	Não aplicável
10	GroomResourceUsageRawDataRetentionDays	Dados de utilização do recurso - dados brutos	3	3
11	GroomResourceUsageHourDataRetentionDays	Dados de resumo de utilização do recurso - granularidade por hora	30	30
12	GroomResourceUsageDayDataRetentionDays	Dados de resumo de utilização do recurso - granularidade por dia	365	31
13	GroomProcessUsageRawDataRetentionDays	Dados de utilização do processo - dados brutos	1	1
14	GroomProcessUsageHourDataRetentionDays	Dados de utilização do processo - granularidade por hora	7	7

	Nome do parâmetro	Limpeza afetada	Dias de retenção para Premium	Dias de retenção para Advanced
15	GroomProcessUsageDataRetentionDays	Dados de utilização do processo - granularidade por dia	30	30
16	GroomSessionMetricsDataRetentionDays	Dados de métricas de sessão	1	1
17	GroomMachineMetricsDataRetentionDays	Dados de métricas de máquina	3	3
18	GroomMachineMetricsSummaryDataRetentionDays	Dados de resumo de métricas de máquina	365	31
19	GroomApplicationDataRetentionDays	Dados do aplicativo	1	1
20	GroomApplicationFaultDataRetentionDays	Dados de falha do aplicativo	1	1

> **Cuidado:**
>
> Você não pode modificar os valores no banco de dados do Monitor Service.

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. Como os dados do painel são extraídos dessa tabela, os requisitos no servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto drástico no desempenho.

- **Dados de sessão e evento.** Estes são os dados coletados toda vez que uma sessão é iniciada

e uma conexão/reconexão é feita. Em um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, em dois anos, essas tabelas reuniriam mais de um TB de dados, exigindo um banco de dados de nível empresarial de alta capacidade.

Diagnóstico de início de sessão

September 5, 2023

> **Nota:**
>
> O diagnóstico de início da sessão está atualmente na fase Preview.

Os inícios de sessão envolvem vários componentes Citrix. Para diagnosticar falhas de inicialização de sessão, use o Citrix Monitor (ou seja, o serviço Citrix Director) para restringir o componente exato e o estágio em que 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:**
>
> Esse recurso está disponível apenas para clientes da nuvem nas regiões dos EUA, APS e UE. Ele não está disponível nas regiões do Japão e Governo.

Pré-requisitos

Se você estiver usando o Citrix DaaS, a integração é automática. Os clientes de nuvem que usam o StoreFront local devem garantir que uma versão compatível do StoreFront seja integrada.

- Se você estiver usando o Citrix Analytics for Performance, consulte Fontes de dados para ver as etapas para integrar o StoreFront local.
- Se você não estiver usando o Citrix Analytics for Performance:
  1. Vá para `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
  2. Clique em **Connect to StoreFront deployment**, insira os detalhes e baixe o arquivo de configuração. Para obter mais informações, consulte Integrar sites locais usando o StoreFront.

  > **Nota:**
  >
  > Administradores com funções Cloud Administrator podem integrar implantações do Store-

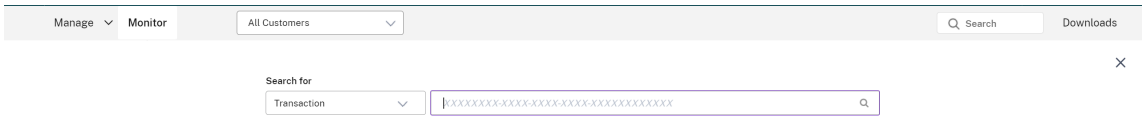
> Front, enquanto administradores com função Full Monitor Administrator só podem exibir as implantações do StoreFront.

As versões mínimas suportadas de outros componentes são as seguintes:

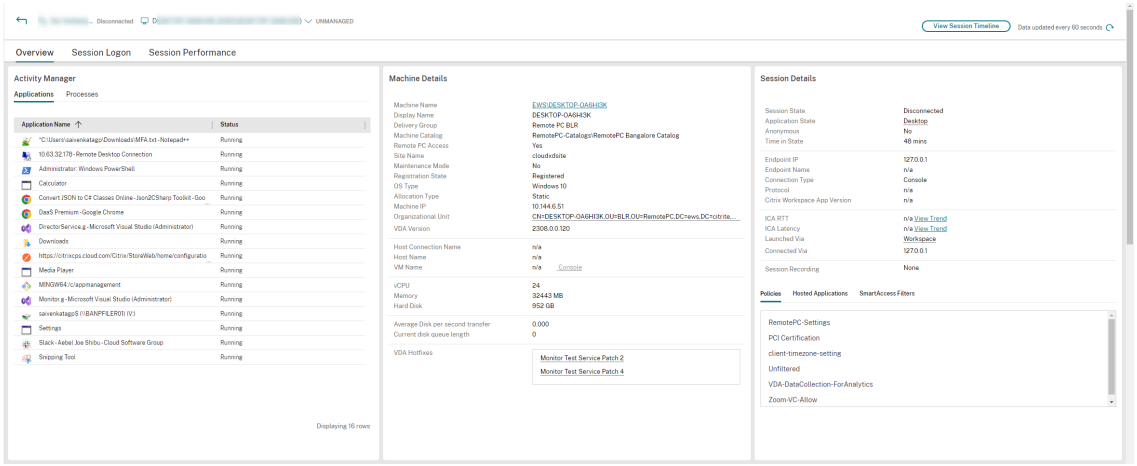
- Aplicativo Citrix Workspace para Windows 2109
- Aplicativo Citrix Workspace para Mac 2112
- Aplicativo Citrix Workspace para Linux 2112
- Aplicativo Citrix Workspace para HTML5 2110
- Aplicativo Citrix Workspace para Chrome 2110
- Aplicativo Citrix Workspace para Android 2110
- VDA versão Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

Etapas para diagnosticar a falha no início da sessão

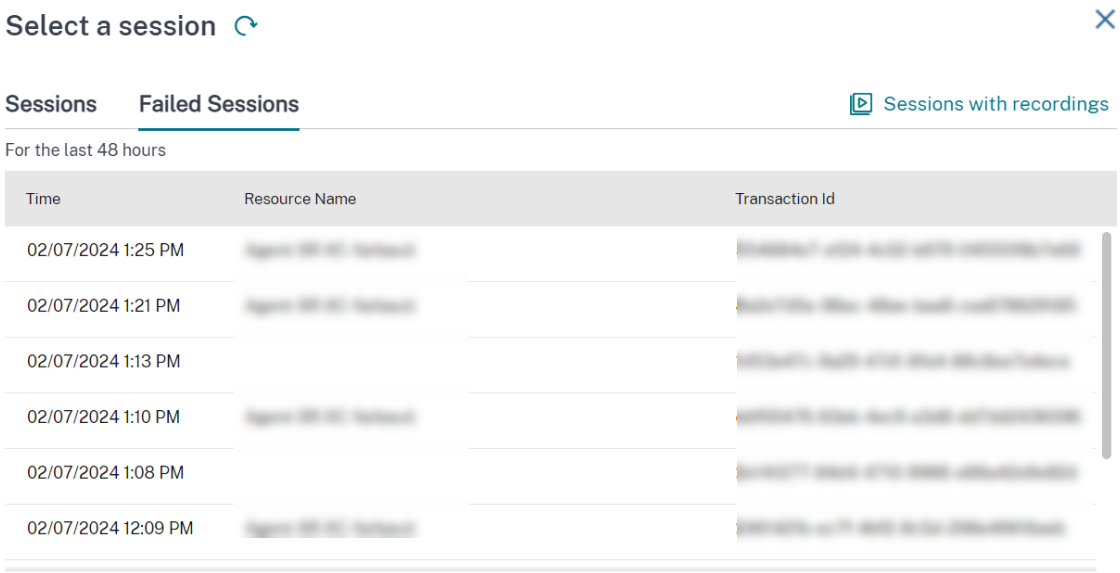
1. Copie o valor de Transaction ID do início da sessão com falha do aplicativo Citrix Workspace.
2. Na interface do usuário Monitor, procure o ID da transação de 32 dígitos e clique em **Details**.



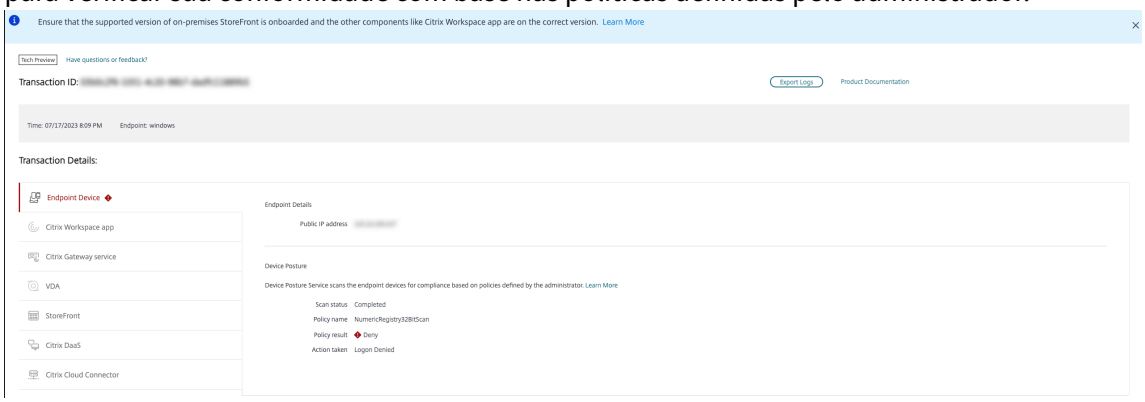
3. Se o ID da transação não estiver disponível, pesquise usando o nome do usuário. O Activity Manager do usuário é exibido.



4. Clique no seletor de sessão. Vá até a guia **Failed Sessions**. Uma lista das sessões que falharam nas últimas 48 horas é exibida. Clique na sessão selecionada.



5. O Citrix Monitor exibe informações importantes sobre a transação, como nome do usuário, carimbo de data/hora e o aplicativo ou área de trabalho em que a falha ocorreu.
6. O painel de detalhes da transação contém uma lista de componentes que indicam a ocorrência da falha.
7. Clique em **Endpoint Device** na lista de componentes para ver o status de varredura de postura do dispositivo. O serviço Device Posture faz a varredura do dispositivo do ponto de extremidade para verificar sua conformidade com base nas políticas definidas pelo administrador.



