Citrix Virtual Apps e Desktops 7 2407

> **Importante:**
>
> A estratégia de ciclo de vida do produto para Versões Atuais (CR) e Versões de Serviço de Longo Prazo (LTSR) é descrita em Marcos do Ciclo de Vida.

> O Citrix Virtual Apps and Desktops oferece uma solução de virtualização para entrega de aplicativos e desktops a qualquer dispositivo, em qualquer rede, ao mesmo tempo em que aprimora a segurança dos dados, reduz custos e aumenta a produtividade.

O programa Long Term Service Release (LTSR) para Citrix Virtual Apps and Desktops oferece estabilidade e suporte de longo prazo para as versões do Citrix Virtual Apps and Desktops.

A Atualização Cumulativa 5 (CU5) é a atualização mais recente para o LTSR 2203. Os LTSRs também estão disponíveis para o Citrix Virtual Apps and Desktops 1912.

- Para obter informações sobre casos de uso, consulte `<https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>`.
- Para saber mais sobre os componentes e tecnologias nas implantações do Citrix Virtual Apps and Desktops, consulte Visão geral técnica.

Versões anteriores

A documentação para outras versões atualmente disponíveis está localizada em Citrix Virtual Apps and Desktops.

Para versões ainda anteriores, a documentação está arquivada em Documentação Legada.

Citrix Virtual Apps and Desktops no Citrix Cloud™

A oferta do Citrix Cloud Virtual Apps and Desktops é o Citrix DaaS. Para obter mais informações, consulte Citrix DaaS.

Links úteis

- Citrix Supportability Pack
- LTSR FAQ
- Opções de serviço do Citrix Virtual Apps and Desktops
- Datas do ciclo de vida do produto
- Programa LTSR para Citrix Workspace app

O que há de novo

Sobre a versão

Esta versão do Citrix Virtual Apps and Desktops inclui novas versões dos Agentes de Entrega Virtual (VDAs) do Windows e novas versões de vários componentes principais. Você pode:

- **Instalar ou atualizar um site**: Use a ISO desta versão para instalar ou atualizar componentes principais e VDAs. A instalação ou atualização para a versão mais recente permite que você use os recursos mais recentes.
- **Instalar ou atualizar VDAs em um site existente**: Se você já tem uma implantação e não está pronto para atualizar seus componentes principais, ainda pode usar vários dos recursos HDX™ mais recentes instalando (ou atualizando para) um novo VDA. A atualização apenas dos VDAs pode ser útil quando você deseja testar aprimoramentos em um ambiente que não seja de produção.

  Após atualizar seus VDAs para esta versão (da versão 7.9 ou posterior), você não precisa atualizar o nível funcional do catálogo de máquinas. O valor **7.9 (ou posterior)** permanece o nível funcional padrão e é válido para esta versão. Para obter mais informações, consulte Versões de VDA e níveis funcionais.

Para instruções de instalação e atualização:

- Se você estiver construindo um novo site, siga a sequência em Instalar e configurar.
- Se você estiver atualizando um site, consulte Atualizar uma implantação.

Citrix Virtual Apps e Desktops 7 2407

Suporte para Windows Server 2025

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

Configurações Padrão Seguras

O instalador do VDA tem uma nova opção que altera a configuração padrão para vários recursos de habilitado para desabilitado para uma configuração pronta para uso mais segura. Para obter mais informações, consulte Instalar VDAs.

Aprimoramento no relatório de telemetria de uso

O recurso de relatório de telemetria de uso foi aprimorado para coletar e processar dados sobre como as licenças são utilizadas para produtos, componentes e recursos Citrix® que são implantados em ambientes gerenciados pelo cliente. Este aprimoramento garante a conformidade com o licenciamento para produtos Citrix on-premises.

Para aproveitar este aprimoramento, atualize para a versão mais recente do servidor de licenças. Para obter mais informações, consulte:

- Telemetria de licenciamento Citrix
- Atualizações necessárias do servidor de licenças
- Perguntas frequentes sobre telemetria de licença Citrix

Para a lista de elementos de dados de Telemetria de Licenciamento, consulte Elementos de dados de Telemetria de Licenciamento Citrix.

Exclusões de porta de loopback virtual

Agora você tem a opção de excluir portas específicas do loopback virtual para que as chamadas feitas por aplicativos para o endereço de loopback em quaisquer portas especificadas não sejam alteradas para o endereço de loopback específico da sessão. Para obter mais informações, consulte Loopback virtual.

Dimensionamento aprimorado da janela LogonUI para aplicativos contínuos

O dimensionamento da janela **LogonUI** foi aprimorado para cenários em que a passagem de autenticação não ocorre. A janela LogonUI é dimensionada com base na resolução do monitor e nas configurações de DPI usadas, o que garante que a janela LogonUI completa seja visível sem nenhum corte. Para obter mais informações, consulte Como modificar o LogonUI para visualizar a mensagem de isenção de responsabilidade do Windows em tamanho real ao abrir aplicativos publicados.

Aprimoramentos do verificador de logoff para aplicativos publicados

Com este novo recurso, agora você tem a opção de detectar automaticamente os aplicativos de inicialização configurados no sistema e adicioná-los automaticamente à lista de processos do sistema para que esses aplicativos não bloqueiem o logoff quando a última janela do aplicativo publicado for fechada. Para obter mais informações, consulte Solução de problemas de logoff de sessão com aplicativos publicados.

Lista de permissões de canal virtual para DVC

Agora você pode usar a lista de permissões de canal virtual para DVC para controlar quais canais virtuais dinâmicos personalizados são permitidos em seu ambiente. Para obter mais informações, consulte Lista de permissões de canal virtual para DVC.

Virtual Delivery Agents (VDAs) 2407

Reestruturação de documentos para métodos de implantação de VDA de terceiros

A página de implantações de VDA de terceiros foi reestruturada para conter instruções detalhadas adicionais. Para obter mais informações, consulte Implantações de VDA de terceiros.

Registro de VDA baseado em token para VDAs não provisionados por MCS (Prévia)

Com esse recurso, agora você pode gerar e gerenciar tokens de registro para VDAs não provisionados por MCS. Essa implementação permite o registro de VDA via WebSocket sem provisionar os VDAs com MCS. Esse recurso também oferece suporte a Linux Virtual Delivery Agent, Citrix Virtual Delivery Agent para macOS e VDAs não ingressados no domínio com Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Registrar VDAs não provisionados por MCS usando tokens.

Web Studio

Clareza sobre políticas dependentes

Algumas configurações dependem de outras configurações. Por exemplo, uma configuração filha pode ser configurada, mas se sua configuração pai não estiver habilitada, a configuração filha configurada não terá efeito. As dependências não eram claras antes. A partir desta versão, é fornecida clareza sobre quais são as políticas pai que devem ser configuradas primeiro antes que

você possa configurar as políticas filhas. Para obter mais informações, consulte Configurações de política.

Políticas de seleção múltipla

Agora você pode selecionar várias políticas e verificar os seguintes aprimoramentos:

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

Observação:

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

Proteção de Aplicativo Contextual

Com esse recurso, os administradores podem aplicar o controle de Proteção de Aplicativo **Anti-Captura de Tela** e **Anti-registro de teclas** em dispositivos e usuários de forma contextual, em vez de ter os controles sempre habilitados ou sempre desabilitados. Essa implementação ajuda você a aplicar a Proteção de Aplicativo Anti-Captura de Tela e Anti-registro de teclas somente quando necessário. Para obter mais informações, consulte Gerenciar Proteção de Aplicativo.

Suporte à autenticação por cartão inteligente

O Web Studio agora oferece suporte à autenticação por cartão inteligente, permitindo que os administradores acessem o Web Studio usando cartões PIV e CAC. Para obter mais informações, consulte Configurar autenticação por cartão inteligente para Web Studio e Habilitar autenticação por cartão inteligente.

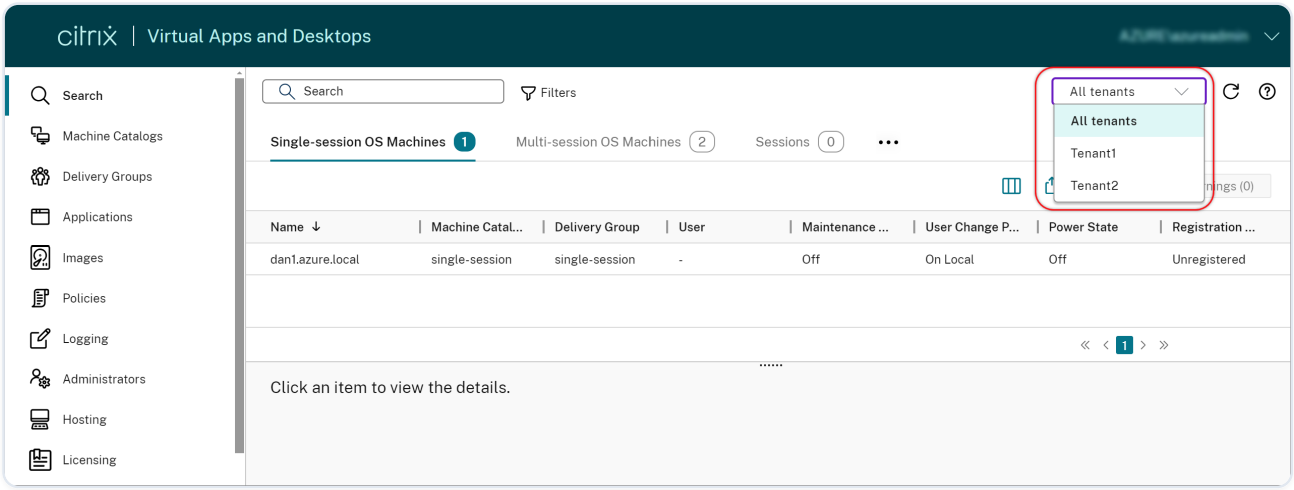
Gerenciamento de locatários

Com o gerenciamento de locatários, agora você pode configurar partições de gerenciamento dentro de um único site do Citrix Virtual Apps and Desktops. Este recurso é ideal para organizações que operam com diferentes silos de negócios, como divisões independentes ou equipes de gerenciamento de TI separadas.

Para configurar o gerenciamento de locatários, siga estas etapas:

1. Criar locatários. Vá para **Administradores > Escopos**, crie escopos de locatário e associe esses escopos a recursos e configurações relacionados, como catálogos de máquinas e grupos de entrega.
2. Adicionar administradores para locatários. Vá para **Administradores > Administradores** e atribua contas de usuário com funções e locatários conforme necessário.

Como administrador com acesso apropriado a um locatário, você pode visualizar e selecionar seu nome na lista suspensa **Todos os Locatários** no canto superior direito do Web Studio. Em seguida, gerencie recursos e configurações associados apenas a esse locatário. Para obter mais informações, consulte Configurar o gerenciamento de locatários.



Habilitar Cache de Host Local (LHC) para VDAs agrupados de sessão única gerenciados por energia

Por padrão, VDAs agrupados de sessão única provisionados usando MCS ou Citrix Provisioning ficam indisponíveis no modo LHC. Com o Web Studio, agora você pode substituir esse comportamento padrão por grupo de entrega, tornando esses VDAs disponíveis para novas conexões durante o LHC. Para obter mais informações, consulte Criar grupos de entrega e Gerenciar grupos de entrega.

Gerar e gerenciar tokens de registro de VDA

O registro de VDA baseado em token reduz a carga nos Cloud Connectors e diminui os pontos potenciais de falha. Com o Web Studio, agora você pode gerar e gerenciar tokens de registro para VDAs não provisionados por MCS, otimizando as implantações baseadas em token de registro. Para obter mais informações, consulte Gerar e gerenciar tokens de registro.

Criar VMs persistentes de várias sessões

Ao criar um catálogo de máquinas de várias sessões, agora você pode especificar se deseja torná-las persistentes. Para máquinas persistentes de várias sessões, lembre-se de que as alterações que os usuários fazem nos desktops são salvas e acessíveis a todos os usuários autorizados. Para obter mais informações, consulte Criar catálogos de máquinas.

Peak Autoscale™ Atribuição de Ligação

Quando os desktops persistentes são ligados, mas permanecem sem uso ou se nenhum usuário faz logon, os administradores podem definir o tempo de espera para realizar ações como, nenhuma ação, suspender ou desligar.

- Para máquinas atribuídas, onde ela está ligada, mas uma sessão não foi conectada a ela dentro do tempo definido após o início do horário de pico, você pode adicionar uma política no nível do grupo de entrega para desligar a máquina.
- Para máquinas atribuídas, onde ela está em estado de retomada, mas uma sessão não foi conectada a ela dentro do tempo definido após o início do horário de pico, você pode adicionar uma política no nível do grupo de entrega para suspender a máquina.

Este recurso é útil se houver um usuário final de licença, ou que não fez logon, ou se uma empresa tiver um feriado prolongado, então você pode definir o tempo de espera e as ações de desconexão da máquina a serem tomadas para ajudar a reduzir o custo de consumo do Azure. Para obter mais informações, consulte Grupos de entrega aleatórios de SO de sessão única e Grupo de entrega estático de SO de sessão única.

Entregue aplicativos empacotados para desktops estáticos de sessão única e PCs de escritório

Com este aprimoramento, agora você pode entregar aplicativos empacotados para todos os tipos de desktops. Para entregar aplicativos empacotados para desktops, adicione esses aplicativos aos grupos de entrega usando estas formas:

- Adicione aplicativos durante a criação do grupo de entrega.

- Adicione aplicativos a um grupo de entrega existente usando uma destas entradas: **Delivery Groups > Add Applications > Applications**, **Applications > Properties > Groups**, ou **App Packages > Packages > Add Delivery Groups**.

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

Modificar nomes de exibição de desktop

Aprimoramos a página **Alocação de Máquina** para grupos de entrega *estáticos de SO de sessão única* introduzindo uma nova coluna, **Nome de exibição**. Com esta adição, agora você pode modificar os nomes de exibição de desktop para máquinas atribuídas a usuários. Para obter mais informações, consulte Gerenciar atribuições de usuário.

Reiniciar e desligar máquinas de sessão única na guia Sessões do nó Pesquisar

Na guia **Sessões** do nó **Pesquisar**, agora você pode procurar sessões de usuário em um estado não saudável e reiniciar ou desligar facilmente as máquinas de sessão única associadas dentro da mesma guia. Este recurso aumenta a eficiência, permitindo uma ação rápida sobre problemas de sessão identificados em uma única interface.

Atribuir letras de unidade a discos de cache de write-back

Anteriormente, você só podia atribuir uma letra de unidade específica ao disco de cache de write-back usando um cmdlet do PowerShell. Agora você pode realizar a mesma tarefa usando o Web Studio. Para obter mais informações, consulte Criar catálogos Microsoft.

Tentar novamente a criação do catálogo após falha

Quando a criação do catálogo falha, agora você pode tentar novamente a criação do catálogo. Para garantir uma criação bem-sucedida, verifique as informações de solução de problemas e resolva os problemas. As informações descrevem os problemas encontrados e fornecem recomendações para resolvê-los. Catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, vá para a guia **Solução de problemas** de cada catálogo. Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Exibir IPs de cliente em logs de configuração

Em **Registro > Eventos**, agora você pode visualizar detalhes de endereço IP em logs, facilitando o rastreamento das origens das ações. Para mostrar a coluna de endereço IP na visualização

principal, clique no ícone **Colunas a Exibir** no canto superior direito dos logs e, em seguida, selecione **IP do Cliente**.

Aprimoramentos na ajuda contextual

Redesenhamos o painel de ajuda para fornecer uma experiência mais informativa, oferecendo informações direcionadas para cada nó dentro do Web Studio. Ao clicar no ícone de Ajuda em qualquer nó, agora você pode acessar um conjunto abrangente de recursos destinados a fornecer uma experiência de aprendizado completa, ajudando você a entender melhor os recursos relacionados:

- Acesse documentos-chave especificamente relacionados ao nó selecionado.
- Mantenha-se informado sobre as atualizações de serviço, incluindo Roteiro da Citrix, Problemas conhecidos, Limites, Requisitos do sistema e Recursos novos.
- Acesse recursos expandidos como Blogs da Citrix, Comunidade Citrix, Recurso Citrix Explicado, Documentação do Produto Citrix, Suporte Citrix e Documentação do Desenvolvedor.

Pesquisa aprimorada

Aprimoramos o nó Pesquisar introduzindo os seguintes novos recursos:

- Dois novos filtros, **Zona** e **Tipo de Provisionamento**, para maior precisão e usabilidade aprimorada.
- Duas novas colunas:
  - Coluna **Nome de Exibição do Usuário** na guia **Sessões**. Com esta coluna, você pode identificar rapidamente as sessões associadas a um usuário específico.
  - Coluna **Nome de Exibição da Área de Trabalho** nas guias **Máquinas OS de sessão única** e Sessões. Com esta coluna, você pode identificar rapidamente a máquina associada a uma área de trabalho específica.
- Novos filtros para pesquisa eficiente. Para obter mais informações sobre essas duas colunas, consulte Ações e colunas da máquina e Ações e colunas da sessão.
- Fixadores de filtro no painel de pesquisa dos nós **Pesquisar** e **Catálogos de Máquinas**, permitindo que você mantenha os filtros de pesquisa usados com frequência acessíveis nas páginas.

Aprimoramentos no nó Aplicativos

Implementamos os seguintes aprimoramentos no nó Aplicativos:

- Funcionalidade estendida de Colunas para Exibir e Exportar para as guias Aplicativos e Grupos de Aplicativos. Com os ícones recém-introduzidos no canto superior direito, agora você pode personalizar as visualizações principais para aplicativos e grupos de aplicativos e exportar registros dessas visualizações para arquivos CSV.
- Adicionado o campo Zonas no painel Detalhes dos aplicativos, permitindo que você visualize as zonas onde um aplicativo reside. Esta informação é útil ao distinguir entre aplicativos que compartilham nomes idênticos, mas que se originam de zonas diferentes. Para obter mais informações, Zonas.

Cache de dados para os nós Catálogos de Máquinas e Hospedagem

Introduzimos o cache de dados para o nó **Catálogos de Máquinas** do Citrix DaaS™. Este aprimoramento reduz significativamente os tempos de carregamento da página quando você navegar para o nó **Catálogos de Máquinas**, melhorando a experiência geral do usuário.

Interface do usuário da Política de Acesso redesenhada para controle de acesso a recursos mais flexível

Redesenhamos a interface do usuário **Editar grupo de entrega > Política de Acesso** para oferecer mais flexibilidade no gerenciamento do acesso a recursos para grupos de entrega. A seguir estão os principais recursos disponíveis com o novo design:

- **Suporte para adicionar políticas.** Agora você pode adicionar políticas de acesso para restringir o acesso a recursos com base nos atributos das conexões do usuário. Uma política pode consistir em dois tipos de critérios:
  - **Critérios de inclusão.** Permitem especificar as conexões de usuário que têm permissão para acessar o grupo de entrega.
  - **Critérios de exclusão.** Permitem especificar as conexões de usuário que estão proibidas de acessar o grupo de entrega.
- **Suporte a filtros expandido.** Agora você pode definir critérios de inclusão e exclusão usando uma variedade de filtros SmartAccess. Esses filtros incluem filtros de Workspace, como `Citrix.Workspace.UsingDomain` e `Citrix-Via-Workspace`, bem como filtros para acesso adaptativo baseado na localização da rede.

- **Suporte à lógica 'Corresponder a Todos' para critérios incluídos.** A nova lógica permite que você alcance um alto nível de precisão e controle ao especificar conexões de usuário permitidas para grupos de entrega.

Para obter mais informações, consulte Restringir o acesso a recursos em um grupo de entrega.

Filtragem avançada de imagens para criação de catálogo AWS

Ao selecionar modelos de máquina durante a criação de catálogo AWS, agora você pode filtrar o inventário de AMI da AWS para um modelo de destino usando estes critérios de pesquisa:

- Nome da imagem
- ID da imagem
- Tags da imagem

A lista de modelos de máquina é carregada dinamicamente à medida que você rola a lista para baixo — 25 itens são carregados inicialmente e mais são carregados à medida que você rola.

Suporte para criação de VMs que suportam hibernação na AWS

Agora você pode criar catálogos de máquinas que suportam a hibernação de VMs em seus ambientes AWS, aumentando a relação custo-benefício geral de sua implantação. Observe que você também pode editar um catálogo para incluir VMs com capacidade de hibernação se o perfil de máquina associado suportar essa capacidade. Para obter mais informações, consulte Hibernação.

Novas validações de política

Validações de política adicionais são adicionadas. Como resultado, habilitar políticas ou fazer um upgrade in-place pode levar à perda de dados de política se configurações de política inválidas estiverem presentes. Se você criar ou editar as políticas usando um método diferente do Web Studio, a Citrix recomenda que você use a versão mais recente do SDK e do snap-in. Para obter mais informações, consulte CTX676686.

Conjuntos de políticas

Em **Web Studio > Políticas**, agora você pode agrupar políticas para acesso simplificado baseado em função usando conjuntos de políticas. Você pode então atribuir escopos e grupos de entrega aos seus conjuntos de políticas para que apenas administradores autorizados possam gerenciar as políticas que se aplicam aos seus usuários e máquinas relevantes. Para obter mais informações, consulte Conjuntos de políticas.

Políticas de seleção múltipla

Agora você pode selecionar várias políticas e verificar as seguintes melhorias:

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

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

Clareza sobre políticas dependentes

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

Atualizações simplificadas de sub-redes para catálogos de máquinas

Anteriormente, para alterar as configurações de sub-rede de um catálogo de máquinas, era necessário excluí-lo e recriá-lo. Com este recurso, agora você pode obter a mesma funcionalidade editando o catálogo. Observe que apenas as novas máquinas virtuais criadas sob o catálogo estarão nas sub-redes recém-associadas. Essa melhoria reduz a necessidade de exclusão de catálogo e tarefas associadas. Para obter mais informações, consulte Editar um catálogo.

Nova configuração de política - Coleta de métricas de sessão

Essa configuração permite que a Citrix colete métricas de sessão de usuário e máquina entre o VDA e o Workspace para melhorar a experiência do usuário.

A Citrix coleta dados como sistema operacional, tempo de atividade, informações do sistema do computador, detalhes do controlador de vídeo, versão do VDA, tipo de implantação e status de ingresso no domínio. Além disso, algumas configurações de sessão, juntamente com dados de desempenho e confiabilidade, são coletadas para auxiliar nos esforços de melhoria do produto. Por padrão, essa configuração está habilitada. Para obter mais informações, consulte Coleta de métricas de sessão.

Integração do Secure Private Access com o Web Studio

A partir da versão 2407, a integração do Secure Private Access com o Web Studio foi aprimorada para que os administradores possam acessar o console SPA dentro do console do Web Studio. Para obter mais informações, consulte Integração do Secure Private Access com o Web Studio.

Citrix Studio

Citrix Studio agora em modo de manutenção

A partir desta versão, o Citrix Studio entra em modo de manutenção. Não adicionaremos mais novos recursos a ele, mas nos concentraremos em sua estabilidade e segurança por meio de correções de bugs e patches de segurança regulares. Recomendamos a transição para o Web Studio, a próxima geração do Citrix Studio. O Web Studio é um console de gerenciamento baseado na web que oferece paridade total de recursos com o Citrix Studio, juntamente com uma experiência de gerenciamento moderna, recursos aprimorados e novos recursos poderosos. Para obter mais informações, consulte Instalar o Web Studio.

Citrix Director

Gráficos de monitoramento de uso de aplicativos no Dashboard

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

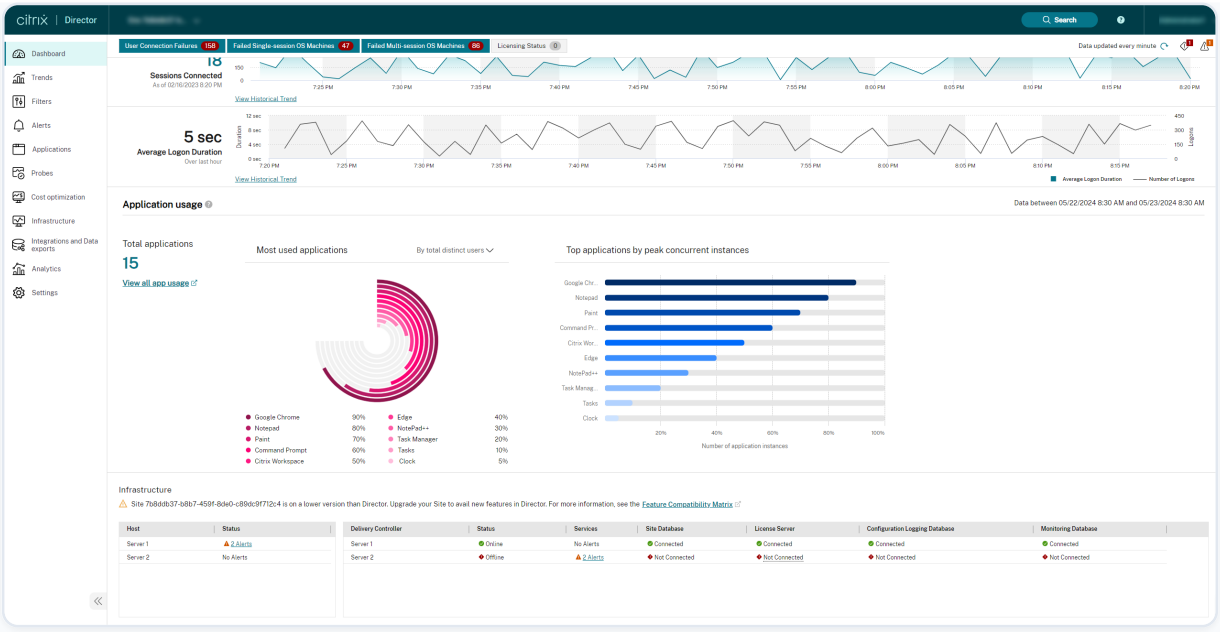
Esses gráficos compreendem os seguintes pontos de dados para as últimas 24 horas:

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

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

Observação:

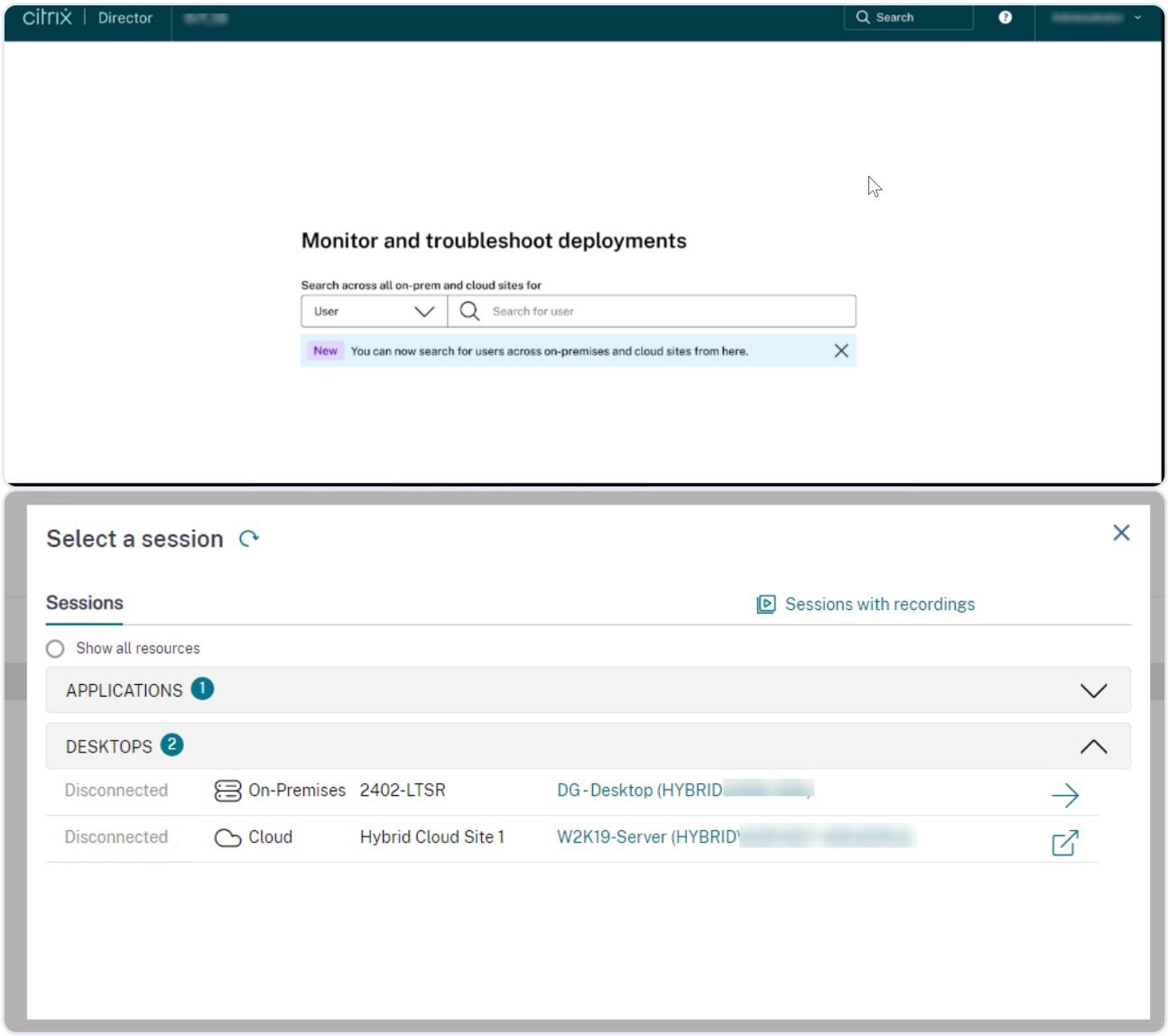
Este recurso está disponível apenas para sites com licença platinum.



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

Pesquisa unificada para usuários em nuvem e locais

Anteriormente, durante a triagem, ao pesquisar um usuário no Director, você obtinha os detalhes do usuário somente se ele fosse de um site local. Se o usuário fosse de um site na nuvem, você precisava ir para Monitor e pesquisar novamente. Com essa funcionalidade de pesquisa aprimorada, você pode pesquisar usuários de sites na nuvem ou sites locais usando a opção **Pesquisar** no Director. Esse recurso reduz o tempo médio para resolver problemas e oferece uma experiência perfeita com um único console, sem qualquer crescimento rápido no tamanho do banco de dados.



Para obter mais informações, consulte Pesquisa unificada para usuários em nuvem e locais.

Visualização de logon de sessão aprimorada

A nova opção **Inicialização da Máquina** com as seguintes subseções na guia **Logon da Sessão** na página **Filtros** -> **Detalhes do Usuário** fornece o detalhamento do tempo levado para iniciar uma máquina virtual durante diferentes fases:

- **Ligar** - Exibe o tempo necessário para ligar uma máquina virtual
- **Inicialização e registro** - Exibe o tempo necessário para inicializar e registrar uma máquina virtual

O botão recolhível recém-introduzido na página **Logon de Sessão** ajuda a recolher ou expandir as opções em **Inicialização da Máquina** e **Sessão Interativa**.

Juntamente com as opções padrão da tabela **Fases de Duração do Logon**, que são **Fase de Logon da Sessão** e **Duração**, você também pode escolher as seguintes colunas na página **Logon de Sessão**:

- Hora de início
- Hora de término
- Média de 7 dias do Grupo de Entrega (seg)
- Média de 7 dias do Usuário (seg)

Você também pode exportar os dados precedentes para um arquivo .CSV.

As colunas recém-adicionadas **Ligar** e **Inicialização e registro** podem ser adicionadas à tabela **Duração do Logon por Sessão do Usuário** em **Tendências** -> **Desempenho do Logon** > **Escolher Colunas**. Você também pode exportar os relatórios na tela **Desempenho do Logon**.

Este aprimoramento ajuda a entender e solucionar facilmente problemas relacionados à duração do logon. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Opções para solucionar problemas quando os dados de ICA® RTT ou Duração de Logon da Sessão não são preenchidos

Anteriormente, quando o serviço EUEM ou o serviço de Gerenciamento de Perfil falhava ao ser executado, o motivo da falha na obtenção dos dados relacionados ao ICA RTT ou à Duração do Logon da Sessão não era exibido. Com este novo recurso, você pode obter o motivo da falha e a solução correspondente para a falha.

Para obter mais informações, consulte Opções para solucionar problemas quando os dados de ICA RTT ou Duração do Logon da Sessão não são preenchidos.

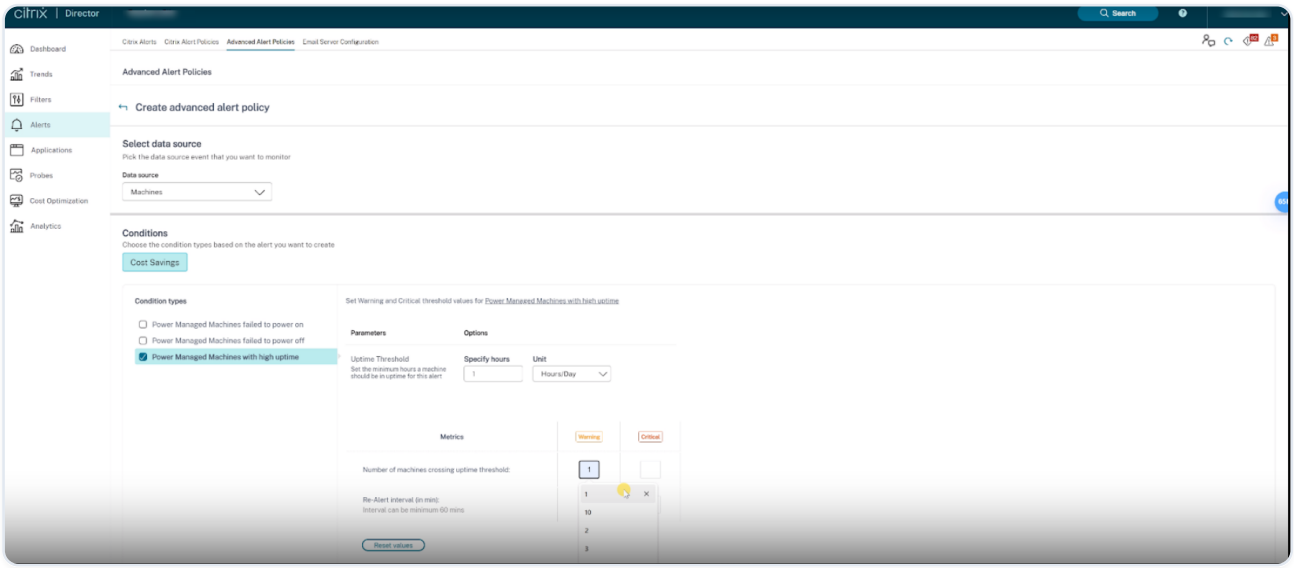
Nome da área de trabalho publicada

O Citrix Director agora exibe o nome da área de trabalho publicada na interface do usuário. Este novo campo permite diferenciar entre grupos de usuários dentro do mesmo grupo de entrega. Você também pode gerar relatórios personalizados para esses grupos de usuários. Este novo campo é adicionado às seções **Filtros**, **Relatórios Personalizados** ou **Detalhes da Máquina** da interface do usuário do Citrix Director.