Os valores de Scan status, Policy name, Policy result e Action taken são exibidos. Certifique-se de que o serviço Device Posture esteja configurado com DaaS conforme descrito no artigo sobre a postura do dispositivo. Os erros registrados no log pelo Device Posture estão descritos em Device Posture Error Logs.

8. Clique nos outros nomes de componentes para verificar os detalhes em Component Details e Last known failure details.
9. O motivo da falha e o código de erro são exibidos. Clique no link **Learn more about the error** para ver o código de erro específico na seção Error codes que contém a descrição detalhada e

a ação recomendada.

10. Você pode exportar os logs para visualizá-los. O arquivo de log lista as etapas de inicialização da sessão em ordem cronológica e mostra o componente exato e o estágio em que a falha ocorreu.
11. Caso mais de uma falha tenha ocorrido nos componentes, somente os detalhes da última falha conhecida são exibidos na página Transaction. Os logs exportados contêm os detalhes de todas as falhas relacionadas à transação.

> **Nota:**
>
> Os códigos de erro e as informações de diagnóstico do lado do cliente estão disponíveis somente quando o Citrix StoreFront está integrado e enviando dados. Para obter mais informações sobre a integração do StoreFront, consulte Pré-requisitos.

Agente intermediário

bka.prepare.session.failure.validation

- Descrição: falha ao validar a solicitação de preparação da sessão.
- Ação recomendada: repita a ação. Se a falha se repetir, verifique se os conectores estão em um estado íntegro.

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: o HDX apresenta falha na preparação.
- Ação recomendada: reinicie o VDA.

bka.hdx.validate.failure.ticket_not_found

- Descrição: inicialização ou tíquete referenciado não está no cache de início.
- Ação recomendada: certifique-se de que o VDA pode se comunicar com o conector.

bka.ticketing.validate.failure.unlicensed

- Descrição: não é possível verificar a licença para inicialização.
- Ação recomendada: entre em contato com o suporte Citrix.

bka.ticketing.validate.failure.general

- Descrição: falha genérica durante a validação do tíquete.
- Ação recomendada: reúna logs do VDA e entre em contato com o suporte Citrix.

bka.set.configuration.failure.policy

- Descrição: ocorreu um erro durante a configuração de 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.

Agente

brk.validate.credentials.failure.invalid

- Descrição: falha ao validar credenciais devido a um problema. O motivo pode ser expandido no parâmetro da mensagem.
- Ação recomendada: repita a ação. Se a falha se repetir, verifique se os conectores estão em um estado íntegro.

brk.resolve.machine.failure.general

- Descrição: falha ao enumerar ou resolver o worker. O motivo pode ser expandido 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 tenham atingido sua capacidade.

brk.license.check.failure.constraints

- Descrição: as restrições de licenciamento falharam no início da sessão.
- Ação recomendada: verifique se há licenças disponíveis para esse tipo de aplicativo ou área de trabalho.

brk.resolve.machine.failure.timeout

- Descrição: o agente expirou ao durante o contato com o banco de dados.
- Ação recomendada: problemas de comunicação com o banco de dados do site. Entre em contato com o suporte Citrix.

brk.poweron.forlaunch.queued.failure.general

- Descrição: falha no enfileiramento da ação de energia.
- Ação recomendada: problemas de comunicação com o banco de dados do site. Entre em contato com o suporte 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 de comunicação 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 a sessão.
- Ação recomendada: verifique o status de integridade do site e assegure que todos os conectores e o Citrix DDC estejam operacionais.

brk.validate.ticket.failure.general

- Descrição: chamada de geração de tíquete inválida.
- Ação recomendada: entre em contato com o suporte Citrix.

brk.reverse.prepare.failure.general

- Descrição: falha genérica durante o início da sessão.
- Ação recomendada: verifique o status de integridade do site e assegure que todos os conectores e o Citrix DDC estejam operacionais.

brk.reverse.prepare.failure.lease_revoked

- Descrição: a concessão para a sessão foi revogada.
- Ação recomendada: repita a ação; se a falha se repetir, verifique se os conectores estão em um estado íntegro.

brk.reverse.prepare.failure.resource_unavailable

- Descrição: o recurso já está em uso ou está temporariamente indisponível.
- Ação recomendada: repita a ação; se a falha se repetir, verifique se os conectores estão em um estado íntegro.

brk.reverse.prepare.failure.app_protection

- Descrição: a proteção de aplicativos está ausente e é necessária para esta sessão.
- Ação recomendada: verifique se a proteção de aplicativos está ativada no 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-se a uma sessão no estado pré-logoff.
- Ação recomendada: tente iniciar novamente mais tarde; isso dará tempo para o logoff da sessão.

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Descrição: reconectar-se a uma sessão não existente.
- Ação recomendada: tente iniciar novamente mais tarde. Se ainda assim falhar, entre em contato com o suporte Citrix.

VDA_LINUX_ERR_SAME_KEY

- Descrição: preparar-se para uma conexão, mas há uma sessão existente com a mesma chave de sessão.
- Ação recomendada: entre em contato com o suporte 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 ouvinte CGP em execução.
- Ação recomendada: verifique se a política de **conexões de confiabilidade da sessão** está ativada. Verifique se o ouvinte CGP está escutando na porta esperada no VDA (a porta padrão é 2598, pode ser alterada por meio da política de **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 pode ser acessado pelo 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 gerar novamente os certificados da autoridade de certificação. Verifique se o FQDN do serviço Gateway é confiado pelo VDA.

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Descrição: falha ao aceitar o handshake de EDT do cliente.
- Ação recomendada: entre em contato com o suporte 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 pode ser acessado pelo VDA.

VDA_LINUX_ERR_TLS_CONNECT

- Descrição: falha ao estabelecer um handshake de 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 gerar novamente os certificados da autoridade de certificação. Verifique se o FQDN do serviço Gateway é confiável.

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Descrição: falha ao estabelecer um handshake do Rendezvous com o serviço Gateway.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Descrição: falha ao aceitar uma conexão ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Descrição: não é permitido reconectar-se a uma sessão anônima.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Descrição: a conexão não é permitida.
- Ação recomendada: se o código resultante for 3, verifique se a licença não expirou; caso contrário, tente iniciar novamente mais tarde. Se você não conseguir resolver, entre em contato com o suporte Citrix.

VDA_LINUX_ERR_CONN_GENERAL

- Descrição: falha ao validar a conexão.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Descrição: o usuário final cancelou o logon.

- Ação recomendada: esse erro é esperado quando o SSO está desabilitado e o usuário final clica no botão “Cancel”na caixa de login; caso contrário, entre em contato com o suporte Citrix.

VDA_LINUX_ERR_GET_TARGET

- Descrição: falha ao obter a sessão de destino.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_START_LOGON_TIMERS

- Descrição: falha ao iniciar os timers de logon.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Descrição: falha ao enviar o comando para a sessão de destino.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Descrição: falha ao postar um evento de reconexão.
- Ação recomendada: entre em contato com o suporte Citrix.

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Descrição: tempo limite de reconexão à sessão do usuário expirou.
- Ação recomendada: entre em contato com o suporte Citrix.

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous por TCP falhou.
- Ação recomendada: falhas esporádicas podem ocorrer devido a más condições de rede. Isso é esperado. Verifique a configuração do VDA se isso ocorrer com frequência e entre em contato com o suporte Citrix.

RENDEZVOUS_CONNECT_FAILED_EDT

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous por TCP falhou.
- Ação recomendada: falhas esporádicas podem ocorrer devido a más condições de rede. Isso é esperado. Verifique a configuração do VDA se isso ocorrer com frequência e entre em contato com o suporte Citrix.

RENDEZVOUS_CONNECT_FAILED_PROXY

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous falhou devido a uma configuração de proxy inválida.
- Ação recomendada: verifique a configuração do proxy do Rendezvous, entre em contato com o suporte Citrix.

RENDEZVOUS_CONNECT_FAILED_DTLS

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous falhou devido à falha no handshake de transporte seguro.
- Ação recomendada: verifique a configuração do Rendezvous, verifique a configuração criptográfica. Entre em contato com o suporte Citrix.

RENDEZVOUS_CONNECT_FAILED_TLS

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous falhou devido a uma falha no handshake de transporte seguro.
- Ação recomendada: verifique a configuração do Rendezvous, verifique a configuração criptográfica e entre em contato com o suporte Citrix.

RENDEZVOUS_CONNECT_FAILED_CGP

- Descrição: uma tentativa de conexão de saída do transporte Rendezvous falhou devido a um problema de configuração do CGP.
- Ação recomendada: verifique se o CGP (confiabilidade da sessão) está ativado e as portas CGP estão sendo escutadas, entre em contato com o suporte Citrix.

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Descrição: a interrupção da rede não foi resolvida devido ao tempo limite ter expirado, a confiabilidade da sessão não conseguiu restabelecer a conexão.

- Ação recomendada: falhas esporádicas podem ocorrer devido a más condições de rede. Isso é esperado.

CGP_SR_SUSPEND_RESUME_FAILED

- Descrição: a interrupção da rede não foi resolvida devido a um erro inesperado, a confiabilidade da sessão não conseguiu restabelecer a conexão.
- Ação recomendada: falhas esporádicas podem ocorrer devido a más condições de rede. Isso é esperado.

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: verifique a configuração do VDA, entre em contato com o suporte Citrix.

Error: 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 Citrix.

PREPARE_LISTENING_FAILED

- Descrição: o VDA falhou ao iniciar os ouvintes para a conexão ICA de entrada.
- Ação recomendada: verifique a configuração da rede, verifique se as portas do ouvinte não estão sendo usadas por outros aplicativos, entre em contato com o suporte Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED

- Descrição: o VDA falhou ao notificar a pilha do ICA para iniciar a conexão de saída do Rendezvous.
- Ação recomendada: verifique a configuração do Rendezvous, verifique a configuração do proxy do Rendezvous, verifique a configuração do CGP (confiabilidade da sessão), entre em contato com o suporte Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Descrição: o VDA falhou ao solicitar a pilha do ICA para iniciar uma conexão do Rendezvous de saída devido a um erro de configuração de proxy.
- Ação recomendada: verifique a configuração do proxy do Rendezvous, entre em contato com o suporte 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: entre em contato com o suporte Citrix.