Políticas de alerta avançadas

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

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



Para obter mais informações, consulte Políticas de alerta avançadas.

Aprimoramentos no conteúdo do alerta

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

Atualmente, esse aprimoramento está disponível apenas nos seguintes alertas:

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

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

Opção para visualizar e filtrar tipo de sessão e último horário de inicialização

O Citrix Director agora oferece uma opção para adicionar **Tipo de Sessão** como uma nova coluna. Os diferentes tipos de sessão disponíveis são área de trabalho e aplicativo. Você também pode adicionar **Tipo de Sessão** como uma nova coluna adicionando-a em **Filtros** > **Sessões** > **Escolher Colunas.** Isso também é adicionado em **Tendências > Sessões.**

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

Opção para filtrar dados por período de tempo em Sessões e instâncias de Aplicativos

O Citrix Director agora inclui o filtro de período de tempo nas **Sessões** e **instâncias de Aplicativos** da guia **Filtros**. Agora você pode filtrar as sessões e instâncias de aplicativos para:

- Últimos 60 minutos
- Últimas 24 horas
- Últimos 7 dias

Além disso, a opção de período de tempo personalizado foi adicionada nas guias **Sessões**, **Conexões** e **Instâncias de aplicativo** da guia **Filtros**.

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

Painel de Métricas de Desempenho Aprimorado

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

Para obter mais informações, consulte Métricas de Desempenho.

Aprimoramento na guia Desempenho da Sessão

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

- Detalhes adicionais sobre o Conector e o Citrix Gateway na exibição Topologia da Sessão, como IP do endpoint, SO do endpoint e versão do aplicativo Citrix Workspace™ no salto do endpoint
- ID Pop, localização e país do serviço de gateway, IP do conector, nome do conector e localização do recurso
- Detalhes sobre os elementos de dados ausentes do Conector e do Citrix Gateway e links para baixar a versão mais recente
- Detalhes do hipervisor, como o tipo de hipervisor, nome da conexão do host e nome do host
- Nome do protocolo HDX na seção de detalhes da sessão e na exibição de topologia da sessão
- As seguintes métricas de endpoint que existem no aplicativo Citrix Workspace para Windows:
    - Força do sinal Wi-Fi
    - Taxa de transferência de entrada e saída
    - Tipo de interface de rede
    - Velocidade do link

Esse aprimoramento ajuda a solucionar problemas relacionados a sessões rapidamente.

Aprimoramento na triagem de problemas de carregamento de perfil de usuário

O Citrix Director agora oferece suporte à coleta de métricas de duração de carregamento de perfil e de contêiner do contêiner do Citrix Profile Management e do contêiner FSLogix. Este aprimoramento auxilia os administradores a receber dados abrangentes de uso e desempenho de perfil em relatórios de sessão do usuário. Com esses dados, você pode identificar e resolver problemas com maior eficiência.

Para obter mais informações, consulte Carregamento de perfil.

Otimização de custos

O Citrix Director agora apresenta um novo recurso chamado Otimização de Custos, que ajuda a analisar o uso de máquinas virtuais e sessões de forma eficaz. Este recurso fornece

representações visuais perspicazes sobre como otimizar o custo. Ele também ajuda a eliminar máquinas desnecessárias e, assim, reduzir custos.

A página **Otimização de Custos** inclui os seguintes recursos:

- Economia de custos
- Dimensionamento de infraestrutura

Economia de custos

A página **Economia de custos** fornece uma representação visual da economia de infraestrutura acumulada durante um período selecionado e prevê a economia esperada para os dias restantes. Ao analisar o uso e as sessões da máquina, esta página ajuda você a identificar a economia alcançada e as oportunidades de redução de custos. Esta página oferece:

- Visão sobre a otimização dos custos de infraestrutura
- O valor economizado
- Informações sobre uma série de cenários que podem resultar na superação dos custos projetados
- Oportunidades potenciais para identificação e planejamento estratégico para realizar economia de custos de infraestrutura

A página **Otimização de Custos** > **Economia de custos** inclui **Economia estimada** e **Relatório de economia do Autoscale.**

A **Economia estimada** ajuda a avaliar a utilização eficiente dos recursos de infraestrutura. A Economia estimada ajuda a avaliar a utilização eficiente dos recursos de infraestrutura. A economia de custos é exibida na moeda do hipervisor ou como uma porcentagem do custo incorrido. Você pode visualizar os resultados para os últimos:

- Sete dias
- Trinta dias
- Três meses
- Seis meses
- Doze meses

O gráfico de **Economia estimada** exibe o seguinte:

- Economias estimadas - Exibe o valor das economias alcançadas na infraestrutura para a duração selecionada

- Máquinas com gerenciamento de energia - Exibe o número total de máquinas com gerenciamento de energia.
- Economia projetada - Exibe quanta economia de infraestrutura pode ser feita para a duração restante

O relatório de **Economia do Autoscale** exibe informações sobre o grupo de entrega para o qual o autoscale está configurado e habilitado. Este relatório é aplicável apenas para máquinas com gerenciamento de energia.

Para obter mais informações, consulte Economia de custos.

Dimensionamento de infraestrutura

A página **Dimensionamento de Infraestrutura** ajuda você a analisar os aspectos de provisionamento e dimensionamento do seu grupo de entrega com base na utilização dos recursos. Com base nesta análise, você pode otimizar o provisionamento e o dimensionamento da máquina para corresponder ao padrão de utilização. Você pode otimizar seus custos de infraestrutura reduzindo os gastos com recursos não utilizados. Você também pode optar por máquinas com especificações de CPU e memória mais baixas se a utilização dos recursos for consistentemente menor do que o provisionado. Você pode otimizar o desempenho optando por máquinas com especificações de CPU e memória mais altas se a utilização dos recursos for consistentemente maior e houver evidências de que isso afeta a experiência da sessão, como as métricas de *Logon e ICARTT*.

Você pode filtrar o dimensionamento da infraestrutura usando o seguinte:

- Grupo de Entrega - Você pode filtrar por grupos de entrega de SO de sessão única ou SO de múltiplas sessões
- Tags - Tags são os nomes de tags aplicados à máquina. Assim, você pode filtrar máquinas com as mesmas tags. Você pode selecionar várias tags, até cinco tags. Ao selecionar várias tags, você pode filtrar todas as máquinas que possuem pelo menos uma das tags de máquina selecionadas aplicadas.
- Período de tempo - Você pode filtrar os dados para as últimas 24 horas, 7 dias e 30 dias.

A página de dimensionamento da infraestrutura oferece:

- Visão detalhada dos detalhes de utilização
- Resumo da utilização dos recursos
- Tendências na utilização de recursos

Clique na guia **Otimização de Custos** no menu esquerdo da página inicial. Em seguida, clique na guia **Dimensionamento de infraestrutura** para acessar a página **Dimensionamento de infraestrutura**.

Você também pode clicar no link **Dimensionar este grupo de entrega** na seção **Detalhes da infraestrutura** na guia **Otimização de Custos** > **Economia de custos** para acessar a página **Dimensionamento de infraestrutura**.

Para obter mais informações, consulte Dimensionamento de infraestrutura.

Inspecionar máquinas com ações de energia recentes

Agora você pode inspecionar máquinas com o status das ações de energia bem-sucedidas e falhas. Este recurso ajuda você a analisar o seguinte:

- Falha ao ligar que causa problemas ao usuário
- Falha ao desligar que aumenta o custo

> **Observação:**
>
> Os dados estão disponíveis apenas para a máquina gerenciada por energia. Os dados não estão disponíveis para as ações de energia realizadas antes que o recurso fosse suportado.

> Você pode visualizar o status da ação de energia das máquinas das seguintes maneiras:

- Na guia **Filtros** -> **Máquinas**. Nesse caso, por padrão, as colunas **Hora da Ação de Energia** e **Resultado da Ação de Energia** ficam visíveis. Você também pode selecionar as colunas que deseja que fiquem visíveis.
- Na guia **Otimização de Custos**. Neste caso, o filtro padrão é **Ação de Energia Acionada Por** está definido como **Autoscale** e o **Resultado da Ação de Energia** está definido como **Falha.**

Com este recurso, você pode visualizar os detalhes dos controles de ação de energia. Por exemplo, você pode visualizar quem acionou a ação, qual ação alterou o estado de energia, o motivo da falha e a hora em que a ação foi concluída. Você também pode exportar esses detalhes.

Para obter mais informações, consulte Inspecionar máquinas com ação de energia recente.

Alerta de ação de ligar falha e ação de desligar falha

O recurso de Notificação e Alerta Proativo do Director foi aprimorado para incluir dois novos alertas, **ação de ligar falha** e **ação de desligar falha**, com base no número de máquinas gerenciadas por energia que falharam ao ligar ou desligar em um grupo de entrega. A nova condição de alerta permite configurar limites de alerta como o número de máquinas gerenciadas por energia que falharam ao ligar ou desligar em um grupo de entrega.

Para mais informações, consulte Ação de ligar falha e Ação de desligar falha.

Alerta de tempo de atividade da máquina

O recurso de Notificação e Alerta Proativo do Director foi aprimorado para incluir um novo alerta, alerta de tempo de atividade da máquina, com base no tempo de atividade de uma máquina gerenciada por energia em um grupo de entrega. Para cada grupo de entrega para o qual as máquinas excederam o limite, você recebe um anexo ou alerta de webhook apenas para esse grupo de entrega.

A nova condição de alerta permite configurar limites de alerta como o número de horas por dia, horas por semana ou horas por mês em que uma máquina é ligada em um grupo de entrega.

Para obter mais informações, consulte Alerta de tempo de atividade da máquina.

Alerta de máquinas não registradas

O recurso de Notificação e Alerta Proativo do Director foi aprimorado para incluir um novo alerta, **Máquinas Não Registradas (em %)**, com base na porcentagem de máquinas não registradas em um grupo de entrega. A nova condição de alerta permite configurar valores de limite de aviso e crítico como uma porcentagem de máquinas não registradas em um grupo de entrega.

Para obter mais informações, consulte Máquinas não registradas.

Integrações e exportações de dados

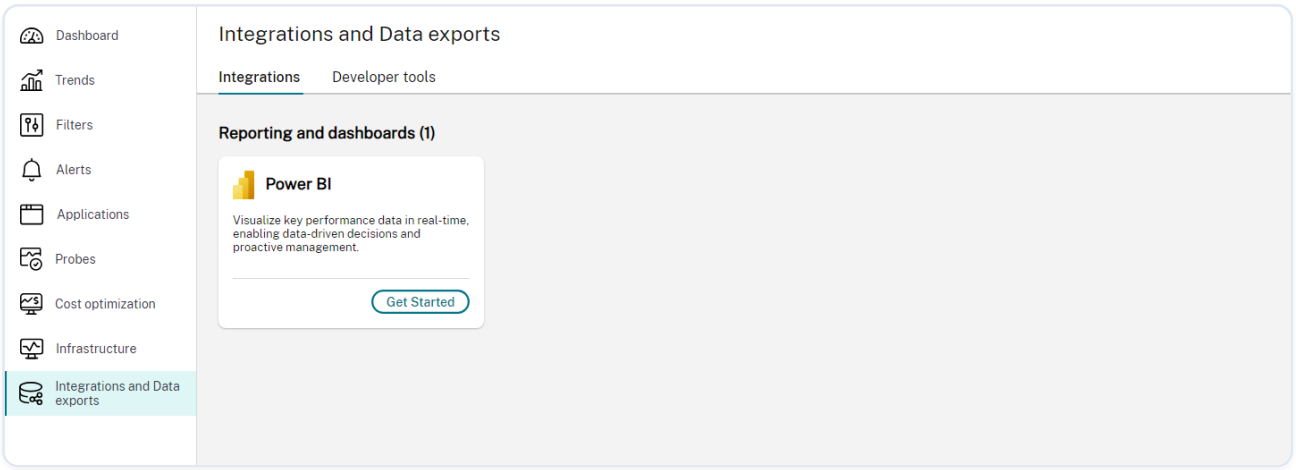
O Citrix Director agora oferece uma nova interface de usuário para integrações e exportações de dados. Este recurso ajuda a melhorar a conscientização sobre as várias interfaces e integrações de terceiros disponíveis no Citrix Director. A página de Integrações e Exportações de Dados recém-introduzida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

- Integrações disponíveis
- Ferramentas de desenvolvedor compatíveis

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

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

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



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

Diagnosticar sessões de usuário históricas

O Citrix Director agora exibe os detalhes das sessões em estado ativo, desconectado ou encerrado. Anteriormente, você só podia ver os detalhes das sessões ativas. Com este recurso, os administradores de help desk podem solucionar problemas com uma sessão que foi encerrada ou em estado encerrado. Os detalhes da sessão estão disponíveis para as últimas 24 horas e os últimos 2 dias. Você pode visualizar os seguintes detalhes de uma sessão encerrada ou terminada:

- Painel Detalhes da Máquina - Exibe os detalhes disponíveis da máquina onde a sessão selecionada foi iniciada.
- Painel Detalhes da Sessão - Exibe os detalhes disponíveis da sessão selecionada.
- Duração do logon da sessão - Exibe as informações sobre a duração do logon para a sessão selecionada. Você pode visualizar o gráfico sobre o tempo gasto para intermediação, inicialização da máquina, conexão HDX, autenticação, GPOs, scripts de logon, carregamento de perfil em disco e sessão interativa.

Para obter mais informações, consulte Diagnosticar sessões de usuário históricas.

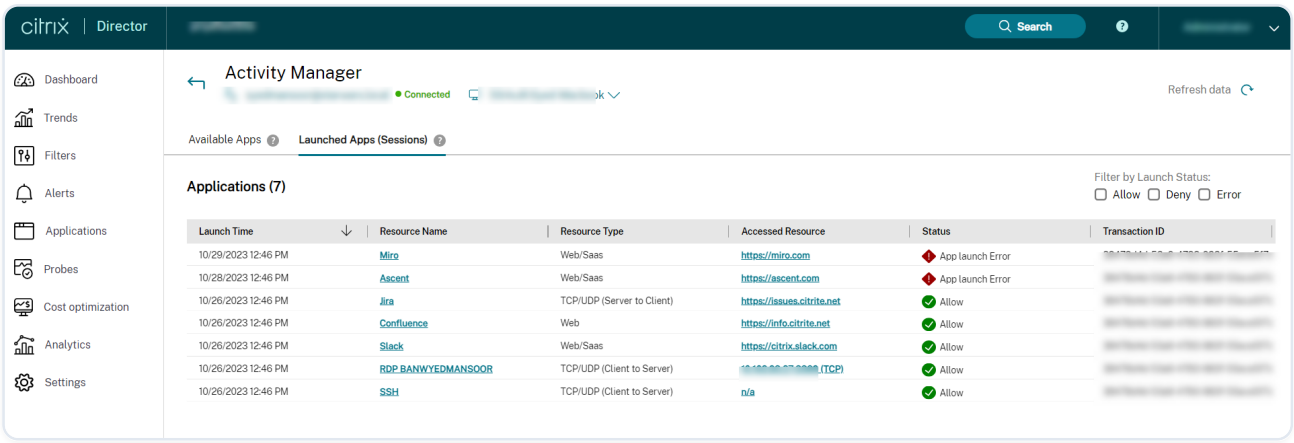
Gerenciador de Atividades para sessão de Acesso Privado Seguro

O Citrix Director oferece a visualização do Gerenciador de Atividades para sessões de Acesso Privado Seguro, que fornece uma visão geral das atividades da sessão. O Gerenciador de Atividades oferece uma visão abrangente de todos os aplicativos e desktops que foram abertos com sucesso, falharam ao abrir e o resultado das políticas definidas no aplicativo Acesso Privado Seguro.

O Gerenciador de Atividades é exibido com os detalhes de **Aplicativos Disponíveis** e **Aplicativos Iniciados**. Você pode encontrar os seguintes detalhes da sessão:

- Hora de início
- Nome do recurso
- Tipo de recurso
- Recurso acessado
- Status
- ID da Transação

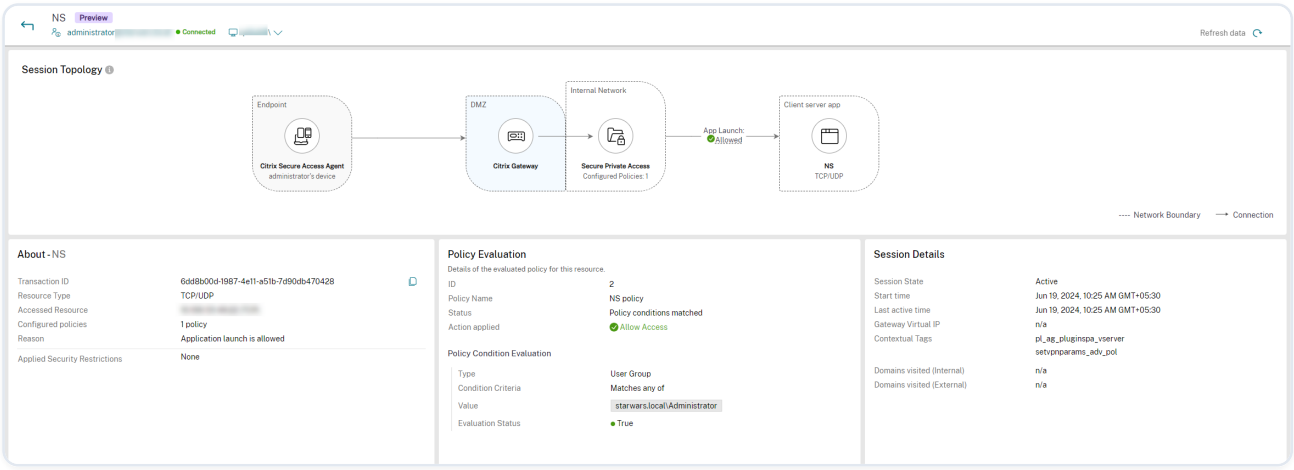
Você também pode filtrar os detalhes anteriores pelo status do aplicativo, como Permitir, Negar e Erro. Você também pode classificar os detalhes com as setas para cima e para baixo.



Para obter mais informações, consulte Exibir o Gerenciador de Atividades para a sessão de Acesso Privado Seguro.

Exibição da topologia da sessão para aplicativos de Acesso Privado Seguro

Você pode visualizar a topologia da sessão para os aplicativos abertos usando o Acesso Privado Seguro. Clique no aplicativo desejado no Gerenciador de Atividades para visualizar a Topologia da Sessão do aplicativo selecionado.



Na exibição **Topologia da Sessão**, você pode visualizar o aplicativo que é aberto usando o Acesso Privado Seguro, o status da avaliação da política e o status do lançamento do aplicativo. Você também pode encontrar os detalhes do aplicativo, da avaliação da política e os detalhes da sessão.

Para obter mais informações, consulte a exibição da topologia da sessão para aplicativos de Acesso Privado Seguro.

Monitoramento de infraestrutura

O Citrix Director agora oferece visibilidade sobre a saúde operacional dos componentes do Citrix Virtual Apps and Desktops. Esse recurso ajuda você a identificar, solucionar e resolver facilmente problemas relacionados à sua infraestrutura. Atualmente, a saúde dos componentes Citrix Provisioning™ (PVS) e StoreFront é monitorada.

Para suportar esse recurso, um novo executável do Windows chamado Citrix Infrastructure Monitor foi introduzido. Isso auxilia na coleta e transmissão de métricas de saúde relevantes dos servidores PVS ou StoreFront™ para o Director.

Esse recurso ajuda você a obter conjuntos de dados de monitoramento críticos e alertas proativos em relação às métricas do sistema dos servidores PVS e StoreFront em um único console no Director. Os dados são coletados a cada cinco minutos dos componentes de monitoramento para garantir as informações mais recentes.

Este recurso visa aprimorar a eficiência operacional, oferecendo monitoramento proativo, métricas detalhadas e alertas automatizados, garantindo que sua infraestrutura Citrix funcione de forma suave e eficiente.

Principais recursos

Monitoramento em tempo real:

- Monitoramento contínuo de componentes da infraestrutura Citrix, como servidores Citrix Provisioning (PVS) e StoreFront.
- Visualizações de painel apresentando a saúde do sistema, utilização de recursos e métricas de desempenho relevantes.

Análise detalhada:

- Fornece análise detalhada sobre as métricas de saúde do sistema, como status de conectividade e status de serviço ou processo para cada componente.
- Detalhes sobre as métricas de utilização de recursos, como CPU, memória e utilização de disco.

Alertas e notificações automatizados:

- Limites de alerta personalizáveis para várias métricas e estados com escopos granulares.
- Notificações em tempo real por e-mail e webhooks.

Casos de uso

Eficiência operacional:

Garante que as equipes de administração da Citrix possam manter alta disponibilidade e desempenho de seus servidores e serviços Citrix. Esse recurso também ajuda a minimizar o tempo de inatividade, identificando proativamente e alertando os administradores sobre problemas antes que eles afetem grupos de usuários significativos.

Resolução mais rápida de tickets:

Monitora as principais métricas de integridade e desempenho do servidor para avaliar a entrega ideal de aplicativos e desktops virtuais aos usuários. Use essas métricas para diagnosticar e resolver reclamações de usuários relacionadas ao desempenho, analisando os componentes associados.

Para mais informações, consulte a seção Monitoramento de infraestrutura [Pré-visualização].

Política de infraestrutura

Esta política foi introduzida para criar alertas relacionados à integridade dos componentes compatíveis do Citrix Virtual Apps and Desktops.

Após a conclusão da configuração do Monitoramento de infraestrutura, você pode usar os dados de integridade disponíveis no Director para configurar alertas para qualquer componente

necessário. Os administradores podem definir condições, escopos e meios de notificação para receber alertas importantes por e-mail ou um payload JSON por meio de webhooks. Os alertas gerados também estão disponíveis na seção **Citrix Alerts** para análise e gerenciamento.

Como parte desta política, as quatro novas categorias a seguir são introduzidas:

- Acessibilidade
- Serviços dependentes
- Impacto
- Utilização de recursos

Você pode definir diferentes condições e modificar a severidade das categorias precedentes conforme necessário nas seções **Crítico** e **Aviso**. Você também pode agendar intervalos de re-alerta para esses alertas.

As condições dentro de cada categoria podem ser definidas com a severidade de Crítico e Aviso com base nas prioridades da sua organização. Você também pode agendar intervalos de re-alerta para esses alertas.

Para obter mais informações, consulte a seção Políticas de infraestrutura (Pré-visualização).

Citrix Scout

Aprimoramento do procedimento de Rastreamento e Reprodução

Anteriormente, você podia usar a interface do usuário para importar os rastreamentos CDF salvos no procedimento de Rastreamento e Reprodução.

A partir da versão 2407, esta opção de interface do usuário foi removida. Ao habilitar a coleta de log adicional, o Scout detecta automaticamente as ferramentas relacionadas ao CDC instaladas em sua máquina e coleta automaticamente os logs de rastreamento relacionados à ferramenta CDC no pacote zip. Você pode personalizar este arquivo zip e anexá-lo ao Scout. Com essa automação, você pode usar o Citrix Scout de forma mais eficaz e diagnosticar os problemas rapidamente.

Para obter mais informações, consulte Habilitar coleta de log adicional.

Machine Creation Services™ (MCS)

Limite aumentado de réplicas por versão de imagem no Azure

O Azure aumentou a contagem máxima de réplicas para uma única versão de imagem da galeria para 100. Com o aumento do limite, agora você pode definir a propriedade `SharedImageGalleryReplicaMaximum` para um valor máximo de 100 ao criar um catálogo de máquinas MCS usando a imagem da Galeria de Computação do Azure. Para obter mais informações, consulte Configurar a Galeria de Computação do Azure.

Suporte para virtualização aninhada do Azure

Com este recurso, se você configurar a VM mestre com virtualização aninhada habilitada, todas as VMs no catálogo de máquinas MCS criadas usando essa VM mestre terão a virtualização aninhada habilitada. Este recurso é aplicável a VMs persistentes e não persistentes. Você pode atualizar um catálogo de máquinas MCS existente e VMs existentes para ter virtualização aninhada por meio da atualização da imagem.

Atualmente, apenas os tamanhos de VM Dv3 e Ev3 suportam virtualização aninhada.

Para obter informações sobre virtualização aninhada, consulte o blog da Microsoft Virtualização Aninhada no Azure.

Obter mensagens de aviso para falha de hibernação

Agora você pode obter mensagens de aviso usando um comando PowerShell Get-ProvOperationEvent em caso de falha de hibernação de VMs provisionadas por MCS e VMs existentes com capacidade de hibernação. Para obter mais informações, consulte Obter mensagens de aviso para falha de hibernação.

Validar permissões na conexão do host no Azure

Anteriormente, em ambientes Azure, você podia validar apenas as credenciais de conexão do host (ID do cliente ou ID do aplicativo) usadas para criar uma conexão com o Azure.

Com este recurso, você pode:

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

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

Alterar a criptografia de disco no Azure

Com este recurso, agora você pode alterar a criptografia de disco em ambientes de virtualização do Azure. Você pode fazer o seguinte:

- Crie um catálogo de máquinas MCS com um conjunto de criptografia de disco (DES) diferente do DES da imagem mestre.
- Altere o tipo de criptografia de disco de uma chave DES para outra chave DES de um catálogo de máquinas MCS existente e VMs existentes.
- Atualize um catálogo de máquinas MCS e uma VM que não estavam habilitados para CMEK anteriormente para ter criptografia de chave de criptografia gerenciada pelo cliente (CMEK) (DES), criptografia de disco no host ou criptografia dupla.
- Atualize um catálogo de máquinas MCS e uma VM existentes para não serem criptografados, se foram criptografados anteriormente.
- Habilitar a criptografia de disco com ponto de extremidade privado (um catálogo de máquinas MCS que usou uma conexão de host habilitada com ProxyHypervisorTrafficThroughConnector).

Para obter mais informações, consulte Alterar a criptografia de disco.

Suporte para modificar as configurações do arquivo de paginação

Com este recurso, você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas a um catálogo existente sem atualizar a imagem mestre. Atualmente, este recurso é aplicável apenas a ambientes Azure.

Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell. Para obter mais informações sobre como modificar as configurações do arquivo de paginação, consulte Modificar configurações do arquivo de paginação.

MCS cria discos de ID com tipo de volume GP3 no ambiente AWS

Anteriormente, em ambientes AWS, os discos de identidade (ID) das VMs eram do tipo de volume GP2. Com este recurso, o MCS agora pode provisionar VMs com discos de identidade do tipo de

volume GP3. Como o tipo de volume GP3 é a opção mais barata oferecida pela AWS, este recurso minimiza custos.

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

Suporte para capturar propriedades adicionais usando a origem do perfil da máquina no AWS

Em ambientes AWS, com este aprimoramento, agora você pode criar ou atualizar um catálogo baseado em perfil de máquina para incluir o seguinte:

- Capturar opções de CPU, tipo de locação e capacidade de hibernação da origem do perfil da máquina ao criar um catálogo de máquinas MCS.
- Alterar o tipo de locação da origem do perfil da máquina ao editar um catálogo de máquinas MCS. Esta funcionalidade é aplicável às novas VMs adicionadas ao catálogo.
- Alterar a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS. Esta funcionalidade é aplicável às novas VMs adicionadas ao catálogo.

A origem do perfil da máquina pode ser uma VM ou uma versão de modelo de inicialização. Este recurso é aplicável a catálogos persistentes e não persistentes.

Para mais informações, consulte Criar um catálogo usando um perfil de máquina.

Suporte para criptografar o disco de ID de VMs de catálogo de máquinas MCS na AWS

Anteriormente, em ambientes AWS, o MCS permitia a criptografia apenas do disco do SO das VMs provisionadas. Com este recurso, agora você pode criptografar o disco de ID, além do disco do SO. Essa funcionalidade permite que você use chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) para realizar operações criptográficas nos discos anexados a uma VM.

Para criptografia de discos de SO e ID, configure uma das seguintes opções:

- Use uma imagem mestre criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz criptografado com chave KMS)
- Use uma origem de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz criptografado.

Para obter mais informações, consulte Criptografar discos de SO e ID.

Validar permissões na conexão do host na AWS

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

Suporte para herdar rótulos de uma origem de perfil de máquina para as VMs e discos no GCP

Com este recurso, as VMs e discos do catálogo de máquinas MCS (Disco de Identidade, Disco de Retorno de Cache de Gravação e disco do SO) agora podem herdar os rótulos de uma origem de perfil de máquina (instância de VM do GCP ou modelo de instância). Você pode usar os rótulos para distinguir instâncias pertencentes a diferentes equipes (por exemplo, team:research e team:analytics) e usá-los ainda mais para contabilidade de custos ou orçamento. Para obter mais informações sobre rótulos, consulte o documento do GCP Organize resources using labels.

Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Você pode criar um novo catálogo de máquinas MCS, atualizar um catálogo existente e atualizar VMs existentes para herdar os rótulos de uma origem de perfil de máquina.

Para obter informações, consulte VMs e discos com rótulos herdados.

Criar catálogos do Citrix Provisioning usando comandos PowerShell do MCS no XenServer®

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

Suporte para herdar tags personalizadas do perfil de máquina para as VMs provisionadas

Agora você pode adicionar as tags personalizadas de uma VM SCVMM às VMs provisionadas pelo MCS, juntamente com a tag padrão CitrixProvisioningSchemeId. Para adicionar as tags personalizadas às VMs provisionadas, você deve usar a VM SCVMM como um perfil de máquina

ao criar ou atualizar um catálogo de máquinas MCS. Se você remover uma VM de um catálogo, apenas a CitrixProvisioningSchemeId será removida da tag. As tags personalizadas não são excluídas da VM. Este recurso se aplica a um novo catálogo de máquinas MCS e a novas VMs adicionadas a um catálogo existente. Para obter mais informações, consulte Criar um catálogo com um perfil de máquina.

Validar a configuração antes de criar um catálogo de máquinas MCS

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

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

Reparar as informações de identidade de contas de computador ativas na AWS, GCP e XenServer

Em ambientes AWS, GCP e XenServer, agora você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes. Atualmente, o recurso é suportado apenas para ambientes de virtualização AWS, Azure, GCP, VMware e XenServer. Para obter mais informações, consulte Reparar as informações de identidade de contas de computador ativas.

Suporte para atribuir uma letra de unidade específica ao disco de cache de write-back de E/S do MCS

Anteriormente, o sistema operacional Windows atribuía automaticamente uma letra de unidade ao disco de cache de write-back de E/S do MCS. Com este recurso, agora você pode atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS. Esta implementação ajuda a evitar conflitos entre a letra de unidade de quaisquer aplicativos que você usa e a letra de unidade do disco de cache de write-back de E/S do MCS. Este recurso é aplicável apenas ao sistema operacional Windows. Para obter mais informações, consulte Atribuir uma letra de unidade específica ao disco de cache de write-back de E/S do MCS.

Gerenciamento de Perfis

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Linux VDA

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Gravação de Sessão

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Workspace Environment Management™

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Citrix Provisioning

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Federated Authentication Service

Para obter informações sobre novos recursos, consulte o artigo Novidades em seu próprio documento.

Problemas corrigidos

O Citrix Virtual Apps and Desktops™ 7 2407 inclui os seguintes problemas corrigidos:

Gráficos

- Você pode encontrar interrupções intermitentes na tela com duração de aproximadamente 10 segundos enquanto trabalha, durante as quais o processo gráfico do software Citrix (`Ctxgfx.exe`) é redefinido. O thread `twencode` experimenta uma exceção de violação de acesso, o que faz com que `ctxExceptionHandler` registre minidumps e cause este

problema. `ctxExceptionHandler` está configurado para gerar despejos completos para exame.

Machine Creation Services™

- Ao atualizar um site Multi-Delivery Controller de algumas versões LTSR pré-2402 (incluindo as versões 2302, 2305, 2308, 2311) para a LTSR 2402, as ações de energia em uma VM podem falhar se o site for apenas parcialmente atualizado. Para obter mais informações, consulte CTX666299.

VDA para SO de sessão única

Área de transferência

- Ao usar o VDA 2203 LTSR Cu4 e copiar e colar conteúdo no formato WebP, `WfShell` para de funcionar.
- A opção de copiar para a área de transferência no aplicativo remoto publicado não está funcionando para as versões CU3 e CU4.
- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA de Servidor, onde o consumo de memória atinge até 100%.

Sessão/Conexão

- O aplicativo OpenTEXT ETX falha ao abrir devido a violação de acesso com o seguinte módulo:

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

Cartões Inteligentes

- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA de Servidor, onde o consumo de memória atinge até 100%.