ICA_ESTABLISH_FAILED

- Descrição: conexões ICA com falha de handshake ou aceitação.
- Ação recomendada: entre em contato com o suporte Citrix.

VALIDATE_FAILED

- Descrição: o agente falhou ao validar uma solicitação de conexão ICA recebida do VDA.
- Ação recomendada: entre em contato com o suporte Citrix.

VALIDATE_TICKETING_FAILED

- Descrição: o agente falhou ao validar uma solicitação de conexão ICA recebida do VDA devido a um problema de geração de tíquetes.
- Ação recomendada: entre em contato com o suporte Citrix.

MCS

brk.poweron.forlaunch.execution.generalfailure

- Descrição: erros gerais.
- Ação recomendada: entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.insufficientresourcefailure

- Descrição: uma operação do hipervisor não pode ser concluída devido a recursos insuficientes no hipervisor.
- Ação recomendada: verifique a cota de recursos no hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Descrição: o ID da máquina não existe.
- Ação recomendada: verifique o ID da máquina no hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Descrição: não é 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 você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- Descrição: credenciais inválidas.
- Ação recomendada: verifique as credenciais da conexão do hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.authorizationfailure

- Descrição: privilégios ou credenciais insuficientes.
- Ação recomendada: verifique a permissão atribuída às credenciais para conexão do hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.sslcertauthfailure

- Descrição: uma conexão não pode ser estabelecida devido a um problema de autenticação SSL.
- Ação recomendada: verifique o certificado de conexão do hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.ratelimitedfailure

- Descrição: a conexão com a nuvem informa que é limitada por taxa.
- Ação recomendada: tente novamente a conexão mais tarde se a solicitação for bloqueada pela limitação de taxa do hipervisor. Se você não conseguir encontrar uma solução, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.connectorconnectionfailure

- Descrição: existem erros no conector da nuvem. Por exemplo, o tempo limite expira enquanto aguarda a conexão. Quando o tempo limite é atingido, o conector da nuvem é desconectado.
- Ação recomendada: reinicie o conector da nuvem. Se isso falhar, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- Descrição: não foram encontrados erros no plug-in de proxy remoto/HCL ou no ponto de extremidade ao configurar a conexão com o plug-in.
- Ação recomendada: reinicie o conector. Se isso falhar, entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- Descrição: foi fornecida uma credencial expirada.
- 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 Citrix.

brk.poweron.forlaunch.execution.detachdiskfailed

- Descrição: o disco de desanexação usado pela máquina virtual falhou.
- Ação recomendada: entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.createclonefailed

- Descrição: falha na criação do disco de clone no hipervisor.
- Ação recomendada: entre em contato com o suporte 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 Citrix.

brk.poweron.forlaunch.execution.invalidvmstate

- Descrição: a operação não pode continuar devido a um estado de VM inválido.
- Ação recomendada: reinicie a VM primeiro e repita a operação.

brk.poweron.forlaunch.execution.insufficientresources

- Descrição: recursos insuficientes durante a operação.
- Ação recomendada: verifique a cota de recursos usada pelo hipervisor.

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- Descrição: a operação não pode continuar porque o hipervisor está no modo de manutenção.
- Ação recomendada: verifique se o hipervisor está no 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 Citrix.

brk.poweron.forlaunch.execution.recreatevmfailed

- Descrição: a recriação da VM falhou.
- Ação recomendada: entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.unknownvirtualmachine

- Descrição: máquina virtual desconhecida.
- Ação recomendada: entre em contato com o suporte Citrix.

brk.poweron.forlaunch.execution.ratelimitexceed

- Descrição: a conexão com a nuvem é limitada por taxa.
- Ação recomendada: tente novamente a conexão mais tarde se a solicitação foi bloqueada pela limitação de taxa do hipervisor.

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Descrição: o disco virtual não é armazenado.
- Ação recomendada: tente novamente mais tarde. Se isso falhar, entre em contato com o suporte Citrix.

Profile Management

xendesktop.upm.userprofile.error.failure

- Descrição: o Citrix Profile Management falhou ao processar o perfil do usuário. Em vez disso, use um perfil temporário.
- Ação recomendada: este erro não causa falha de logon. O Citrix Profile Management usa um perfil temporário. 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 prazo especificado.
- Ação recomendada: este erro não causa 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 Workspace Environment Management (WEM) falhou ao processar 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 de serviço do agente do WEM.

wem.agent.userpolicy.error.timeout

- Descrição: o agente Workspace Environment Management (WEM) falhou ao processar políticas de grupo para o usuário dentro do prazo 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 de serviço do agente do WEM.

Android pós-inicialização

SessionManager.Launch.EngineLoadFailed

- Descrição: falha ao carregar ou inicializar o mecanismo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.Launch.ConnectionFailed

- Descrição: o mecanismo terminou antes de se conectar.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.Launch.LogonFailed

- Descrição: sessão desconectada sem concluir o login.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.LeaseResolution.Failed

- Descrição: não foi possível tentar o início da concessão.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.clxmtp.SoftDeny

- Descrição: falha na negociação CLXMTP do mecanismo (negação de software).
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.clxmtp.SoftDeny_Implicit

- Descrição: falha na conexão do CLXMTP do mecanismo (negação de software implícita).
- Ação recomendada: entre em contato com o suporte Citrix.

Transport.Connect.NoCGP_Fail

- Descrição: falha ao conectar (CGP desativado).
- Ação recomendada: entre em contato com o suporte Citrix.

Transport.Connect.FallbackFail

- Descrição: falha ao conectar. Tentativa pelo ICA fallback.
- Ação recomendada: entre em contato com o suporte Citrix.

Transport.Connect.Fail

- Descrição: a conexão não está disponível.
- Ação recomendada: entre em contato com o suporte Citrix.

Android pré-inicialização

CWA-ICADOWNLOAD_ERR_00001

- Descrição: o tipo de solicitação de envio ICA 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: a loja é nula para a solicitação ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: o URL da loja é nulo para a solicitação ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: o parâmetro do recurso é nulo para a solicitação ICA.
- Ação recomendada: entre em contato com o suporte 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 Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: o parâmetro de recurso fornecido para a solicitação ICA é nulo para o URL de inicialização ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: a solicitação ICA é nula com os parâmetros do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Descrição: o corpo da solicitação ICA é nulo.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000010

- Descrição: falha ao criar uma entidade HTTP a partir do corpo da solicitação ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000011

- Descrição: falha ao baixar o arquivo ICA devido a uma exceção na criação da solicitação do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000012

- Descrição: falha ao baixar o arquivo ICA devido a uma exceção na execução da solicitação do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000013

- Descrição: falha ao baixar o arquivo ICA devido a uma resposta inesperada da solicitação do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000014

- Descrição: falha ao baixar o arquivo ICA quando você copia o inputStream da resposta do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000015

- Descrição: falha ao analisar o documento ICA usando o inputStream da resposta do Authentication Manager.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000016

- Descrição: o documento ICA baixado é nulo sem nenhuma exceção.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000017

- Descrição: falha ao baixar o arquivo ICA devido a uma resposta malsucedida.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000018

- Descrição: o recurso não está disponível.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000019

- Descrição: o recurso a ser iniciado não existe, não está ativado ou não está visível para o usuário.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000020

- Descrição: não há mais sessões ativas.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000021

- Descrição: o servidor não tem a licença necessária para realizar a atividade solicitada.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000022

- Descrição: não há estações de trabalho disponíveis.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000023

- Descrição: não é possível conectar-se à estação de trabalho. O servidor recusou a conexão.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000024

- Descrição: a estação de trabalho está em manutenção e não está disponível para uso.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000025

- Descrição: não é possível iniciar o recurso devido a um erro `resourceerror` no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000026

- Descrição: não é possível iniciar o recurso devido a um erro `generalapplauncherror` no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000027

- Descrição: não é possível iniciar o recurso devido a um erro desconhecido no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000028

- Descrição: não é possível iniciar o recurso devido a um erro de reinicialização no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000029

- Descrição: não é possível iniciar o recurso devido a um erro de retomada no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000030

- Descrição: não é possível iniciar o recurso devido a um erro indefinido no arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_000031

- Descrição: não é possível baixar o arquivo ICA. No entanto, o código de erro não é encontrado no mapa definido.
- Ação recomendada: entre em contato com o suporte Citrix.

Linux pós-inicialização

SessionManager.Launch.EngineLoadFailed

- Descrição: falha ao carregar o mecanismo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.Launch.Failed

- Descrição: falha ao iniciar a sessão.
- Ação recomendada: entre em contato com o suporte Citrix.

SessionManager.Launch.ConnectionFailed

- Descrição: o mecanismo terminou antes de se conectar.
- Ação recomendada: procure outros erros associados à tentativa de inicialização.

SessionManager.Launch.LogonFailed

- Descrição: sessão desconectada sem concluir o login.
- Ação recomendada: esse erro indica falha de login, possivelmente incluindo uma falha do usuário ao inserir manualmente as credenciais. Investigue como o usuário tentou entrar no VDA remoto.

SessionManager.LeaseResolution.Failed

- Descrição: não foi possível tentar o início da concessão.
- Ação recomendada: verifique se as concessões foram sincronizadas com a máquina cliente e se ainda são válidas. O usuário pode entrar no Citrix Workspace no modo online para disparar a (res)sincronização de concessões. Procure erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar os motivos da falha.

Transport.Connect.NoCGP_Fail

- Descrição: falha ao conectar (CGP desativado).
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com um VDA via TCP ou EDT.

Transport.Connect.FallbackFail

- Descrição: falha ao conectar. Tentativa pelo ICA fallback.
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com um Gateway, Connector ou VDA via TCP ou EDT.

Transport.Connect.Fail

- Descrição: o aplicativo Citrix Workspace falhou ao se conectar ao Gateway, Connector ou VDA por meio de TCP, EDT ou UDP.
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com o Gateway, Connector ou VDA por meio de TCP, EDT ou UDP. O firewall entre o cliente e o host talvez não permita os protocolos (UDP/TCP) ou as portas necessárias.

SessionManager.clxmtp.SoftDeny

- Descrição: falha na negociação CLXMTP do mecanismo (negação de software).
- Ação recomendada: esse erro não indica que a inicialização deve falhar. Ele indica que o mecanismo não será bem-sucedido por meio de um caminho de rede específico. Procure erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar os motivos da falha.

SessionManager.clxmtp.SoftDeny_Implicit

- Descrição: falha na conexão do CLXMTP do mecanismo (negação de software implícita).
- Ação recomendada: esse erro não indica que a inicialização deve falhar. Ele indica que o mecanismo não será bem-sucedido por meio de um caminho de rede específico. Investigue por que o cliente não consegue entrar em contato com um Connector ou Gateway. Pode-se esperar que o host fique inacessível devido à topologia de rede ou às restrições de firewall.

Linux pré-inicialização

CWA-ICADOWNLOAD_ERR_00001

- Descrição: não é possível conectar-se à loja devido à ausência de resposta do aplicativo Citrix Workspace.
- Ação recomendada: verifique se o Citrix Workspace ou o StoreFront estão inativos. Além disso, verifique a conectividade com a Internet.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: o usuário cancelou o início da sessão.
- Ação recomendada: reinicie a sessão depois de algum tempo.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: não foi possível conectar-se 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 ativado ou não está visível para o usuário.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: as estações de trabalho não estão disponíveis para essa solicitação.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: o servidor não tem a licença necessária para realizar a atividade solicitada.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: o servidor recusou a conexão com a estação de trabalho.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: a estação de trabalho solicitada está em manutenção e não está disponível para uso.
- Ação recomendada: entre em contato com o suporte 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 em detalhes.
- Ação recomendada: entre em contato com o suporte Citrix.

Mac pós-inicialização

Falha ao iniciar a área de trabalho

- Descrição: a área de trabalho “Nome da área de trabalho”falhou ao iniciar. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar o visualizador

- Descrição: o visualizador falhou ao iniciar. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar a área de trabalho

- 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 o administrador com os detalhes do erro.

Falha ao iniciar o aplicativo

- Descrição: “Nome do aplicativo”falhou ao iniciar.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar o aplicativo

- Descrição: “Nome do aplicativo”falhou ao iniciar. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar a área de trabalho

- Descrição: a área de trabalho “Nome da área de trabalho”falhou ao iniciar.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar a área de trabalho

- Descrição: a área de trabalho “Nome da área de trabalho”falhou ao iniciar. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar o visualizador

- Descrição: o visualizador falhou ao abrir o “Nome do aplicativo”. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar o visualizador

- Descrição: o visualizador falhou ao abrir a área de trabalho “Nome da área de trabalho”. ID da transação - “ID da transação”.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar a área de trabalho

- Descrição: a área de trabalho “Nome da área de trabalho”está em manutenção planejada.
- Ação recomendada: entre em contato com o administrador com os detalhes do erro.

Falha ao iniciar a área de trabalho

- 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 o administrador com os detalhes do erro.

Não é possível conectar-se à área de trabalho

- Descrição: não foi possível acessar a área de trabalho “nome da área de trabalho”ID da transação - “ID da transação”. Tente mais tarde.
- Ação recomendada: se o problema persistir, entre em contato com o administrador com os detalhes do erro.

Mac pré-inicialização

CWA-ICADOWNLOAD_ERR_00001

- Descrição: o arquivo ICA é inválido.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: a solicitação de inicialização atingiu o tempo limite.
- Ação recomendada: verifique a conexão com a Internet ou entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: o servidor não respondeu.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: o recurso a ser iniciado não existe, não está ativado ou não está visível para o usuário.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: o servidor não está acessível.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: erro ao iniciar o visualizador.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: falha ao iniciar um evento de abertura da Apple.
- Ação recomendada: entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: o caminho do visualizador não está acessível.
- Ação recomendada: entre em contato com o suporte 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 não está disponível para uso.
- Ação recomendada: peça ao usuário para tentar 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 mais assistência.

CWA-ICADOWNLOAD_ERR_000014

- Descrição: falha ao baixar o arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

Windows pós-inicialização

SessionManager.Launch.EngineLoadFailed

- Descrição: os componentes principais para estabelecer uma conexão a uma área de trabalho ou aplicativo remoto não foram carregados ou inicializados corretamente. Detalhes extras podem ser fornecidos na mensagem de erro.
- Ação recomendada: o aplicativo Citrix Workspace não está funcionando conforme o 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: esse erro é uma falha genérica que indica que uma tentativa de inicialização falhou. Outros erros enviados podem indicar uma causa.
- Ação recomendada: procure outros erros associados à tentativa de inicialização.

SessionManager.Launch.LogonFailed

- Descrição: esse 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 outro sistema operacional).
- Ação recomendada: esse erro indica alguma falha de login, possivelmente incluindo uma falha do usuário ao inserir manualmente as credenciais. Investigue como o usuário tentou entrar no VDA remoto.

SessionManager.Launch.Cancelled

- Descrição: a tentativa de conexão do mecanismo Citrix foi cancelada, provavelmente por ação do usuário.
- Ação recomendada: esse erro indica por que uma conexão não foi estabelecida com êxito, mas provavelmente indica o comportamento correto.

SessionManager.LeaseResolution.Failed

- Descrição: indica que uma inicialização offline (também chamada de “baseada em concessão”) falhou. Essa falha ocorre porque uma concessão válida e necessária para o recurso não foi en-

contrada na máquina cliente. Além disso, o Gateway ou o Cloud Connector rejeitou a solicitação de inicialização, ou a solicitação de inicialização estava inválida por algum motivo.
- Ação recomendada: verifique se as concessões foram sincronizadas com a máquina cliente e se ainda são válidas. O usuário pode entrar no Citrix Workspace no modo online para disparar a (res)sincronização de concessões. Procure erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar os motivos da falha.

SessionManager.clxmtp.SoftDeny

- Descrição: tentativa de inicialização de concessão, e um Connector ou Gateway informou ao cliente que não é possível concluir a inicialização solicitada. No entanto, os outros Connectors ou Gateways podem ajudar na inicialização.
- Ação recomendada: esse erro não indica que a inicialização deve falhar. Ele indica que o mecanismo não será bem-sucedido por meio de um caminho de rede específico. Procure erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar os motivos da falha.

SessionManager.clxmtp.SoftDeny_Implicit

- Descrição: houve uma tentativa de inicialização de concessão, e o Connector ou Gateway estava inacessível. No entanto, os outros Connectors ou Gateways podem ajudar na inicialização.
- Ação recomendada: esse erro não indica que a inicialização deve falhar. Ele indica que o mecanismo não será bem-sucedido por meio de um caminho de rede específico. Investigue por que o cliente não consegue entrar em contato com um Connector ou Gateway. Pode-se esperar que o host fique inacessível devido à topologia de rede ou às restrições de firewall.

Transport.Connect.NoCGP_Fail

- Descrição: os componentes (mecanismo) principais do aplicativo Citrix Workspace falharam ao se conectar a um host VDA por meio do protocolo ICA (porta 1494). Tentativas de conexão com um gateway ou VDA por meio do protocolo CGP não foram realizadas se esse evento foi enviado.
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com um VDA por meio de TCP ou EDT.

Transport.Connect.FallbackFail

- Descrição: os componentes (mecanismo) principais do aplicativo Citrix Workspace falharam ao se conectar a um host VDA por meio do protocolo ICA (porta 1494). Após essa falha, o aplicativo

Citrix Workspace não consegue se conectar a um Gateway ou VDA por meio do protocolo CGP (porta 2598).
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com um Gateway, Connector ou VDA por meio de TCP ou EDT.

Transport.Connect.Fail

- Descrição: os componentes (mecanismo) principais do aplicativo Citrix Workspace falharam ao se conectar a um Gateway ou VDA por meio do protocolo CGP (porta 2598). Tentativas de conexão com um VDA por meio do protocolo ICA não foram realizadas se esse evento foi emitido.
- Ação recomendada: investigue por que o cliente não consegue entrar em contato com um Gateway, Connector ou VDA por meio de TCP ou EDT.

Windows pré-inicialização

CWA-ICADOWNLOAD_ERR_00001

- Descrição: não é possível conectar-se à loja devido à ausência de resposta do aplicativo Citrix Workspace.
- Ação recomendada: verifique se o Citrix Workspace ou o StoreFront estão inativos. Além disso, verifique a conectividade com a Internet.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: o usuário cancelou o início da sessão.
- Ação recomendada: reinicie a sessão depois de algum tempo.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: não foi possível conectar-se 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 ativado ou não está visível para o 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 essa solicitação.
- Ação recomendada: entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: o servidor não tem 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 não está disponível 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: 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 em detalhes.
- Ação recomendada: entre em contato com o administrador de TI com os detalhes do erro.

Workspace

StoreLaunchIcaEndpoint.LaunchFailed

- Descrição: ocorreu um erro durante a inicialização.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

StoreLaunchSessionEndpoint.BadRequest

- Descrição: os parâmetros da solicitação de inicialização estavam inválidos ou vazios.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreLaunchSessionEndpoint.FarmUnavailable

- Descrição: não havia farms disponíveis para a inicialização.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops.

StoreLaunchSessionEndpoint.Error

- Descrição: ocorreu um erro interno durante a inicialização.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreGetIcaFileEndpoint.BadRequest

- Descrição: não foi fornecido um tíquete de inicialização na solicitação.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- Descrição: o Workspace não conseguiu recuperar o arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreGetIcaFileEndpoint.Error

- Descrição: o Workspace não conseguiu recuperar o arquivo ICA.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- Descrição: ocorreu um problema de autenticação.
- Ação recomendada: tente reautenticar. Entre em contato com o suporte Citrix.

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- Descrição: ocorreu um erro interno ao iniciar o aplicativo.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- Descrição: a inicialização falhou porque o aplicativo não foi encontrado.
- Ação recomendada: verifique os logs do Citrix Virtual Apps and Desktops e a configuração do aplicativo.

WebProxyLaunchIcaEndpoint.DSAuthFailure

- Descrição: ocorreu um problema de autenticação.
- Ação recomendada: tente reautenticar. Entre em contato com o suporte Citrix.

WebProxyLaunchIcaEndpoint.LaunchFailed

- Descrição: ocorreu um erro interno ao iniciar o aplicativo.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxyLaunchIcaEndpoint.ResourceNotFound

- Descrição: a inicialização falhou porque o aplicativo não foi encontrado.
- Ação recomendada: verifique os 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 poderá ser encerrada.
- Ação recomendada: reinicie o aplicativo.