VDA para SO multissessão

Área de Transferência

- Ao usar o VDA 2203 LTSR Cu4 e copiar e colar conteúdo no formato WebP, `WfShell` para de funcionar.
- A opção de copiar para a área de transferência no aplicativo remoto publicado não está funcionando para as versões CU3 e CU4.

- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA de Servidor, onde o consumo de memória atinge até 100%.

Sessão/Conexão

- O aplicativo OpenTEXT ETX falha ao abrir devido a violação de acesso com o seguinte módulo:

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

Cartões Inteligentes

- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA de Servidor, onde o consumo de memória atinge até 100%.

Problemas conhecidos

O Citrix Virtual Apps and Desktops™ 7 2407 inclui os seguintes problemas conhecidos:

Observações

- Se um problema conhecido tiver uma solução alternativa, ela será fornecida após a descrição do problema.
- O seguinte aviso se aplica a qualquer solução alternativa que sugira a alteração de uma entrada de registro:

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Geral

- Quando o metainstalador é usado para instalar os componentes do Citrix Virtual Apps and Desktops em uma máquina executando o Windows Server 2025, os eventos `MsiInstall` não são gravados nos logs de eventos.

- Se você iniciar a barra de aplicativos e, em seguida, abrir o menu Connection Center no aplicativo Citrix Workspace™ para Windows, a barra de aplicativos não aparecerá sob o servidor que a hospeda.
- Se você usar o aplicativo Citrix Workspace para Windows e iniciar a barra de aplicativos em uma posição vertical, a barra cobrirá o menu Iniciar ou a bandeja do relógio do sistema.
- A caixa de combinação pode não ser exibida corretamente quando um usuário seleciona uma caixa de combinação que já está em foco no host. Como solução alternativa, selecione outro elemento da interface do usuário e, em seguida, selecione a caixa de combinação.
- O Serviço de Área de Trabalho Citrix pode falhar ao iniciar após a realização de uma atualização in-loco do sistema operacional do Windows 10 para o Windows 11. Para resolver o problema, reinicie a máquina.
- As configurações de **limites de sessão** para VDAs multissessão são recusadas em hosts de sessão executando Windows Server 2022, Windows 10 Enterprise multissessão e Windows 11 Enterprise multissessão. Como solução alternativa, você pode configurar os **limites de tempo de sessão RDS** por meio de GPO.
- A caixa de diálogo de Segurança do Windows associada ao FIDO2 não será exibida na frente da janela da sessão ICA® se você estiver executando o aplicativo com privilégios de administrador. É por design do sistema operacional que a caixa de diálogo de Segurança do Windows ficará oculta atrás da janela da sessão ICA se estiver sendo executada como um processo elevado.
- A cópia e colagem da área de transferência pode falhar para dados maiores que 100 MB do cliente para a sessão ICA. Cópias de buffer grandes não são suportadas.
- O Windows 10 ou Windows 11 Multi-session OS não oferece suporte à Restauração do Sistema do Windows. Consequentemente, a opção de criar um ponto de restauração não está disponível na interface do usuário. As opções de linha de comando `/EnableRestore` ou `/EnableRestoreCleanup` são ignoradas e a mensagem "**Desabilitando a Restauração do Sistema** não é atualmente suportada em sistemas operacionais multissessão do Windows 10/11" é registrada.
- A Citrix assina binários gerados pela Citrix e de terceiros. Isso significa que os binários são autenticados pela Citrix. As versões dos binários de terceiros permanecem as mesmas, pois são adquiridas de terceiros. Se um binário já estiver instalado, uma atualização do VDA não instalará os binários porque as versões correspondem. Para evitar essa limitação:

  a. Inclua os binários em uma **lista de permissões**. Isso elimina a necessidade de assinar os binários.

b. Desinstale o VDA antigo e instale o novo VDA. Isso se assemelha a uma nova instalação do VDA e as versões assinadas são aplicadas.

- Em alguns cenários, ao usar o filtro de política de IP do Cliente, o endereço IP usado para avaliar a política está incorreto.
- Ao usar o pass-through de domínio aprimorado para logon único, o SSO na sessão pode falhar se o dispositivo cliente ou o host da sessão estiver executando o Windows 11.
- Os dados da política podem ser perdidos quando o site é atualizado com configurações de política inválidas. Se você encontrar esse problema, abra um caso de suporte técnico usando o portal de Suporte da Citrix.
- Ao instalar o Citrix Rendezvous V2 usando os pacotes VDAWorkstationSetup_2402, VDAServerSetup_2402 ou VDAWorkstationCoreSetup_2402, a instalação pode falhar porque o arquivo Citrix.Diagnostics.Tracing.dll está ausente nesses pacotes. Como solução alternativa:
  - Instale o Citrix Rendezvous V2 do pacote completo CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR ou do Citrix_Virtual_Apps_and_Desktops_7_2402_LTSR.iso.
  - Alternativamente, substitua o arquivo Citrix.Diagnostics.Tracing.dll ausente. Para substituir o arquivo:
    a. Copie o arquivo Citrix.Diagnostics.Tracing.dll do pacote CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR ou do ISO na pasta “x64\XenDesktop Setup”.
    b. Crie uma pasta temporária. Por exemplo: “C:\Workaround” .
    c. Extraia o pacote do instalador mínimo para a pasta temporária executando o comando: VDAWorkstationSetup_2402.exe /extract "C:\Workaround" .
    d. Copie o arquivo Citrix.Diagnostics.Tracing.dll para a pasta "C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup”.
    e. Inicie a instalação do VDA executando o comando: "C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVdaSetup.exe”
- Há um atraso de 5 minutos entre a atualização de qualquer configuração de política e a geração do blob no serviço do site. Como resultado, as políticas podem levar algum tempo para serem atualizadas e refletidas nas sessões.

Áudio

Para alguns aplicativos de terceiros (por exemplo, aplicativo Zoom ou aplicativo Teams) em execução em um VDA de sessão única, os nomes dos dispositivos de áudio não são atualizados corretamente nos aplicativos de terceiros após uma desconexão, reconexão ou redefinição forçada da sessão ICA.

Como solução alternativa, você pode reiniciar o aplicativo de terceiros e os nomes dos dispositivos de áudio serão atualizados conforme o esperado.

Web Studio

Ao editar um catálogo no Web Studio para Google Cloud usando CMEK para discos, pular etapas no assistente pode causar falha em casos futuros de adição de máquinas. Para evitar esse problema, conclua o assistente inteiro sem pular nenhuma etapa ou use o SDK do PowerShell para realizar a operação.

Secure Private Access com Web Studio

- A barra de navegação fica parcialmente visível quando um usuário é redirecionado da guia Visão Geral > link "Adicionar URL do servidor de licenças" para a página Configurações > Integrações. Atualize a página para ver a barra de navegação.
- Um pop-up de aviso em branco aparece quando uma URL de gateway incorreta é inserida. Passe o mouse sobre o ícone de aviso para ver a mensagem de aviso.
- Ao realizar uma integração do Dia 0 e tentar configurar um banco de dados, o texto dentro do pop-up de aviso não é exibido após a mudança do modo manual para o modo automático. Passe o mouse sobre o ícone de aviso para ver a mensagem.
- A barra de rolagem vertical fica parcialmente visível para todas as guias no console. Nenhuma solução alternativa é necessária para este problema, e ele não afeta nenhum recurso ou experiência do usuário.
- Na guia **Configurações > Integrações**, a barra de rolagem horizontal não fica visível na parte inferior da página se a janela do navegador for pequena. A barra de rolagem horizontal não é necessária se a janela do navegador estiver maximizada.
- Nos logs de **Solução de problemas**, a barra de rolagem vertical não fica visível na parte inferior da página quando a caixa de diálogo de detalhes do log é aberta. Nenhuma solução alternativa é necessária para este problema, e ele não afeta nenhum recurso ou experiência do usuário.
- A guia **Visão Geral** não é destacada ao fazer login no console do Secure Private Access ou ao navegar de volta para o WS e retornar ao console do Secure Private Access. Nenhuma

solução alternativa é necessária para este problema, e ele não afeta nenhum recurso ou experiência do usuário.

- Na guia **Configurações > Integrações**, as mensagens de erro aparecem atrás da caixa de diálogo em vez de na frente dela. Nenhuma solução alternativa é necessária para este problema, e ele não afeta nenhum recurso ou experiência do usuário.

Observação:

Todos os problemas acima ocorrem apenas quando você acessa o Secure Private Access a partir do Web Studio. Eles não são aplicáveis se você acessar o Secure Private Access autônomo.

Gráficos

- Se você iniciar uma pré-visualização de vídeo usando um aplicativo de webcam de 64 bits com compactação Theora, a sessão poderá travar.
- Você pode notar webcams extras conectadas à área de trabalho remota no aplicativo Skype para desktop. A visualização dessas webcams extras é bloqueada e pode mostrar uma tela preta por motivos de segurança. Você pode ignorar a webcam extra e continuar usando a webcam para o endpoint.

Machine Creation Services™

- Em um ambiente VMware hospedado na AWS, a criação do catálogo de máquinas MCS falha se a imagem mestre estiver com vTPM ativado. Esse problema afeta todas as versões do Citrix Virtual Apps and Desktops e é devido a um problema no ambiente VMware. Para obter assistência, entre em contato com o suporte VMware.

Impressão

- As impressoras do Universal Print Server selecionadas na área de trabalho virtual não aparecem na janela **Dispositivos e Impressoras** no painel de controle. No entanto, quando os usuários estão trabalhando em aplicativos, eles podem usar essas impressoras. Esse problema ocorre apenas no Windows 10. Para obter mais informações, consulte CTX213540.
- A impressora padrão pode não estar marcada corretamente na janela de diálogo de impressão. Esse problema não afeta os trabalhos de impressão enviados para a impressora padrão.
- Alguns trabalhos de impressão de impressoras de rede com balanceamento de carga podem falhar quando as conexões SSL para os Universal Print Servers estão ativadas. Isso ocorre quando os trabalhos de impressão são disparados rapidamente, um após o outro.

- A Microsoft confirma que há um problema em manter as configurações de impressão entre os trabalhos de impressão ao usar a caixa de diálogo de impressão moderna, e eles estão trabalhando para resolvê-lo. A projeção atual é o primeiro semestre de 2025. A caixa de diálogo de impressão moderna é ativada por padrão em versões mais recentes do sistema operacional, como Windows 11 e Windows Server 2025. O sistema operacional pode ser configurado para usar a caixa de diálogo de impressão herdada realizando a seguinte ação:

1. Abra o Editor do Registro
2. Vá para HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog
3. Clique com o botão direito e selecione Novo > Valor DWORD (32 bits)
4. Renomeie o valor como PreferLegacyPrintDialog
5. Clique com o botão direito em PreferLegacyPrintDialog e selecione Modificar
6. Defina os dados do valor como 1 e clique em OK

Problemas de terceiros

- O Chrome oferece suporte à Automação de UI apenas para barras de ferramentas, guias, menus e botões em torno de uma página da web. Devido a esse problema do Chrome, o recurso de exibição automática do teclado pode não funcionar em um navegador Chrome em dispositivos de toque. Como solução alternativa, execute `chrome --force-renderer-accessibility` ou você pode abrir uma nova guia do navegador, digitar `chrome://accessibility` e habilitar o suporte à **API de acessibilidade nativa** para páginas específicas ou todas as páginas. Além disso, ao publicar um aplicativo contínuo, você pode publicar o Chrome com a opção `--force-renderer-accessibility`.
- Você pode ver uma tela preta ao iniciar uma sessão se tiver o FSLogix 2201 HF1 instalado no host da sessão. Para resolver esse problema, você deve atualizar o FSLogix para uma versão mais recente.

Gerenciamento de Perfis

- Documentação do Profile Management 2407 fornece informações específicas sobre as atualizações nesta versão.

Linux VDA

- Documentação do Linux VDA 2407 fornece informações específicas sobre as atualizações nesta versão.

Gravação de Sessão

- Documentação do Session Recording 2407 fornece informações específicas sobre as atualizações nesta versão.

Workspace Environment Management™

- Documentação do Workspace Environment Management 2407 fornece informações específicas sobre as atualizações nesta versão.

Citrix Provisioning™

- Documentação do Citrix Provisioning 2407 fornece informações específicas sobre as atualizações nesta versão.

Federated Authentication Service

- Documentação do Federated Authentication Service 2407 fornece informações específicas sobre as atualizações nesta versão.

Descontinuação

Os anúncios neste artigo têm como objetivo fornecer um aviso antecipado sobre plataformas, produtos Citrix e recursos que estão sendo descontinuados para que você possa tomar decisões de negócios oportunas. A Citrix monitora o uso e o feedback dos clientes para determinar quando eles serão retirados. Os anúncios podem mudar em versões subsequentes e podem não incluir todos os recursos ou funcionalidades descontinuados. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo Política de Suporte ao Ciclo de Vida do Produto. Para obter informações sobre a opção de serviço Long Term Service Release (LTSR), consulte `<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549>`.

Descontinuações e remoções

A tabela a seguir mostra as plataformas, produtos Citrix® e recursos que foram descontinuados ou removidos. As datas em **negrito** indicam alterações nesta versão.

Descontinuações

Descontinuação significa que pretendemos remover o recurso ou a capacidade de uma versão futura. O recurso ou a capacidade continuará funcionando e será totalmente suportado até ser oficialmente removido. Esta notificação de descontinuação pode durar alguns meses ou anos.

Após a remoção, o recurso ou a capacidade não funcionará mais. Este aviso serve para lhe dar tempo suficiente para planejar e atualizar seu código antes que o recurso ou a capacidade seja removido. Alternativas para itens descontinuados são sugeridas sempre que possível.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	ALTERNATIVA
Ganchos de múltiplos monitores	2407	-
Autenticação de passagem de domínio	2407	Use autenticação de passagem de domínio aprimorada para logon único.
Rendezvous V1	2402	Use o Rendezvous V2.
Secure ICA®	2402	-
Suporte a VDA no Windows Server 2016	2402	Atualize para as versões mais recentes do Windows Server.
Suporte para Delivery Controller™, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI para SO de sessão única, VDA para SO de múltiplas sessões, floresta e domínio do Active Directory e Universal Print Server no Windows Server 2016	2402	Atualize para a versão mais recente do Windows Server.
Suporte para as versões 2016 e 2017 do Microsoft SQL Server para os bancos de dados de configuração do site, registro de configuração e monitoramento	2402	Atualize para a versão mais recente do Microsoft SQL Server.
Suporte para configurar o cache de write-back para incluir apenas um cache de	2402	Use a opção de configuração de tamanho do cache de

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	ALTERNATIVA
disco e nenhum cache de memória		memória e aloque um tamanho diferente de zero.
Suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos "legados")	2402	Recrie VMs de catálogo herdadas do Azure. Os catálogos são provisionados sob demanda e, assim, economizam custos de armazenamento.
A política de **Taxa de Quadros Mínima Alvo**	2311	Use o **Indicador de Status Gráfico** para modificar a taxa de quadros mínima alvo.
Suporte para Citrix Connector 3.1 para System Center Configuration Manager	2311	Faça a atualização da imagem ou do aplicativo manualmente.
Suporte para usar uma imagem mestre em uma região diferente da região onde o catálogo é criado	2311	Use a Galeria de Computação do Azure para replicar a imagem mestre para a região desejada.
Configuração do Limite de Memória de Exibição Gráfica HDX	2311	A quantidade mínima de memória necessária é alocada para garantir que o layout de exibição do cliente seja totalmente acomodado.
Suporte ao modo progressivo em HDX Graphics	2311	Use Thinwire. Consulte Modo progressivo.
Suporte para redirecionamento de conteúdo do navegador no Internet Explorer 11	2311	Use o redirecionamento de conteúdo do navegador baseado no Google Chrome.
Removido o suporte para o worker de volume AWS	2311	Use o upload e download direto de disco. Consulte

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	ALTERNATIVA
		Upload e download direto de disco.
Suporte para SQL Server 2016 no Broker	2308	Use as versões mais recentes. Para obter mais informações, consulte Requisitos do sistema.
Suporte para XenApp 5.x no Director	2308	---
Suporte para XenApp 6.x no Director	2308	---
SCOM Pack para alertas no Director	2308	---
Suporte para plug-in no Director	2308	---
Suporte para o formato WebRTC SDP (Plano B)	2308	Atualize o Citrix Workspace™ App para uma versão compatível.
Suporte para o modo de Janela Única na Otimização do Microsoft Teams	2308	Atualize o Citrix Workspace App para uma versão que suporte o modo MultiWindow. Para obter mais informações, consulte Matriz de recursos e suporte de versão.
Suporte para `AwsCaptureInstanceProperties` usado em ambientes AWS	2308	Use um perfil de máquina. Consulte Criar um catálogo usando um perfil de máquina.
`Schedule-ProvVMUpdate` comando PowerShell	2305	Use `Set-ProvVMUpdateTimeWindow`.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	ALTERNATIVA
`Request-ProvVMUpdate` comando PowerShell	2305	Use `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.
`Cancel-ProvVMUpdate` comando PowerShell	2305	Use `Clear-ProvVMUpdateTimeWindow`.
Parâmetro `DedicatedTenancy` usado no comando `New-ProvScheme`	2303	Use o parâmetro `TenancyType`.
License Server VPX	2206	---
Disco não gerenciado para provisionar VMs em ambientes Azure.	2206	Use discos gerenciados.
Redirecionamento de Host para Cliente (URL)	2203	Redirecionamento de conteúdo bidirecional.
Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress` usados em ambientes de nuvem e locais.	2203	---
Citrix Files for Windows e Citrix Files for Outlook do metainstalador do VDA.	2203	Use os instaladores autônomos.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	ALTERNATIVA
Componente do Agente WEM do metainstalador do VDA.	2203	---
Opção Wake on LAN integrada ao SCCM para Acesso Remoto a PC.	2012	Use o recurso Wake on LAN autônomo.
Citrix SCOM Management Packs para XenApp e XenDesktop, Provisioning Services e StoreFront. Para as versões de produto que podem ser monitoradas, consulte a documentação do Citrix SCOM Management Packs.	1912	Use o Director para monitorar e gerenciar sua implantação. Para obter mais informações sobre o EOL do SCOM e alternativas, consulte https://support.citrix.com/article/CTX266943.
Mobility SDK / Mobile SDK (do antigo Citrix Labs)	7.16	Substituído pelas configurações de política de experiência móvel e experiências nativas para desktops/aplicativos hospedados.