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- Descrição: ocorreu um problema de autenticação.
- Ação recomendada: tente reautenticar. Entre em contato com o suporte Citrix.

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- Descrição: o Workspace não conseguiu se reconectar à sessão HDX existente. Sua sessão poderá ser encerrada.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxySessionsLaunchIcaEndpoint.Error

- Descrição: ocorreu um erro interno ao se reconectar à sessão.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- Descrição: ocorreu um problema de autenticação.
- Ação recomendada: tente reautenticar. Entre em contato com o suporte Citrix.

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- Descrição: o Workspace não conseguiu se reconectar à sessão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

WebProxySessionsGetLaunchStatusEndpoint.Error

- Descrição: ocorreu um erro interno ao se reconectar à sessão.
- Ação recomendada: entre em contato com o suporte Citrix.

DetermineGateway.Error

- Descrição: o Workspace não conseguiu determinar a qual gateway se conectar.
- Ação recomendada: verifique a configuração do seu Gateway. Entre em contato com o suporte Citrix.

ConnectionRoutingProviderLaunch.Error

- Descrição: o Workspace não conseguiu determinar a qual gateway se conectar.
- Ação recomendada: verifique a configuração do seu Gateway. Entre em contato com o suporte 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 Citrix.

BrokerGetAddressCall.LeasingError

- Descrição: o Workspace recebeu um erro do agente do Citrix Virtual Apps and Desktops.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

BrokerGetAddressCall.ServiceConnectionError

- Descrição: o Workspace não conseguiu entrar em contato com nenhum agente 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 Citrix.

BrokerGetAddressCall.BrokerError

- Descrição: o Workspace recebeu um erro de um agente do Citrix Virtual Apps and Desktops.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte 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 Citrix.

BrokerGetAddressCall.Error

- Descrição: o Workspace não pode recuperar os detalhes do VDA do agente do Citrix Virtual Apps and Desktops.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

GetLaunchReference.NoAccessToken

- Descrição: o Workspace não consegue se conectar com êxito ao VDA.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

GetLaunchReference.BrokerError

- Descrição: o Workspace não consegue se conectar com êxito ao VDA.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

GetLaunchReference.Error

- Descrição: o Workspace não consegue se conectar com êxito ao VDA.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

GenerateIcaFile.InvalidIcaSetting

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

StoreIcaFileAndGetTicket.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetFasVdaLogonTicket.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GenerateSTATicket.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetVdaAddress.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetTicket.NoAccessToken

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetTicket.BrokerError

- Descrição: o agente do Citrix Virtual Apps and Desktops não conseguiu iniciar a sessão HDX.
- Ação recomendada: verifique o ID na mensagem de erro e verifique seus logs do Citrix Virtual Apps and Desktops.

GetTicket.ServiceConnectionError

- Descrição: o Workspace não pode contatar um agente do Citrix Virtual Apps and Desktops.
- Ação recomendada: entre em contato com o suporte Citrix.

GetTicket.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetNetscalerConfigurationByCustomer.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

DiscoverMPSServerCapabilities.Error

- Descrição: ocorreu um problema ao fazer uma solicitação ao agente do Citrix Virtual Apps and Desktops.
- Ação recomendada: verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte Citrix.

GetResourceLocationNetScalerConfig.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetCustomerResourceLocations.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetResourceLocationFromResourceProvider.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetNetScalerGatewayInfo.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetCustomerEntitlements.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetResourceLocationForServerFeed.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

GetResourceInformation.Error

- Descrição: ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: entre em contato com o suporte Citrix.

Citrix Gateway como Serviço

CGS-ICASN_ERR_00001

- Descrição: falha na inicialização do aplicativo devido ao erro de análise da solicitação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS-ICASN_ERR_00002

- Descrição: falha ao validar o tíquete de autenticação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS-ICASN_ERR_00003

- Descrição: falha ao validar o tíquete de autenticação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS-ICASN_ERR_00004

- Descrição: falha ao validar o tíquete de autenticação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS-ICASN_ERR_00005

- Descrição: falha ao estabelecer conexão com o Connector.
- Ação recomendada: verifique a integridade do conector. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00006

- Descrição: a solicitação de conexão com o Connector atingiu o tempo limite.
- Ação recomendada: verifique a integridade do conector. Verifique se alguma configuração de proxy bloqueia o tráfego entre Connector/VDA e NGS. Verifique a conectividade entre o VDA e o Connector. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00007

- Descrição: o aplicativo Citrix Workspace fechou a conexão.
- Ação recomendada: verifique se a conectividade de rede do lado do cliente está estável. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00008

- Descrição: o backend fechou a conexão.
- Ação recomendada: verifique a integridade do conector. Verifique a estabilidade da rede do Connector/VDA à rede pública (NGS). Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00009

- Descrição: falha no estabelecimento da conexão entre VDA e NGS (Rendezvous).
- Ação recomendada: verifique a integridade do conector. O VDA deve ser capaz de acessar o Serviço NGS. Verifique a conectividade entre o VDA e o Connector. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00010

- Descrição: fallback de EDT para TCP. Verifique o pré-requisito para EDT.
- Ação recomendada: o Rendezvous deve estar ativado e o VDA deve ser capaz de acessar o serviço NGS por UDP. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00011

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00012

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00013

- Descrição: falha na validação do GCT.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00014

- Descrição: falha na validação do GCT.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00015

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00016

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00017

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00018

- Descrição: falha ao validar o tíquete de autenticação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00019

- Descrição: falha ao validar o tíquete de autenticação.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00020

- Descrição: erro no licenciamento interno do CGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00021

- Descrição: fallback do Rendezvous v2 devido ao sinalizador de recurso desativado.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00022

- Descrição: falha no serviço interno do NGS.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00023

- Descrição: tempo limite na troca CLXMTP.
- Ação recomendada: verifique se os conectores estão íntegros e acessíveis para o serviço NGS. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00024

- Descrição: falha na validação do CLXMTP VSR.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00025

- Descrição: falha na validação do CLXMTP VSR.
- Ação recomendada: entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00026

- Descrição: o Connector não está disponível no CLXMTP.
- Ação recomendada: verifique se o conector está em um estado íntegro para a localização do recurso. Se o problema persistir, entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00027

- Descrição: o redirecionamento de CLXMTP para o Connector falhou após o máximo de tentativas.
- Ação recomendada: verifique se o conector está em um estado íntegro para a localização do recurso. Verifique se o serviço `Citrix ClxMtp Service` está sendo executado em todos os conectores. Entre em contato com o suporte Citrix.

CGS_ICASN_ERR_00028

- Descrição: falha de comunicação com o Controller.
- Ação recomendada: entre em contato com o suporte Citrix.

Success: CGS_ICASN_SUCCESS_00001

- Descrição: solicitação de inicialização de sessão recebida.
- Ação recomendada: não aplicável

Success: CGS_ICASN_SUCCESS_00002

- Descrição: solicitação de inicialização de sessão concluída.
- Ação recomendada: não aplicável

Proxy XAXD

XDPXY_INF_00001

- Descrição: o agente 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 agente.
- Ação recomendada: não aplicável

XDPXY_ERR_00001

- Descrição: falha de comunicação 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00002

- Descrição: o XaxdProxy atingiu o tempo limite aguardando 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00003

- Descrição: encontrada uma exceção ou falha do 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_INF_00003

- Descrição: a solicitação de validação para uma conexão de entrada ICA ou RDP é chamada pela pilha.
- Ação recomendada: não aplicável

XDPXY_INF_00004

- Descrição: a validação da conexão de entrada ICA ou RDP está estabelecida.
- Ação recomendada: não aplicável

XDPXY_ERR_00001

- Descrição: falha de comunicação 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00002

- Descrição: o XaxdProxy atingiu o tempo limite aguardando uma resposta do 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00003

- Descrição: encontrada uma exceção 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_INF_00005

- Descrição: a solicitação de tráfego de sessão HDX direto para o VDA foi feita.
- Ação recomendada: não aplicável

XDPXY_INF_00006

- Descrição: o VDA estabelece a 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 à rede pública.
  - Se você tiver um proxy da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00006

- Descrição: a solicitação XML tem um formato inválido.
- Ação recomendada: entre em contato com o suporte Citrix.

XDPXY_ERR_00007

- Descrição: a solicitação XML tem cabeçalhos e/ou formato de credencial inválidos.
- Ação recomendada: faça logout e login novamente e tente a ação de novo. Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_INF_00011

- Descrição: a inicialização da continuidade do serviço é solicitada pelo usuário via WSA.
- Ação recomendada: não aplicável

XDPXY_INF_00012

- Descrição: a inicialização da continuidade do serviço é solicitada 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 da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00008

- Descrição: a inicialização da continuidade do serviço falhou porque o XaxdProxy atingiu o tempo limite aguardando uma resposta.
- Ação recomendada: verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Se você tiver um proxy da Web entre o Connector e o Broker, verifique se ele está configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte Citrix.

XDPXY_ERR_00009

- Descrição: a inicialização da continuidade do serviço falhou devido ao bloqueio e/ou revogação da concessão.
- 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 Citrix.

Citrix DaaS para Citrix Service Providers

August 18, 2022

Este artigo descreve como o **Citrix Service Provider (CSP)** pode configurar o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) para clientes locatários no Citrix Cloud. Para obter uma visão geral dos recursos disponíveis para os parceiros Citrix, consulte Citrix Cloud para parceiros.

Requisitos

- Ser um parceiro Citrix Service Provider.
- Ter uma conta do Citrix Cloud.
- Ter uma assinatura do Citrix DaaS.

Limitações e problemas conhecidos

Limitações

- As alterações no nome do locatário levam até 24 horas para serem aplicadas em todas as interfaces.
- Ao criar um locatário, o endereço de e-mail deve ser exclusivo.
- A filtragem em **Manage > Full Configuration** por escopo (semelhante a Monitor) não está disponível. Para ver os recursos anexados a um escopo, selecione **Administrators** no painel esquerdo. Na guia **Scopes**, selecione o escopo e, em seguida, selecione **Edit Scope** no painel Action.

Problemas conhecidos

- Depois que os escopos são atribuídos a um recurso, você não pode usar o console de gerenciamento para removê-los ou cancelar a atribuição. Essas tarefas são suportadas somente por meio do PowerShell.
- **Manage > Full Configuration** não impõe escopos. Você é responsável por selecionar o escopo apropriado ao criar catálogos de máquinas, grupos de entrega e grupos de aplicativos.
- Quando mais de 15 escopos são criados (criados automaticamente e personalizados), as informações de acesso personalizadas do Citrix Cloud de um administrador (**Identity and Access Management > Administrators**) não são exibidas corretamente. Solução alternativa: limite os escopos a 15 ou menos.

Adicionar um cliente

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.

2. Em Customer Dashboard, selecione **Invite or Add**. Forneça as informações solicitadas.
3. Se o cliente não tiver uma conta do Citrix Cloud, adicione o cliente para criar uma conta de cliente. Ao adicionar o cliente, você também é adicionado automaticamente como administrador com acesso completo à conta do cliente.
4. Se o cliente tiver uma conta do Citrix Cloud:

   a) Um URL do Citrix Cloud é exibido, que você copia e envia para o cliente. Para obter detalhes sobre esse processo, consulte Convidar um cliente para se conectar.
   b) O cliente deve adicioná-lo como administrador com acesso completo à conta. Consulte Adicionar administradores a uma conta do Citrix Cloud.

Você pode adicionar mais administradores posteriormente e controlar quais clientes eles podem ver nos consoles **Manage** e **Monitor**.

Adicionar o Citrix DaaS a um cliente

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.
2. No Customer Dashboard, no menu de reticências do cliente, selecione **Add Service**.
3. Em **Select a service to add**, selecione **Virtual Apps and Desktops**.
4. Selecione **Continue**.

Depois de concluir esse 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 fica visível na exibição **Manage > Full Configuration**. Esse escopo é exclusivo para esse cliente. Você pode renomear o escopo, mas não pode excluí-lo.

Use esse 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, além de dois outros clientes. Para obter detalhes, consulte Controlar o acesso do administrador aos clientes.

Configurar um local de recurso

Um local de recurso contém as máquinas que fornecem aplicativos e áreas de trabalho para seus clientes e componentes de infraestrutura, como Citrix Cloud Connectors. Para obter detalhes, consulte Conectar-se ao Citrix Cloud.

Configurar catálogos e grupos para entregar aplicativos e áreas de trabalho

Um catálogo é um grupo de máquinas virtuais idênticas. Quando você cria 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. The delivery group specifies which users can use those machines, plus the applications or desktops available to those users. Para obter detalhes, consulte Criar grupos de entrega.

Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos que são 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.

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 o escopo A e B. O escopo do grupo de aplicativos pode ser A ou B, ou A e B.

Domínios federados

Os domínios federados permitem que os usuários do cliente usem credenciais de um domínio anexado ao seu local do recurso para entrar no espaço de trabalho. Isso permite que você forneça espaços de trabalho dedicados aos seus clientes que os usuários do cliente podem acessar usando um URL de espaço de trabalho personalizado (por exemplo, customer.cloud.com), enquanto o local do recurso ainda está na sua conta do Citrix Cloud. Você pode fornecer espaços de trabalho dedicados juntamente com o espaço de trabalho compartilhado que os clientes podem acessar usando o URL do espaço de trabalho do CSP (por exemplo, csppartner.cloud.com).

Para permitir que os clientes acessem seus espaços de trabalho dedicados, você os adiciona aos domínios apropriados que você gerencia. Depois de configurar o espaço de trabalho usando Workspace Configuration, os usuários dos clientes podem entrar no espaço de trabalho e acessar os aplicativos e áreas de trabalho que você disponibilizou.

Adicionar um cliente a um domínio

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.

2. No Customer Dashboard, selecione **Identity and Access Management** no menu superior esquerdo.
3. Na guia **Domains**, selecione **Manage Federated Domain** no menu de reticências do domínio.
4. No cartão **Manage Federated Domain**, na coluna **Available customers**, selecione um cliente que você deseja adicionar ao domínio. Selecione o sinal de mais ao lado do nome do cliente. O cliente selecionado agora aparece na coluna **Federated customers**. Repita para adicionar outros clientes. Quando terminar, selecione **Apply**.

Remover um cliente de um domínio

Quando você remove um cliente de um domínio que você gerencia, os usuários do cliente não podem mais acessar seus espaços de trabalho usando as credenciais do seu domínio.

1. No menu Citrix Cloud, selecione **Identity and Access Management** e depois **Domains**.
2. Localize o domínio que você deseja gerenciar e selecione o botão de reticências. Selecione **Manage Federated Domain**.
3. Na lista de clientes federados, localize ou pesquise os clientes que você deseja remover e selecione o botão X. Selecione **Remove all** para remover do domínio todos os clientes na lista. Os clientes selecionados são movidos para a lista de clientes disponíveis.
4. Selecione **Apply**.
5. Revise os clientes que você selecionou e selecione **Remove Customers**.

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 mais tarde.

Para saber mais sobre como restringir o acesso usando funções e escopos no Citrix DaaS, consulte Administração delegada.

Adicionar um administrador com acesso restrito

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.
2. No Customer Dashboard, selecione **Identity and Access Management** no menu superior esquerdo.
3. Na guia **Administrators**, selecione **Add Administrators From** e depois selecione **Citrix Identity**.

4. Digite o endereço de e-mail da pessoa que você está adicionando como administrador e selecione **Invite**.
5. Configure as permissões de acesso apropriadas para o administrador. A Citrix recomenda selecionar **Custom access**, 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 **Custom access**, selecione um ou mais pares de função e escopo para o Citrix DaaS, conforme necessário. Certifique-se de habilitar apenas as entradas que contenham o escopo exclusivo que foi criado para o cliente.
7. Quando terminar de selecionar pares de função e escopo, selecione **Send Invite**.

Quando o administrador aceita o convite, ele tem o acesso que você atribuiu.

Editar permissões de administração delegadas para administradores

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.
2. No Customer Dashboard, selecione **Identity and Access Management** no menu superior esquerdo.
3. Na guia **Administrators**, selecione **Edit Access** no menu de reticências do administrador.
4. Selecione e limpe os pares de função e escopo para o Citrix DaaS, conforme necessário. Certifique-se de habilitar apenas as entradas que contenham o escopo exclusivo que foi criado para o cliente.
5. Selecione **Save**.

Exibir administradores de clientes e suas funções e escopos atribuídos

1. Faça login no Citrix Cloud com suas credenciais do CSP. Selecione **Customers** no menu superior esquerdo.
2. No Customer Dashboard, selecione **My Services > DaaS** no menu superior esquerdo.
3. No Citrix DaaS, selecione **Manage > Full Configuration**.
4. Selecione **Administrators** no painel esquerdo.

As informações estão disponíveis em três guias:

- A guia **Administrators** lista os administradores que foram criados, além de suas funções e escopos.
- A guia **Roles** lista todas as funções. Para exibir detalhes da função, selecione a função no painel central. A parte inferior do painel lista os tipos de objetos e as permissões associadas para a função. Clique na guia **Administrators** no painel inferior para exibir uma lista de administradores que atualmente têm a função.

- A guia **Scopes** lista todos os escopos, incluindo os escopos gerados para clientes de parceiros Citrix.

Configurar espaços de trabalho

O cliente tem seu próprio espaço de trabalho com um URL `customer.cloud.com` exclusivo. Nesse espaço de trabalho os usuários do cliente acessam seus aplicativos e áreas de trabalho publicados.

O URL do espaço de trabalho é exibido em dois locais:

- No Customer Dashboard, selecione **Workspace Configuration** no menu no menu superior esquerdo.
- Na página **Welcome** do Citrix DaaS (a guia **Overview**), o URL do espaço de trabalho aparece na parte inferior da página.

Você pode alterar o acesso e a autenticação de um espaço de trabalho. Você também pode personalizar a aparência e as preferências do espaço de trabalho. Para obter detalhes, consulte os seguintes artigos:

- Configurar espaços de trabalho
- Espaços de trabalho seguros

Monitorar o serviço de um cliente

O painel **Monitor** em um ambiente CSP é essencialmente o mesmo que em um ambiente não CSP. Consulte Monitor para obter detalhes.

Por padrão, o painel **Monitor** exibe informações sobre todos os clientes. Para exibir informações sobre um cliente, use **Select Customer**.

Lembre-se de que a capacidade de ver as exibições de Monitor para um cliente é controlada pelo acesso configurado do administrador. O acesso deve incluir um par de função e escopo que inclua o escopo exclusivo do cliente.

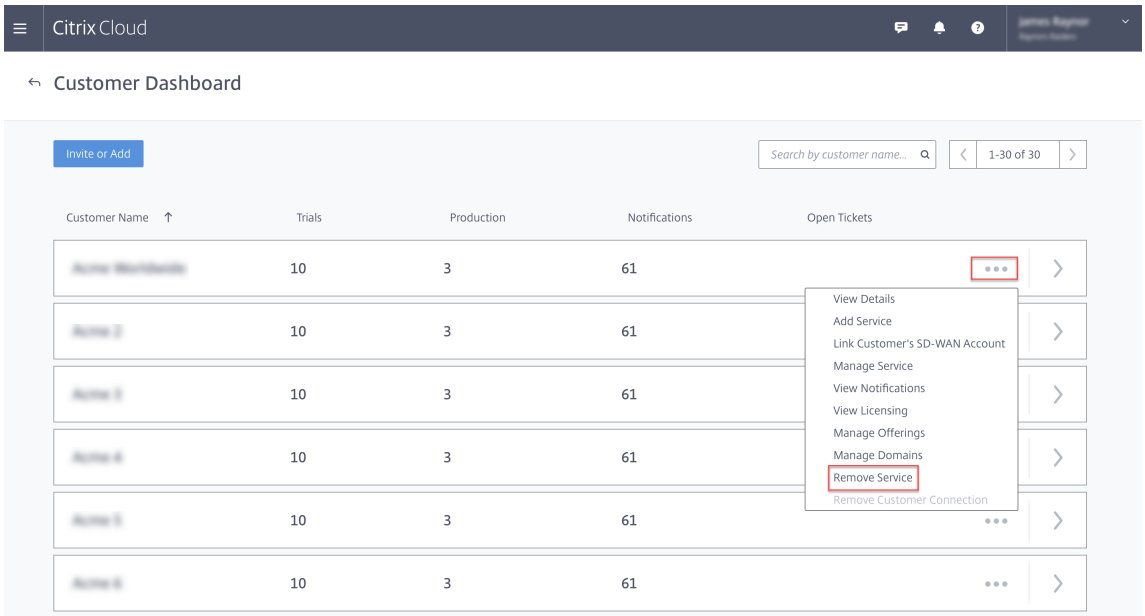
Se você usou funções internas para configurar o acesso, as funções internas controlam se o administrador pode ver as exibições **Manage** e **Monitor**. Se você selecionar apenas pares de função e escopo do cliente que não incluam a visibilidade da guia **Monitor**, o administrador não verá a guia **Monitor** de nenhum cliente selecionado. Por exemplo, se você conceder a um administrador somente acesso **Read Only Administrator,customerABC**, esse administrador não verá a guia **Monitor** do cliente ABC, porque os administradores somente leitura não podem acessar às exibições de Monitor.