Remoções

Os itens removidos são removidos ou não são mais suportados no Citrix Virtual Apps and Desktops.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte para o assistente de importação PVS no Citrix Studio	1912 LTSR	2311	Provisionar máquinas Citrix Provisioning™ usando uma

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			das seguintes formas • Provisione máquinas usando o Citrix Provisioning Console e exporte-as para o Citrix Virtual Apps and Desktops usando o Assistente de Exportação de Dispositivos do Citrix Provisioning. Consulte Assistente de Exportação de Dispositivos para obter mais detalhes.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			• Crie catálogos do Citrix Provisioning usando o Web Studio. Consulte Criar catálogos do Citrix Provisioning no Citrix Studio para obter mais detalhes.
Citrix Workspace app para Windows 1912	---	2402	Use as versões mais recentes.
Otimização de gráficos HDX em tela cheia + texto	2311	2311	
Suporte para NVIDIA Frame Buffer Capture (NVFBC) com HDX 3D Pro	2308	2311	Use a API de Duplicação de Área de Trabalho (DDAPI).
Suporte VDA para a configuração de	7.16	2311	Nenhum. Configuração de política

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
política "Instalação automática de drivers de impressora incluídos".			suportada apenas com VDAs em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores).
Codificação de hardware de GPU NVIDIA (NVENC) com: vGPU 11 e anteriores, e versão de driver 466.77 e anteriores.	2305	2305	Use drivers NVIDIA atualmente suportados: vGPU 13 ou mais recente, versão 471.41 ou mais recente.
Ferramentas de Suporte Citrix (SupportabilityTool_x64 .msi) do Meta-Instalador VDA.	---	2212	---
Console de Administração de Licenças Citrix (última vez incluído no Windows License Server 11.16.3 build 30000 e removido no Windows	2003	2006	Use o Citrix Licensing Manager.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
License Server v11.16.6 build 31000).			
Suporte ao adaptador gráfico Citrix Indirect Display Driver (IDD) no Windows 10 versão 1709 e anteriores.	2003	2003	Use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR.
Codificação de hardware com GPUs NVIDIA (NVENC) usando drivers de vídeo GRID 9 ou anteriores.	2003	2003	Use drivers de vídeo GRID 10 com VDAs do Citrix Virtual Apps and Desktops 7 2003 ou posterior, ou use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR.
Recurso de Redefinição de Senha de Autoatendimento (SSPR).	2003	2006	---
Suporte para versões do Microsoft .NET Framework anteriores à versão 4.8 para	1912	2003	Atualize para a versão 4.8 do .NET Framework.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
VDAs e componentes principais do servidor. Inclui Delivery Controller, Studio, Director.			
VDAs no Windows Server 2012 R2.	1912	2003	Instale VDAs em um sistema operacional compatível.
Componente de migração de aplicativos AppDNA® da edição Citrix Virtual Apps and Desktops Premium.	1909	2003	---
Instalação do Studio em máquinas de 32 bits (x86).	1909	2003	Instale em um sistema operacional x64 compatível.
Suporte para o gancho do Excel em aplicativos contínuos. Isso era usado para criar ícones separados na barra de tarefas para cada pasta de trabalho do	1909	1909	---

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Microsoft Excel 2010.			
Componentes principais do servidor no Windows Server 2012 R2 (incluindo Service Packs). Inclui: Delivery Controller, Studio e Director.	1906	2003	Instale em um sistema operacional compatível mais recente.
Suporte para bancos de dados de Configuração do Site, Registro de Configuração e Monitoramento nas versões do Microsoft SQL Server 2008 R2, 2012 e 2014 (incluindo todos os Service Packs e edições).	1906	2003	Instale bancos de dados em uma versão compatível do Microsoft SQL Server.
Suporte para VDAs no Windows 10 em plataformas x86.	1906	1909*	Instale VDAs em um sistema operacional x64 compatível. *Este recurso ainda é suportado no

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			Citrix Virtual Apps and Desktops 7 1912 LTSR.
Remoção do Citrix Smart Tools Agent da mídia de instalação do Citrix Virtual Apps and Desktops.	1903	1906	---
Suporte para Linux VDA no Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Instale o Linux VDA em uma versão posterior do Red Hat Enterprise Linux.
Suporte do StoreFront para os protocolos TLS 1.0 e TLS 1.1 entre o Citrix Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) e o Citrix Receiver, e o Workspace Hub.	7.17	2203	Atualize os Citrix Receivers para um aplicativo Citrix Workspace que suporte o protocolo TLS 1.2. Para obter mais informações sobre o aplicativo Citrix Workspace, consulte https://docs.citrix.com/pt-br/citrix-workspace-app.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte de VDA para a configuração de política "Instalação automática de drivers de impressora incluídos".	7.16	2311	Nenhum. Configuração de política suportada apenas com VDAs em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores).
Suporte para a tecnologia de acesso remoto de exibição Framehawk	1811	1903	Use Thinwire com transporte adaptável ativado.
Suporte para Citrix Smart Scale em todas as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Esta funcionalidade atingirá o Fim da Vida em 31 May 2019.	1808	1906	Considere usar o Virtual Apps and Desktops Service no Citrix Cloud para uma funcionalidade aprimorada de gerenciamento de energia.
Suporte para as versões 4.5.1, 4.5.2, 4.6,	7.18	1808	Atualize para a versão 4.7.1 ou posterior

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
4.6.1, 4.6.2 e 4.7 do Microsoft .NET Framework pelo Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director e Citrix Delivery Controller.			do .NET Framework. (O instalador instala automaticamente o .NET Framework 4.7.1 se ainda não estiver instalado.)
Suporte para Linux VDA no Red Hat Enterprise Linux 7.3.	7.18	1808	Instale o Linux VDA em uma versão posterior do Red Hat Enterprise Linux.
Suporte para o Linux VDA no SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Instale o Linux VDA na versão SUSE compatível.
Suporte para o driver Citrix WDDM em VDAs	7.16	7.16	O driver Citrix WDDM não é mais instalado com VDAs.
VDAs no Windows 10 versão 1511 (Threshold 2) e versões anteriores do Windows Single-session	7.15 LTSR (e 7.12)	7.16	Instale VDAs de SO de sessão única no Windows 10 versão mínima 1607 (Redstone 1) ou em Canais Semi-

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
OS, incluindo Windows 8.x e Windows 7 (consulte `<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>`).			Anuais mais recentes. Se estiver usando 1607 LTSB, recomendamos um VDA 7.15. Consulte CTX224843.
VDAs no Windows Server 2008 R2 e Windows Server 2012 (incluindo Service Packs)	7.15 LTSR (e 7.12)	7.16	Instale VDAs em um sistema operacional compatível.
Redirecionamento de Composição da Área de Trabalho (anteriormente conhecido como DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Use Thinwire.
Componentes principais no Windows Server 2012 e	7.15 LTSR	7.18	Instale os componentes em um sistema

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Windows Server 2008 R2 (incluindo Service Packs). Inclui: Delivery Controller, Studio, Director, StoreFront, License Server e Universal Print Server.			operacional compatível.
Recurso de Redefinição de Senha de Autoatendimento (SSPR) no Windows Server 2012 e Windows Server 2008 R2 (incluindo Service Packs)	7.15 LTSR	7.18	Instale em um sistema operacional mais recente e compatível.
Studio no Windows 7, Windows 8 e Windows 8.1 (incluindo Service Packs)	7.15 LTSR	7.18	Instale o Studio em um sistema operacional compatível.
Redirecionamento de Flash	7.15 LTSR	1912	Crie conteúdo de vídeo como Vídeo HTML5. Use a Redireção de Vídeo HTML5 para conteúdo gerenciado e a

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			Redireção de Conteúdo do Navegador para sites públicos. Para obter mais informações, consulte a nota Fim da Vida Útil da Redireção Flash.
Integração Citrix Online (produto Goto) com StoreFront	7.14 (e StoreFront 3.11)	StoreFront 3.12	---
A conta de usuário, CtxAppVCOMAdmin, que foi criada durante a instalação do VDA e adicionada ao Grupo de Administradores Locais na máquina VDA, não é mais criada. O mecanismo "COM" subjacente também foi removido.	7.14	7.14	O serviço Windows CtxAppVService executa a mesma função. Ele é instalado e configurado automaticamente e não requer interação do usuário.
Suporte ao componente UpsServer do	7.14	7.14	Instale em um sistema operacional

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Universal Print Server no Windows Server 2008 de 32 bits			mais recente e compatível.
StoreFront e Receiver para Web no Internet Explorer 8	7.13	7.13	---
Opção de instalação de linha de comando do VDA /no_appv para evitar a instalação dos componentes Citrix App-V	7.13	7.13	Use a opção de instalação de linha de comando / exclude "Citrix Personalization for App-V – VDA".
O instalador completo do produto não instala mais o snap-in Citrix.Common.Commands em novas instalações e o remove automaticamente ao atualizar instalações existentes.	7.13	7.13	Alguns comandos PowerShell que foram fornecidos pelo snap-in Citrix.Common.Commands ainda estão disponíveis no SDK do XenApp 6.5.
Funcionalidade parcial para manipular	7.13	7.13	Agora fornecido pelos cmdlets *-

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
dados de ícones que foi fornecida pelos cmdlets *-CtxIcon.			BrokerIcon no Serviço Broker.
Modo Thinwire herdado	7.12	7.16	Use Thinwire. Se você estiver usando o modo Thinwire Herdado no Windows Server 2008 R2, migre para o Windows Server 2012 R2 ou Windows Server 2016 e use o Thinwire.
Atualizações in-loco do StoreFront 2.0, 2.1, 2.5 e 2.5.2	7.13	7.16	Atualize de uma dessas versões para uma versão posterior suportada e, em seguida, para o XenApp e XenDesktop 7.16.
Atualizações in-place do XenDesktop 5.6 ou 5.6 FP1	7.12	7.16	Migre sua implantação do XenDesktop 5.6 ou 5.6 FP1 para a versão atual do XenDesktop. Para fazer isso, primeiro atualize para o

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			XenDesktop 7.6 LTSR (com o CU mais recente) e, em seguida, atualize para a versão mais recente do Citrix Virtual Desktops (anteriormente XenDesktop) ou versão LTSR.
Instalando o Delivery Controller, Director, StoreFront ou License Server em máquinas de 32 bits (x86).	7.12	7.16	Instale em um sistema operacional x64 compatível.
Concessão de conexão	7.12	7.16	Use Cache de Host Local.
XenDesktop 5.6 usado no Windows XP. As instalações do VDA no Windows XP não são suportadas.	7.12	7.16	Instale VDAs em um sistema operacional compatível.
Suporte para conexões CloudPlatform	7.12	2003	Use um hipervisor ou serviço de nuvem

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			compatível diferente.
Suporte para conexões Azure Classic (também conhecido como Azure Service Management)	7.12	2003	Considere usar o serviço Virtual Apps and Desktops no Citrix Cloud.
Funcionalidade AppDisks (e a integração do AppDNA no Studio, que a suporta)	7.13	2003	Use o Citrix App Layering.
Funcionalidade Personal vDisk	7.15	2006†	Use a tecnologia Citrix App Layering user layer ou user personalization layer.

† No Citrix Virtual Apps and Desktops 7 2003, o driver Personal vDisk foi removido do instalador do VDA. No Citrix Virtual Apps and Desktops 7 2006, o fluxo de trabalho do driver Personal vDisk foi removido do Studio.

Requisitos do sistema

Introdução

Os requisitos de sistema neste documento eram válidos quando esta versão do produto foi lançada. As atualizações são feitas periodicamente. Os requisitos de sistema para componentes não abordados aqui (como sistemas host, aplicativo Citrix Workspace™ e Citrix Provisioning™) são descritos em suas respectivas documentações.

Revise Preparar para instalar antes de iniciar uma instalação.

Salvo indicação em contrário, o instalador do componente implanta automaticamente os pré-requisitos de software (como pacotes .NET e C++) se as versões necessárias não forem detectadas na máquina. A mídia de instalação do Citrix® também contém parte desse software pré-requisito.

A mídia de instalação contém vários componentes de terceiros. Antes de usar o software Citrix, verifique se há atualizações de segurança do terceiro e instale-as.

Para componentes e recursos que podem ser instalados em Windows Servers, as instalações do Nano Server não são suportadas, a menos que indicado. O Server Core é suportado apenas para Delivery Controllers e Director.

Requisitos de hardware

Os valores de RAM e espaço em disco são adicionais aos requisitos para a imagem do produto, sistema operacional e outros softwares na máquina. Seu desempenho varia, dependendo da sua configuração. Sua configuração inclui os recursos que você usa, além do número de usuários e outros fatores. Usar apenas o mínimo pode resultar em desempenho lento.

A tabela a seguir lista os requisitos mínimos para os componentes principais.

COMPONENTE	MÍNIMO
Todos os componentes principais e StoreFront™ em um servidor, apenas para avaliação, não para implantação em produção	5 GB de RAM

COMPONENTE	MÍNIMO
Todos os componentes principais e StoreFront em um servidor, para uma implantação de teste ou um pequeno ambiente de produção	12 GB de RAM
Delivery Controller™ (mais espaço em disco necessário para o Local Host Cache)	5 GB de RAM, 800 MB de disco rígido
Studio	1 GB RAM, 100 MB de disco rígido
Director	2 GB RAM, 200 MB de disco rígido
StoreFront	2 GB RAM, consulte a documentação do StoreFront para recomendações de disco
License Server	8 GB RAM; consulte a documentação de Licenciamento para recomendações de disco

Dimensionamento de VMs que entregam desktops e aplicativos

Recomendações específicas não podem ser fornecidas devido à natureza complexa e dinâmica das ofertas de hardware, e cada implantação tem necessidades únicas. Geralmente, o dimensionamento de uma VM do Citrix Virtual Apps™ é baseado no hardware e não nas cargas de trabalho do usuário. A exceção é a RAM. Você precisa de mais RAM para aplicativos que consomem mais.

Para mais informações:

- Citrix Tech Zone contém orientações sobre dimensionamento.
- Citrix Virtual Apps and Desktops Single Server Scalability discute quantos usuários ou VMs podem ser suportados em um único host físico.

Microsoft Visual C++

Ao instalar um Delivery Controller, Virtual Delivery Agent (VDA) ou Universal Print Server, o instalador Citrix instala automaticamente o Microsoft Visual C++ 2015–2022 Redistributable.

- Se a máquina contiver uma versão anterior desse tempo de execução (como 2015-2019), o instalador Citrix a atualizará.

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

Delivery Controller

Sistemas operacionais suportados:

- Windows Server 2025
- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, Edições Standard e Datacenter, e com a opção Server Core

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Windows PowerShell 3.0, 4.0 ou 5.0.
- Microsoft Visual C++ 2015–2022 Redistributable.

Bancos de dados

Versões do Microsoft SQL Server compatíveis para a configuração do site, registro de configuração e bancos de dados de monitoramento:

- SQL Server 2022, Edições Express, Standard e Enterprise.
    - Para novas instalações: Por padrão, o SQL Server Express 2022 com a Atualização Cumulativa 14 é instalado ao instalar o Controller, se uma instalação existente e compatível do SQL Server não for detectada.
- SQL Server 2019, Edições Express, Standard e Enterprise.
- SQL Server 2017, Edições Express, Standard e Enterprise.
    - Para atualizações, nenhuma versão existente do SQL Server Express é atualizada.
- SQL Server 2016 SP2, Edições Express, Standard e Enterprise.

As seguintes soluções de alta disponibilidade de banco de dados são compatíveis (exceto para SQL Server Express, que suporta apenas o modo autônomo):

- Instâncias de Cluster de Failover SQL Server AlwaysOn

- Grupos de Disponibilidade SQL Server AlwaysOn (incluindo Grupos de Disponibilidade Básicos)
- Espelhamento de Banco de Dados do SQL Server

A autenticação do Windows é necessária para conexões entre o Controller e o banco de dados do site do SQL Server.

Considerações sobre o Cache do Host Local: O Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o Cache do Host Local usa de forma autônoma. O Cache do Host Local não requer nenhum componente do SQL Server Express além do SQL Server Express LocalDB.

- Ao instalar um Controller, o Microsoft SQL Server Express LocalDB 2022 com a Atualização Cumulativa 14 é instalado para uso com o recurso Cache do Host Local. (Esta instalação é separada da instalação padrão do SQL Server Express para o banco de dados do site.)
- Ao atualizar um Controller, a versão existente do Microsoft SQL Server Express LocalDB não é atualizada automaticamente. Para requisitos e procedimentos de substituição, consulte Substituir SQL Server Express LocalDB.

Mais informações sobre o banco de dados:

- Bancos de dados
- CTX114501 lista os bancos de dados mais atualmente suportados
- Orientação de dimensionamento do banco de dados
- Cache do Host Local

Web Studio

> **Observação:**
>
> - Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

- O Web Studio é um console de gerenciamento baseado na web que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. Ele foi projetado para uma experiência de usuário aprimorada e geralmente responde mais rápido do que o Citrix Studio, o console de gerenciamento baseado no Windows. Consulte Instalar o Web Studio.

Sistemas operacionais suportados:

- Windows Server 2025
- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, Edições Standard e Datacenter, e com a opção Server Core

Citrix Director

Sistemas operacionais suportados:

- Windows Server 2025
- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, Edições Standard e Datacenter, e com a opção Server Core

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Internet Information Services (IIS) 7.0 e ASP.NET 2.0. Certifique-se de que o serviço de função Conteúdo Estático esteja instalado na função de servidor IIS. Se este software ainda não estiver instalado, será solicitada a mídia de instalação do Windows Server. Em seguida, esse software será instalado para você.
- Para visualizar os logs de eventos em máquinas onde o Citrix Director está instalado, você deve instalar o Microsoft .NET Framework 2.0.

Citrix Profile Management:

- Certifique-se de que o Citrix Profile Management e o Citrix Profile Management WMI Plug-in estejam instalados no VDA (página **Componentes Adicionais** no assistente de instalação) e

que o Serviço Citrix Profile Management esteja em execução para visualizar os detalhes do perfil do usuário no Director.

Requisitos de integração do System Center Operations Manager (SCOM):

- System Center 2012 R2 Operations Manager

Navegadores suportados para visualização do Director:

- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

A resolução de tela ideal recomendada para visualização do Director é 1440 x 1024.

Agente de Entrega Virtual (VDA) para SO de sessão única

Sistemas operacionais suportados:

- Windows 11
- Windows 10 (somente x64), qualquer versão que esteja atualmente em suporte mainstream.
    - Para suporte a edições, consulte o artigo da Central de Conhecimento CTX224843.

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015–2022 Redistributable.

O Acesso Remoto a PC usa este VDA, que você instala em PCs físicos de escritório. Este VDA suporta Inicialização Segura para Citrix Virtual Desktops™ Acesso Remoto a PC no Windows 11 e Windows 10.

Vários recursos de aceleração multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado na máquina onde você instala o VDA. Se a máquina não tiver o Media Foundation instalado, os recursos de aceleração multimídia não serão instalados e não funcionarão. Não remova o Media Foundation da máquina após instalar o software Citrix. Caso contrário, os usuários não conseguirão fazer logon na máquina. Na maioria das edições de SO de sessão única do Windows suportadas, o suporte ao Media Foundation já está instalado e não pode ser removido. No entanto, as edições N não incluem certas tecnologias

relacionadas a mídia; você pode obter esse software da Microsoft ou de terceiros. Para obter mais informações, consulte Preparar para instalar.

Para obter informações sobre o VDA para Linux, consulte os artigos Linux Virtual Delivery Agent.

Para usar o recurso Server VDI, você pode usar a interface de linha de comando para instalar um VDA para SO de sessão única do Windows em uma máquina Windows Server suportada. Consulte Server VDI para obter orientação.

Para obter informações sobre como instalar um VDA em uma máquina Windows 7, consulte Sistemas operacionais anteriores.

Agente de Entrega Virtual (VDA) para SO de múltiplas sessões

Sistemas operacionais suportados:

- Windows Server 2025
- Windows 11 (suportado apenas com Citrix DaaS™)
- Windows 10 (somente x64; suportado apenas com Citrix DaaS), qualquer versão que esteja atualmente em suporte mainstream.
- Windows Server 2022
- Windows Server 2019, Standard e Datacenter Editions

O instalador implanta automaticamente os seguintes requisitos, que também estão disponíveis na mídia de instalação do Citrix nas pastas **Support**:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015–2022 Redistribuível.

O instalador instala e habilita automaticamente os serviços de função dos Serviços de Área de Trabalho Remota, se ainda não estiverem instalados e habilitados.

Vários recursos de aceleração multimídia (como Redirecionamento de Mídia do Windows HDX MediaStream) exigem que o Microsoft Media Foundation esteja instalado na máquina onde você instala o VDA. Se a máquina não tiver o Media Foundation instalado, os recursos de aceleração multimídia não serão instalados e não funcionarão. Não remova o Media Foundation da máquina após instalar o software Citrix; caso contrário, os usuários não conseguirão fazer logon na

máquina. Na maioria das versões do Windows Server, o recurso Media Foundation é instalado através do Gerenciador do Servidor. Para obter mais informações, consulte Preparar para instalar.

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

- Redirecionamento de Mídia do Windows
- Redirecionamento de Vídeo HTML5
- Redirecionamento de Webcam HDX™ RealTime

Para obter informações sobre o VDA para Linux, consulte os artigos Linux Virtual Delivery Agent.

Para obter informações sobre como instalar um VDA em uma máquina Windows Server 2008 R2, consulte Sistemas operacionais anteriores.

Hosts / recursos de virtualização

Os seguintes recursos de host/virtualização (listados em ordem alfabética) são suportados. Quando aplicável, as versões *principal.secundária* são suportadas, incluindo atualizações para essas versões. O artigo da Central de Conhecimento CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

Alguns recursos podem não ser suportados em todas as plataformas de host ou em todas as versões de plataforma. Consulte a documentação do recurso para obter detalhes.

O recurso Wake on LAN do Acesso Remoto para PC requer Microsoft System Center Configuration Manager mínimo 2012.

Hipervisores suportados:

- **XenServer (anteriormente Citrix Hypervisor™)**

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

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

  Inclui qualquer versão do Hyper-V que possa ser registrada nas versões compatíveis do System Center Virtual Machine Manager.

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

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

- **Nutanix Acropolis**

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

  Para obter mais informações, consulte ambientes de virtualização Nutanix.

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

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

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

  Para obter mais informações, consulte VMware virtualization environments.

Hosts de nuvem pública suportados:

- **Amazon Web Services (AWS)**

  Para obter informações sobre como usar o AWS para provisionar máquinas virtuais, consulte ambientes de virtualização do Amazon Web Services.

- **Google Cloud Platform** Para obter mais informações, consulte ambientes de virtualização do Google Cloud Platform e Introdução ao Citrix DaaS no Google Cloud.

- **Microsoft Azure Resource Manager**

  Para obter informações sobre como usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais, consulte Microsoft Azure Resource Manager virtualization environments.

- **Soluções de nuvem e parceiros Nutanix**

  Para obter informações sobre como usar soluções de nuvem e parceiros Nutanix, consulte Nutanix cloud and partner solutions.

- **Soluções de nuvem e parceiros VMware**

  Para obter informações sobre como usar soluções de nuvem e parceiros VMware, consulte VMware cloud and partner solutions.

Ao adicionar conexões de host de nuvem pública à sua implantação, considere o seguinte:

- Você precisa da Licença de Direitos Híbridos. Para obter informações sobre a Licença de Direitos Híbridos, consulte Transition and Trade-Up (TTU) with Hybrid Rights. Para obter informações sobre como adicionar uma licença, consulte Create a site.
- As fontes de informação direcionam você para a documentação do Citrix DaaS. Se você estiver familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local apresenta várias diferenças.
    - No Citrix DaaS, a interface de gerenciamento é conhecida como Configuração Completa. No Citrix Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio.
    - As atualizações são lançadas para o Citrix DaaS aproximadamente a cada quatro semanas. Assim, você pode descobrir que certos recursos disponíveis com o Citrix DaaS não estão disponíveis na versão local.

Níveis funcionais do Active Directory

Os seguintes níveis funcionais para a floresta e o domínio do Active Directory são suportados:

- Windows Server 2025
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

> **Observação:**
>
> Antes de atualizar o site do Citrix Virtual Apps and Desktops, revise os requisitos para recursos individuais, pois recursos mais recentes e VDAs podem precisar de níveis funcionais mínimos específicos do Active Directory.

HDX

Áudio

O áudio UDP para Multi-Stream ICA® é compatível com o aplicativo Citrix Workspace para Windows e o aplicativo Citrix Workspace para Linux 13.

O cancelamento de eco é suportado no aplicativo Citrix Workspace para Windows.

Consulte o suporte e os requisitos específicos dos recursos HDX. Para obter mais informações sobre os recursos HDX e os aplicativos Citrix Workspace, consulte a Matriz de recursos.

Entrega de mídia do Windows HDX

Os seguintes clientes são suportados para busca de conteúdo do lado do cliente do Windows Media, redirecionamento do Windows Media e transcodificação multimídia em tempo real do Windows Media: aplicativo Citrix Workspace para Windows, aplicativo Citrix Workspace para iOS e aplicativo Citrix Workspace para Linux.

Para usar a busca de conteúdo do lado do cliente do Windows Media em dispositivos Windows 8, defina o Citrix Multimedia Redirector como um programa padrão: em **Painel de Controle > Programas > Programas Padrão > Definir seus programas padrão**, selecione **Citrix Multimedia Redirector** e clique em **Definir este programa como padrão** ou **Escolher padrões para este programa**. A transcodificação de GPU requer uma GPU habilitada para NVIDIA CUDA com Capacidade de Computação 1.1 ou superior; consulte `<https://developer.nvidia.com/cuda/cuda-gpus>`.

HDX 3D Pro

O VDA para SO de sessão única do Windows detecta a presença de hardware de GPU em tempo de execução.

A máquina física ou virtual que hospeda o aplicativo pode usar GPU Passthrough ou GPU Virtual (vGPU):

- GPU Passthrough está disponível com:
  - XenServer®
  - Nutanix AHV
  - VMware vSphere e VMware ESX, onde é referido como Aceleração Gráfica Direta virtual (vDGA)

- vGPU está disponível com:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

Consulte `<https://docs.citrix.com/pt-br/citrix-virtual-apps-desktops/2407/graphics/hdx-3d-pro>`.

A Citrix recomenda que o computador host tenha pelo menos 4 GB de RAM e quatro CPUs virtuais com uma velocidade de clock de 2,3 GHz ou superior.

Unidade de Processamento Gráfico (GPU):

- Para aceleração gráfica virtualizada usando a API NVIDIA GRID, você pode usar o HDX 3D Pro com todas as GPUs NVIDIA GRID suportadas pelo software NVIDIA Virtual GPU (vGPU) versão 13 e superior, consulte `<https://docs.nvidia.com/grid/index.html>`. Para uma lista detalhada de Hypervisors e hardware suportados, consulte a documentação do software NVIDIA vGPU.
- A aceleração gráfica virtualizada é suportada nas plataformas gráficas de data center da família de processadores Intel Xeon E3 e na série Intel data center GPU Flex. Para obter mais informações, consulte GPU Flex series.
- As GPUs AMD são suportadas com a virtualização mxGPU da AMD. Para obter mais informações sobre hardware suportado, consulte documentação da AMD.

Dispositivo do usuário:

- A Citrix suporta até 8 monitores 4k, dependendo dos recursos de hardware. Dependendo da GPU utilizada, pode haver outras restrições de hardware para este máximo.
- A Citrix recomenda que os dispositivos do usuário tenham pelo menos 4 GB de RAM e uma CPU com velocidade de clock de 1,6 GHz ou superior. Para um desempenho ideal, recomendamos que os dispositivos do usuário tenham pelo menos 8 GB de RAM e uma CPU dual-core com velocidade de clock de 3 GHz ou superior.
- Para acesso a múltiplos monitores, a Citrix recomenda dispositivos de usuário com CPUs quad-core.
- O aplicativo Citrix Workspace deve estar instalado.

Para obter mais informações, consulte os artigos do HDX 3D Pro e www.citrix.com/xenapp/3d.

Servidor de Impressão Universal

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

O componente UpsServer é suportado em:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

Requisitos:

- Microsoft Visual C++ 2015–2022 Redistribuível
- Microsoft .NET Framework 4.8 (mínimo)

Para VDAs para SO de Múltiplas Sessões, a autenticação do usuário durante as operações de impressão requer que o Universal Print Server esteja unido ao mesmo domínio que o VDA.

Pacotes de componentes de cliente e servidor autônomos também estão disponíveis para download.

Para obter mais informações, consulte Provisionar impressoras.

Outro

Apenas o Citrix License Server 11.17.2 e versões posteriores são suportados. Para obter mais informações, consulte Licenciamento.

Consulte a Matriz de Produtos para obter mais informações sobre a compatibilidade de versões.

Para as versões suportadas do StoreFront, consulte os requisitos de sistema do StoreFront.

O Microsoft Group Policy Management Console (GPMC) é necessário se você armazenar informações de política da Citrix no Active Directory em vez do banco de dados de configuração do site. Se você instalar `CitrixGroupPolicyManagement_x64.msi` separadamente (por exemplo, em uma máquina que não tenha um componente principal do Citrix Virtual Apps and Desktops instalado), essa máquina deve ter o tempo de execução do Visual Studio 2015 instalado. Para obter mais informações, consulte a documentação da Microsoft.

Se você quiser editar GPOs de domínio usando GPMC, habilite o recurso Gerenciamento de Política de Grupo (no Gerenciador do Servidor do Windows) em todas as máquinas que contêm Delivery Controllers.

Múltiplas NICs são suportadas.

Por padrão, o Citrix Workspace app para Windows não é instalado quando você instala um VDA atual. Para obter mais informações, consulte a documentação do Citrix Workspace app para Windows.

Consulte Acesso a Aplicativos Locais para obter informações sobre navegadores suportados para esse recurso.

Esta versão do Citrix Virtual Apps and Desktops requer um mínimo de HDX RealTime Connector 2.9 LTSR. Para obter mais informações, consulte a documentação do HDX RealTime Optimization Pack.

Este produto oferece suporte às versões 3 a 5 do PowerShell.

Visão geral técnica

Citrix Virtual Apps and Desktops™ são soluções de virtualização que dão ao TI o controle de máquinas virtuais, aplicativos, licenciamento e segurança, ao mesmo tempo em que fornecem acesso de qualquer lugar para qualquer dispositivo.

O Citrix Virtual Apps and Desktops permitem:

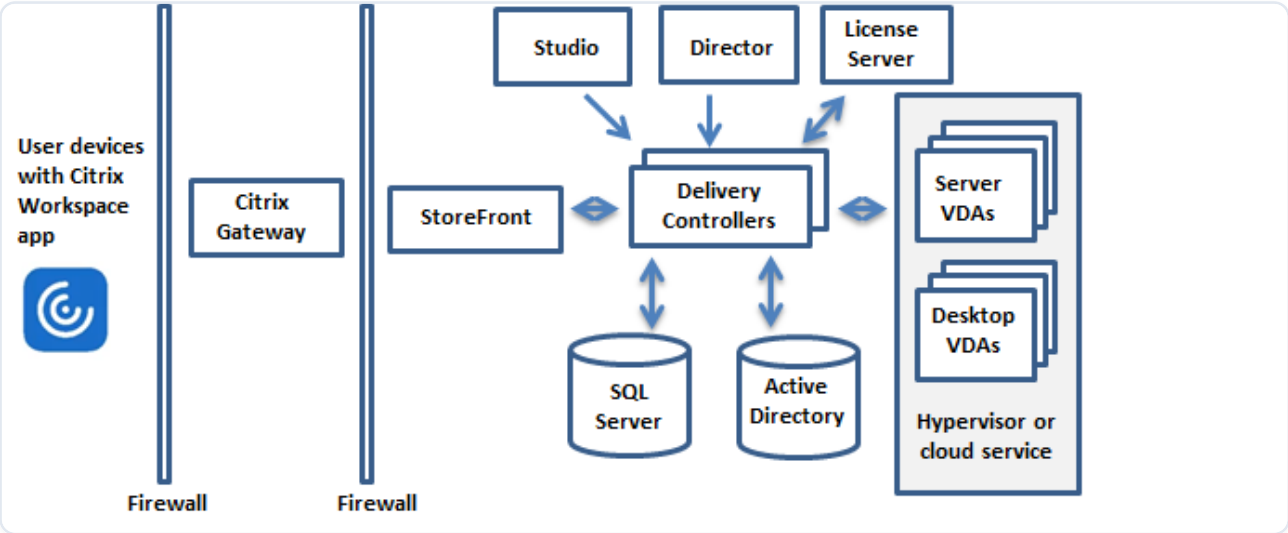
- Que os usuários finais executem aplicativos e desktops independentemente do sistema operacional e da interface do dispositivo.
- Que os administradores gerenciem a rede e controlem o acesso de dispositivos selecionados ou de todos os dispositivos.
- Que os administradores gerenciem uma rede inteira a partir de um único data center.