Remover um serviço

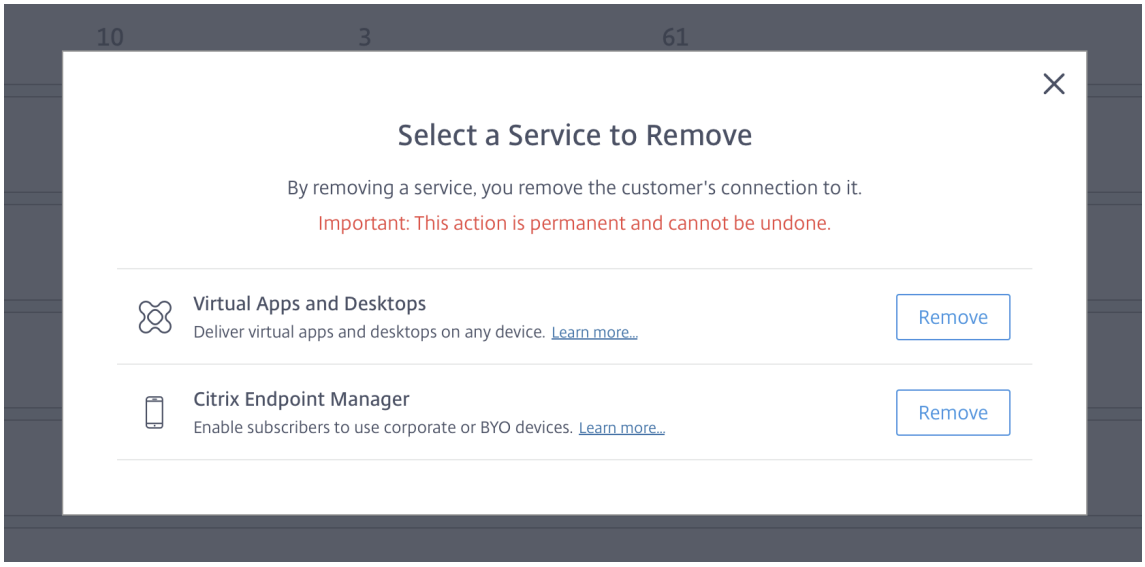
Pré-requisitos

- Certifique-se de que o escopo do seu cliente não esteja vinculado a nenhum objeto Citrix DaaS. Se estiverem vinculados, você não pode remover o serviço. Para desvincular escopos, vá para **Citrix Studio > Administrators > Scopes** e edite o escopo.
- Para conhecer o escopo do seu cliente e gerenciá-lo, consulte Criar e gerenciar escopo.

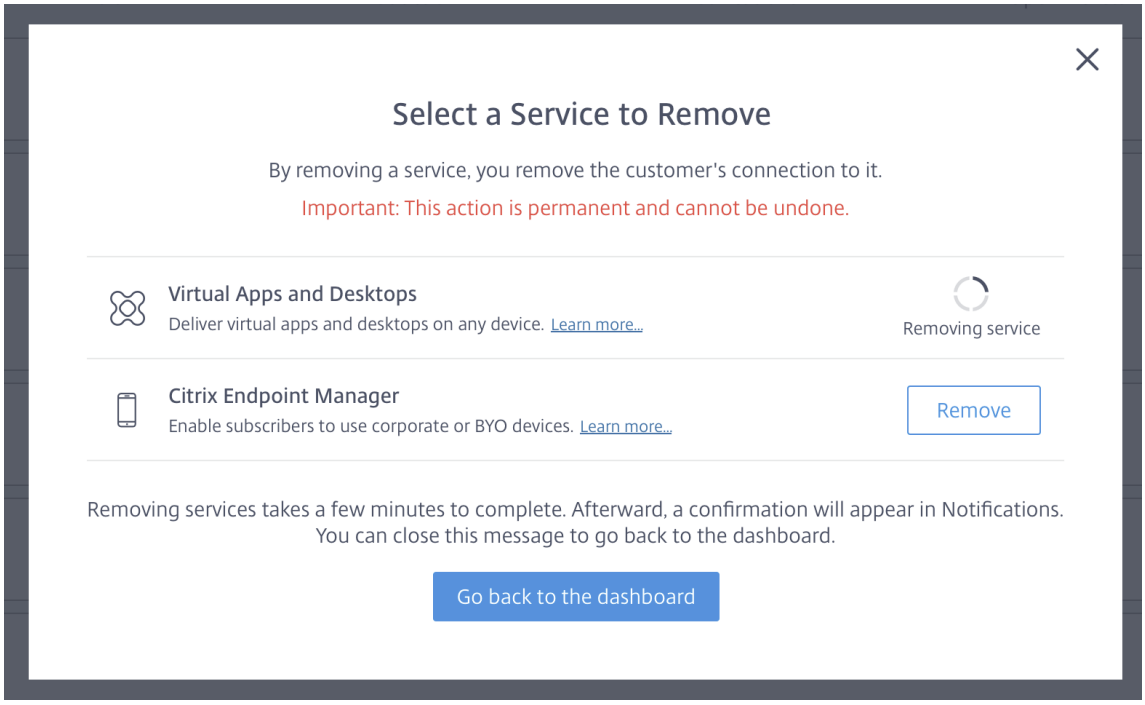
1. Faça login no Citrix Cloud com suas credenciais do Citrix Service Providers.
2. Em **Customer Dashboard**, clique no menu de **reticências** (…) do cliente de onde você deseja remover um serviço e selecione **Remove Service**.



A página **Service to Remove** é exibida.



3. Clique em **Remove** para remover o serviço.



Serviço Citrix Gateway

May 3, 2022

O Citrix Gateway fornece aos usuários acesso seguro aos aplicativos Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service).

O serviço Citrix Gateway permite acesso remoto e seguro 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 muda 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 da 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 o tráfego de rede de camada 4 de camada 7 (L4-L7) de forma inteligente para aplicativos da web. O dispositivo virtual Citrix ADC VPX pode ser hospedado em várias plataformas de virtualização e nuvem. Para obter detalhes, consulte Implantar uma instância Citrix ADC VPX.

SDKs e APIs

December 20, 2023

Citrix DaaS Remote PowerShell SDK

O SDK do PowerShell remoto automatiza tarefas complexas e repetitivas. Ele fornece o mecanismo para configurar e gerenciar o ambiente do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) sem usar as interfaces de usuário do **Manage**.

- Os detalhes do cmdlet são fornecidos no Citrix DaaS SDK.
- Os módulos suportados estão listados em Suporte e limitações. Essa seção também lista os cmdlets desabilitados neste SDK.
- O Remote PowerShell SDK está disponível para download no site da Citrix.

Este produto oferece suporte ao PowerShell versões 3 a 5.

Como esse SDK difere do SDK para implantações gerenciadas pelo cliente

Em uma implantação do Citrix Virtual Apps and Desktops instalada e gerenciada pelos administradores do cliente, esses administradores executam cmdlets e scripts em um site que contém VDAs e Delivery Controllers em uma estrutura de domínio comum. Por outro lado, o Citrix DaaS divide os VDAs e os Controllers em um local do recurso e o plano de controle, respectivamente. Essa divisão significa que o SDK do PowerShell do Citrix Virtual Apps and Desktops não funciona em um ambiente do Citrix DaaS. Ele não pode cruzar o limite seguro do local do recurso para o plano de controle.

A solução é o SDK do PowerShell remoto do Citrix DaaS. Ao executar no local do recurso, o SDK do 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 local do recurso seguro para controlar o limite do plano. Por padrão, `Get-XdAuthentication` solicita aos usuários as credenciais CAS e deve ser feito uma vez por sessão do PowerShell. Como alternativa, o usuário pode definir um perfil de autenticação usando um Secure Client 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 PowerShell SDK. Se esse cmdlet não for executado explicitamente, ele será chamado pelo primeiro cmdlet do PowerShell SDK.

Pré-requisitos

Para usar o Citrix DaaS Remote PowerShell SDK, acrescente as seguintes URLs à lista branca:

Comercial

- `https://accounts.cloud.com`
- `https://[service].citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

Japão

- `https://accounts.citrixcloud.jp`
- `https://[service].citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

Governo

- `https://accounts.cloud.us`
- `https://[service].citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

Instalar e usar o SDK do PowerShell remoto

Requisitos e considerações:

> **Nota:**
>
> Não instale o SDK do PowerShell remoto em uma máquina do Citrix Cloud Connector. Ele pode ser instalado em qualquer máquina ingressada no domínio no mesmo local de recursos.
>
> A Citrix não oferece suporte à execução dos cmdlets desse SDK no Cloud Connectors. A operação do SDK não envolve os Cloud Connectors.
>
> Se você também tiver uma implantação do Citrix Virtual Apps and Desktops (além da implantação do Citrix DaaS), não instale o SDK do PowerShell remoto em uma máquina do Delivery Controller local.

- Instale o **Microsoft Edge WebView2**.
- Assegure que o PowerShell 3.0, 4.0 ou 5.0 esteja disponível na máquina.
- O instalador do SDK baixa e instala o .NET Framework 4.8 se ele (ou uma versão mais recente com suporte) ainda não estiver instalado.
- Se a máquina já tiver o SDK do Citrix Virtual Apps and Desktops instalado, remova esse SDK (dos Programas e Recursos do Windows) antes de instalar o SDK do PowerShell remoto.
- Para um ambiente automatizado, use o parâmetro `-quiet` para instalar o SDK sem a interferência do usuário.

Para instalar o SDK do PowerShell remoto:

1. Na página de download, baixe o SDK do PowerShell remoto do Virtual Apps and Desktops.
2. Instale e execute o SDK.

Os logs de instalação são criados em `%TEMP%\CitrixLogs\CitrixPoshSdk`. Os registros podem ajudar a resolver problemas de instalação.

Execute o SDK em um computador ingressado no domínio nesse local do 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 SDK do PowerShell remoto, que solicita a mesma autenticação que `Get-XdAuthentication`. Se você estiver usando um proxy, deverá se autenticar no proxy para poder usar o cmdlet `Get-XdAuthentication`. Para obter mais informações, consulte Usar o SDK do PowerShell remoto 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 Secure Client 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, a partir do recurso do Windows de remoção ou alteração de programas, selecione **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Clique com o botão direito do mouse e selecione **Desinstalar**. Siga as instruções.

Usar o SDK do PowerShell remoto com um proxy Se você estiver usando um proxy, talvez não consiga usar o cmdlet `Get-xdAuthentication` porque o proxy bloqueia as solicitações HTTP feitas pelo cmdlet.

Há duas maneiras de se autenticar no proxy. Você pode usar o parâmetro `ProxyUseDefault` ou os parâmetros `ProxyUsername` e `ProxyPassword`:

- O parâmetro `ProxyUseDefault` habilita a autenticação no proxy usando as credenciais de proxy padrão. Por exemplo:

```
Get-XdAuthentication -ProxyUseDefault
<!--NeedCopy-->
```

- 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
<!--NeedCopy-->
```

Atividades de exemplo

As atividades comuns incluem a configuração de catálogos de máquinas, aplicativos e usuários. Um exemplo de script 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
```



```
14
15      #Add TSVDA Machine to Catalog
16
17      $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
            -CatalogUid $catalog.uid
18
19      #Create new desktops & applications delivery group
20
21      $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
           $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
           " -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23      #Create notepad application
24
25      New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
           Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27      #Assign users to desktops and applications
28
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
            $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
           IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
           DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
           DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
            $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

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 do Citrix Virtual Apps and Desktops PowerShell são suportados nesta versão:

- Agente
- Identidade do Active Directory (AD)
- Criação de máquina
- Configuração
- Log 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 PowerShell remoto deve ser executado em um computador no local do recurso.

Os cmdlets a seguir são desativados 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 servidores e pacotes App-V

O Citrix DaaS pode fornecer aplicativos contidos em pacotes App-V para os seus pontos de extremidade usando um dos seguintes métodos:

- Método de gerenciamento de administração simples (acessando pacotes de um compartilhamento de rede)
- Método de gerenciamento de administração dupla (acessando pacotes a partir de um servidor de gerenciamento Microsoft App-V)

O processo de registro de pacotes App-V e servidores de gerenciamento e publicação Microsoft App-V na biblioteca de aplicativos usando o Citrix DaaS difere ligeiramente do registro de pacotes usando

uma implantação local. No entanto, o processo de atribuir aplicativos a usuários e iniciá-los no ponto de extremidade de um usuário é idêntico.

O console de gerenciamento do Citrix DaaS no Citrix Cloud não pode exibir os arquivos em um local de recurso. Além disso, ele não pode detectar diretamente pacotes App-V ou servidores Microsoft App-V em sua infraestrutura. O módulo de descoberta fornece funções que detectam informações do pacote App-V na sua infraestrutura local e carrega as informações do pacote 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 detectar informações de pacotes a partir de um compartilhamento de rede ou de um servidor de gerenciamento Microsoft App-V. Você usa o módulo de descoberta em uma máquina no seu local do 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 em que os Citrix Cloud Connectors estão instalados e 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 a partir de compartilhamentos de rede (gerenciamento de administrador simples) e adicionar todos os pacotes App-V publicados a partir do servidor de gerenciamento Microsoft App-V (gerenciamento de administração dupla). Com o método de gerenciamento de administração dupla, você deve gerenciar os pacotes App-V adicionados da mesma forma que faz ao usar o método de gerenciamento de administração simples.

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 de sua escolha.

   > **Nota:**
   >
   > Esse arquivo também é fornecido no Citrix Virtual Apps and Desktops ISO 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. Navegue até 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 métodos a seguir.

   - 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 do cmdlet, digite `Get-Help Import-AppVPackageToCloud`.

   - Para adicionar pacotes App-V a partir de um servidor de gerenciamento Microsoft App-V, execute o cmdlet do PowerShell: `Import-AppVPackagesFromManagementServerToCloud`

     Por exemplo: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Para obter ajuda do cmdlet, digite `Get-Help Import-AppVPackagesFromManagementServe`

     Este comando importa todos os pacotes App-V publicados a partir do servidor de gerenciamento Microsoft App-V para o Citrix Cloud.

     Depois de adicionar os pacotes do App-V ao Citrix Cloud, você deve gerenciá-los da mesma forma que faz usando o método de gerenciamento de administração simples.

6. Faça login no Citrix Cloud. Selecione o cliente-alvo. Depois que o script for executado com êxito, os pacotes App-V serão adicionados à biblioteca de aplicativos no Citrix Cloud.

Funções do PowerShell de alto nível

O módulo contém as seguintes funções de alto nível que você pode chamar do seu próprio script do PowerShell:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Detecta e carrega para o Citrix DaaS todas as informações necessárias para publicar aplicativos a partir de um único pacote App-V.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Detecta os caminhos UNC dos pacotes publicados pelo servidor de gerenciamento e chama **Import-AppVPackageToCloud** para cada um deles.

  Os pacotes detectados dessa maneira são carregados para o Citrix DaaS usando o método de gerenciamento de administração simples. O Citrix DaaS não pode entregar pacotes usando o método de gerenciamento de administração dupla.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Detecta os servidores de gerenciamento e publicação Microsoft App-V e importa o conteúdo para a biblioteca de aplicativos. Esse cmdlet importa todos os pacotes gerenciados usando o servidor de gerenciamento Microsoft App-V e informações relacionadas. Os servidores podem ser adicionados e removidos por meio do PowerShell.

  Esse cmdlet adiciona pacotes App-V no modo de administração dupla. Somente os pacotes do App-V publicados no servidor de gerenciamento Microsoft App-V e que têm grupos do AD adicionados são importados. Se você fizer alterações no servidor de gerenciamento Microsoft App-V, execute esse cmdlet novamente para sincronizar a biblioteca de aplicativos com o servidor de gerenciamento 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 Microsoft App-V adicionados à biblioteca de aplicativos.

  Esse cmdlet remove os servidores de gerenciamento e publicação Microsoft App-V especificados, além de todos os pacotes App-V associados.

Execute o módulo de descoberta para servidores e pacotes App-V em um computador ingressado no domínio nesse local de recurso. Siga as orientações em Instalar e usar o SDK do PowerShell remoto para começar. Continue executando os scripts ou cmdlets do PowerShell. Veja os exemplos a seguir.

Atividades de exemplo

Importe o módulo de descoberta do pacote App-V do Citrix DaaS.

```
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```



```
<!--NeedCopy-->
```

Percorrer o diretório de armazenamento de pacotes App-V e carregar cada pacote.

```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Detectar e carregar pacotes registrados em um servidor de gerenciamento Microsoft App-V.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
<!--NeedCopy-->
```

Detectar servidores de gerenciamento e publicação Microsoft App-V e adicionar a configuração à biblioteca de aplicativos. Isso também importa todos os pacotes gerenciados pelo servidor de gerenciamento Microsoft App-V no modo de administração dupla.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer.domain.net – PublishingServerUrl http://AppVManagementServer.domain.net:8001
<!--NeedCopy-->
```

Ler a documentação de ajuda do PowerShell incluída no módulo.

```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

Limitações

- Você não pode detectar pacotes App-V em sua infraestrutura de localização 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 em tempo real com o servidor de gerenciamento Microsoft App-V. Alterações a pacotes e outras configurações no servidor de gerenciamento Microsoft App-V não são refletidas no console de gerenciamento do Citrix DaaS até que `Import-AppVDualAdminCloud` seja executado novamente.

API Monitor Service OData

Além de usar as funções Monitor para exibir dados históricos, você pode consultar dados usando a API do Monitor Service. Use a API para:

- Analisar tendências históricas para planejamento
- Efetuar a solução detalhada de problemas de conexão e falhas de máquina
- Extrair informações para fornecer a outras ferramentas e processos; por exemplo, usar tabelas PowerPivot do Microsoft Excel para exibir os dados de diferentes maneiras
- Criar uma interface de usuário personalizada além dos 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

As APIs do Citrix DaaS estão disponíveis em https://developer.cloud.com/citrixworkspace/citrix-daas.

Aviso de isenção de responsabilidade

Este software/código de amostra é fornecido a você "NO ESTADO EM QUE SE ENCONTRA", 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 TODA E QUALQUER GARANTIA, EXPRESSA, IMPLÍCITA, ESCRITA, ORAL OU ESTATUTÁRIA, INCLUINDO, SEM LIMITAÇÃO, GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA, TÍTULO E NÃO VIOLAÇÃO. Sem limitar a generalidade do acima exposto, você reconhece e concorda que (a) o software/código de amostra poderá apresentar erros, falhas de projeto ou outros problemas, possivelmente resultando em perda de dados ou danos à propriedade; (b) poderá não ser possível tornar o software/código de amostra totalmente funcional; e (c) a Citrix pode, sem aviso prévio ou responsabilidade perante você, deixar de disponibilizar a versão atual e/ou quaisquer versões futuras do software/código de amostra. Em nenhum caso o software/código deve ser usado para apoiar atividades ultraperigosas, incluindo, mas não se limitando a, suporte de 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 AMOSTRA, INCLUINDO, SEM LIMITAÇÃO, DANOS DIRETOS, ESPECIAIS, INCIDENTAIS, PUNITIVOS, CONSEQUENCIAIS OU OUTROS, MESMO QUE AVISADOS SOBRE A POSSIBILIDADE DE TAIS DANOS. Você concorda em indenizar e defender a Citrix contra quaisquer reclamações decorrentes do uso, modificação ou distribuição do código.