O Citrix Virtual Apps and Desktops compartilham uma arquitetura unificada chamada FlexCast Management Architecture (FMA). As principais características da FMA são a capacidade de executar várias versões do Citrix Virtual Apps ou Citrix Virtual Desktops™ a partir de um único site e o provisionamento integrado.

Componentes principais

Este artigo é mais útil se você é novo no Citrix Virtual Apps and Desktops.

Esta ilustração mostra os componentes principais em uma implantação típica, que é chamada de site.



Delivery Controller™

O Delivery Controller é o componente central de gerenciamento de um site. Cada site possui um ou mais Delivery Controllers. Ele é instalado em pelo menos um servidor no data center. Para confiabilidade e disponibilidade do site, instale os Controllers em mais de um servidor. Se sua implantação incluir um hypervisor ou outro serviço, os serviços do Controller se comunicam com ele para:

- Distribuir aplicativos e desktops
- autenticar e gerenciar o acesso do usuário
- Intermediar conexões entre usuários e seus desktops e aplicativos
- Otimizar conexões de usuário
- Balancear a carga das conexões

O Serviço de Broker do Controller rastreia quais usuários estão logados e onde, quais recursos de sessão os usuários possuem e se os usuários precisam se reconectar a aplicativos existentes. O Serviço de Broker executa cmdlets PowerShell e se comunica com um agente de broker nos VDAs pela porta TCP 80. Ele não tem a opção de usar a porta TCP 443.

O Serviço de Monitoramento coleta dados históricos e os armazena no banco de dados de monitoramento. Este serviço usa a porta TCP 80 ou 443.

Os dados dos serviços do Controller são armazenados no banco de dados do site.

O Controller gerencia o estado dos desktops, iniciando e parando-os com base na demanda e na configuração administrativa.

Banco de dados

Pelo menos um banco de dados Microsoft SQL Server é necessário para cada site para armazenar informações de configuração e sessão. Este banco de dados armazena os dados coletados e gerenciados pelos serviços que compõem o Controller. Instale o banco de dados em seu data center e garanta que ele tenha uma conexão persistente com o Controller.

O site também usa um banco de dados de log de configuração e um banco de dados de monitoramento. Por padrão, esses bancos de dados são instalados no mesmo local que o banco de dados do site, mas você pode alterar isso.

Virtual Delivery Agent (VDA)

O VDA é instalado em cada máquina física ou virtual em seu site que você disponibiliza aos usuários. Essas máquinas entregam aplicativos ou desktops. O VDA permite que a máquina se registre no Controller, o que, por sua vez, permite que a máquina e os recursos que ela hospeda sejam disponibilizados aos usuários. Os VDAs estabelecem e gerenciam a conexão entre a máquina e o dispositivo do usuário. Os VDAs também verificam se uma licença Citrix® está disponível para o usuário ou sessão e aplicam políticas configuradas para a sessão.

O VDA comunica informações de sessão ao Serviço de Broker no Controller através do agente de broker no VDA. O agente de broker hospeda vários plug-ins e coleta dados em tempo real. Ele se comunica com o Controller pela porta TCP 80.

A palavra "VDA" é frequentemente usada para se referir ao agente e à máquina na qual ele está instalado.

Os VDAs estão disponíveis para sistemas operacionais Windows de sessão única e multi-sessão. Os VDAs para sistemas operacionais Windows multi-sessão permitem que vários usuários se conectem ao servidor por vez. Os VDAs para sistemas operacionais Windows de sessão única permitem que apenas um usuário se conecte ao desktop por vez. VDAs Linux também estão disponíveis.

Citrix StoreFront™

O StoreFront autentica usuários e gerencia lojas de desktops e aplicativos que os usuários acessam. Ele pode hospedar sua loja de aplicativos corporativos, que oferece aos usuários acesso de autoatendimento aos desktops e aplicativos que você disponibiliza a eles. Ele também rastreia as assinaturas de aplicativos dos usuários, nomes de atalhos e outros dados. Isso ajuda a garantir que os usuários tenham uma experiência consistente em vários dispositivos.

Aplicativo Citrix Workspace™

Instalado em dispositivos de usuário e outros endpoints (como desktops virtuais), o Citrix Workspace app oferece aos usuários acesso rápido, seguro e de autoatendimento a documentos, aplicativos e desktops. O Citrix Workspace app fornece acesso sob demanda a aplicativos Windows, web e Software como Serviço (SaaS). Para dispositivos que não podem instalar o software Citrix Workspace app específico do dispositivo, o Citrix Workspace app para HTML5 fornece uma conexão através de um navegador web compatível com HTML5.

Studio

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Esta documentação do produto abrange apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Web Studio

O Web Studio é um console de gerenciamento baseado na web que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. Ele foi projetado para uma experiência de usuário aprimorada e geralmente responde mais rápido do que o Citrix Studio, o console de gerenciamento baseado em Windows. Consulte Instalar o Web Studio.

Citrix Studio

O Citrix Studio é o console de gerenciamento onde você configura e gerencia sua implantação do Citrix Virtual Apps and Desktops. O Citrix Studio elimina a necessidade de consoles de gerenciamento separados para gerenciar a entrega de aplicativos e desktops. O Citrix Studio fornece assistentes para guiá-lo pela configuração do ambiente, criação de cargas de trabalho para hospedar aplicativos e desktops e atribuição de aplicativos e desktops aos usuários. Você também pode usar o Studio para alocar e rastrear licenças Citrix para seu site.

O Citrix Studio obtém as informações que exibe do Broker Service no Controller, comunicando-se pela porta TCP 80.

Acesso Privado Seguro

A solução local Citrix Secure Private Access aprimora a postura geral de segurança e conformidade de uma organização com a capacidade de fornecer facilmente Acesso à Rede Zero Trust a aplicativos baseados em navegador (aplicativos web internos e aplicativos SaaS) usando o StoreFront como um portal de acesso unificado a aplicativos web e SaaS, juntamente com aplicativos e desktops virtuais como parte integrante do Citrix Workspace. A solução é compatível

com as versões existentes do NetScaler e do StoreFront sem quaisquer alterações nas versões. Para obter detalhes, consulte Secure Private Access para implantações locais.

Citrix Director

O Director é uma ferramenta baseada na web que permite às equipes de suporte de TI e de help desk monitorar um ambiente, solucionar problemas antes que se tornem críticos para o sistema e realizar tarefas de suporte para usuários finais. Você pode usar uma implantação do Director para se conectar e monitorar vários sites do Citrix Virtual Apps ou Citrix Virtual Desktops.

O Director exibe:

- Dados de sessão em tempo real do Broker Service no Controller, que incluem dados que o Broker Service obtém do agente de broker no VDA.
- Dados históricos do site do Monitor Service no Controller.

O Director usa os dados de desempenho e heurística do ICA® capturados pelo dispositivo Citrix Gateway para construir análises a partir dos dados e, em seguida, os apresenta aos administradores.

Você também pode visualizar e interagir com as sessões de um usuário através do Director, usando o Assistência Remota do Windows.

Citrix License Server

O Servidor de Licenças gerencia suas licenças de produtos Citrix. Ele se comunica com o Controller para gerenciar o licenciamento de cada sessão de usuário e com o Studio para alocar arquivos de licença. Um site deve ter pelo menos um servidor de licenças para armazenar e gerenciar seus arquivos de licença.

Hypervisor ou outro serviço

O hypervisor ou outro serviço hospeda as máquinas virtuais em seu site. Estas podem ser as VMs que você usa para hospedar aplicativos e desktops, e as VMs que você usa para hospedar os componentes do Citrix Virtual Apps and Desktops. Um hypervisor é instalado em um computador host dedicado inteiramente à execução do hypervisor e ao hospedagem de máquinas virtuais.

O Citrix Virtual Apps and Desktops oferece suporte a vários hypervisors e outros serviços.

Embora muitas implantações exijam um hypervisor, você não precisa de um para fornecer Acesso Remoto a PC. Um hypervisor também não é necessário ao usar o Provisioning Services (PVS) para provisionar VMs.

Componentes adicionais

Os seguintes componentes também podem ser incluídos em implantações do Citrix Virtual Apps and Desktops. Para mais informações, consulte a documentação deles.

Citrix Provisioning™

O Citrix Provisioning (anteriormente Provisioning Services) é um componente opcional disponível em algumas edições. Ele oferece uma alternativa ao MCS para provisionar máquinas virtuais. Enquanto o MCS cria cópias de uma imagem mestre, o PVS transmite a imagem mestre para os dispositivos do usuário. O PVS não requer um hypervisor para fazer isso, então você pode usá-lo para hospedar máquinas físicas. O PVS se comunica com o Controller para fornecer recursos aos usuários.

Citrix Gateway

Quando os usuários se conectam de fora do firewall corporativo, o Citrix Virtual Apps and Desktops pode usar a tecnologia Citrix Gateway (anteriormente Access Gateway e NetScaler® Gateway) para proteger essas conexões com TLS. O Citrix Gateway ou o appliance virtual VPX é um appliance SSL VPN que é implantado na zona desmilitarizada (DMZ). Ele fornece um único ponto de acesso seguro através do firewall corporativo.

Citrix SD-WAN™

Em implantações onde desktops virtuais são entregues a usuários em locais remotos, como filiais, a tecnologia Citrix SD-WAN pode ser empregada para otimizar o desempenho. Repetidores aceleram o desempenho em WANs. Com repetidores na rede, os usuários na filial experimentam um desempenho semelhante ao da LAN sobre a WAN. O Citrix SD-WAN pode priorizar diferentes partes da experiência do usuário para que, por exemplo, a experiência do usuário não se degrade no local da filial quando um arquivo grande ou trabalho de impressão é enviado pela rede. A otimização de WAN HDX™ fornece compressão tokenizada e deduplicação de dados, reduzindo drasticamente os requisitos de largura de banda e melhorando o desempenho.

Como funcionam as implantações típicas

Um site é composto por máquinas com funções dedicadas que permitem escalabilidade, alta disponibilidade e failover, e fornecem uma solução que é segura por design. Um site consiste em servidores e máquinas desktop com VDA instalado, e o Delivery Controller, que gerencia o acesso.

Comunicações de componentes em uma implantação(/en-us/citrix-virtual-apps-desktops/2407/media/deployment-overview.png)

O VDA permite que os usuários se conectem a desktops e aplicativos. Ele é instalado em máquinas virtuais no data center para a maioria dos métodos de entrega, mas também pode ser instalado em PCs físicos para Acesso Remoto a PC.

O Controller é composto por serviços Windows independentes que gerenciam recursos, aplicativos e desktops, e otimizam e equilibram as conexões dos usuários. Cada site possui um ou mais Controllers. Como as sessões são afetadas por latência, largura de banda e confiabilidade da rede, coloque todos os Controllers na mesma LAN, se possível.

Os usuários nunca acessam diretamente o Controller. O VDA serve como um intermediário entre os usuários e o Controller. Quando os usuários fazem logon usando o StoreFront, suas credenciais são passadas para o Broker Service no Controller. O Broker Service então obtém perfis e recursos disponíveis com base nas políticas definidas para eles.

Como as conexões de usuário são tratadas

Para iniciar uma sessão, o usuário se conecta através do aplicativo Citrix Workspace instalado no dispositivo do usuário, ou de um site StoreFront.

O usuário seleciona o desktop físico ou virtual ou o aplicativo virtual que é necessário.

As credenciais do usuário se movem por este caminho para acessar o Controller, que determina quais recursos são necessários comunicando-se com um Broker Service. A Citrix recomenda que os administradores coloquem um certificado SSL no StoreFront para criptografar as credenciais provenientes do aplicativo Citrix Workspace.

Fluxo de conexão do usuário(/en-us/citrix-virtual-apps-desktops/2407/media/user-connections.png)

O Broker Service determina quais desktops e aplicativos o usuário tem permissão para acessar.

Após a verificação das credenciais, as informações sobre os aplicativos ou desktops disponíveis são enviadas de volta ao usuário através do caminho StoreFront-aplicativo Citrix Workspace. Quando o usuário seleciona aplicativos ou desktops desta lista, essa informação retorna pelo caminho para o Controller. O Controller então determina o VDA apropriado para hospedar os aplicativos ou desktop específicos.

O Controller envia uma mensagem ao VDA com as credenciais do usuário e, em seguida, envia todos os dados sobre o usuário e a conexão para o VDA. O VDA aceita a conexão e envia as

informações de volta pelos mesmos caminhos para o aplicativo Citrix Workspace. Um conjunto de parâmetros necessários é coletado no StoreFront. Esses parâmetros são então enviados ao aplicativo Citrix Workspace como parte da conversa do protocolo Citrix-Workspace-app-StoreFront, ou convertidos em um arquivo Independent Computing Architecture (ICA) e baixados. Desde que o site tenha sido configurado corretamente, as credenciais permanecem criptografadas durante todo este processo.

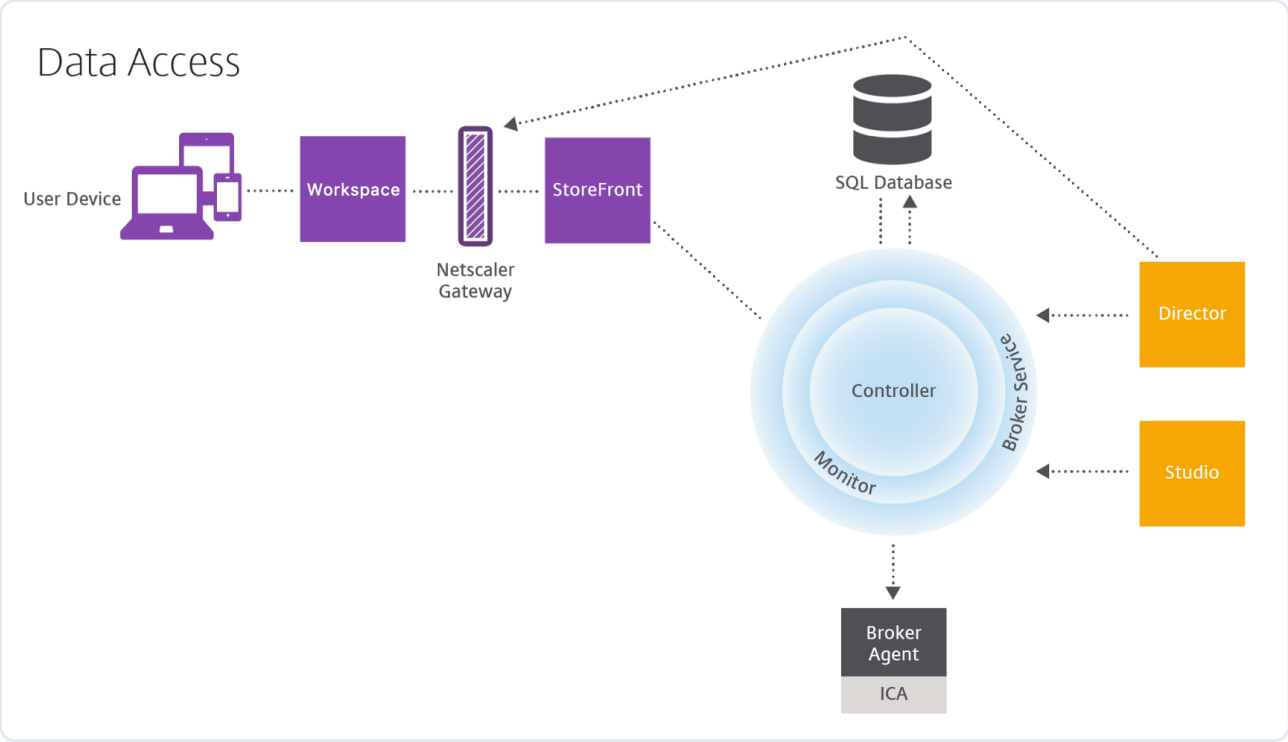
O arquivo ICA é copiado para o dispositivo do usuário e estabelece uma conexão direta entre o dispositivo e a pilha ICA em execução no VDA. Esta conexão ignora a infraestrutura de gerenciamento (aplicativo Citrix Workspace, StoreFront e Controller).

A conexão entre o aplicativo Citrix Workspace e o VDA usa o Citrix Gateway Protocol (CGP). Se uma conexão for perdida, o recurso Session Reliability permite que o usuário se reconecte ao VDA em vez de ter que reiniciar através da infraestrutura de gerenciamento. O Session Reliability pode ser ativado ou desativado nas políticas Citrix.

Depois que o cliente se conecta ao VDA, o VDA notifica o Controller de que o usuário está logado. O Controller então envia essas informações para o banco de dados do site e começa a registrar dados no banco de dados de monitoramento.

Como o acesso a dados funciona

Cada sessão do Citrix Virtual Apps and Desktops produz dados que a TI pode acessar através do Studio ou do Director. Usando o Studio, os administradores podem acessar dados em tempo real do Broker Agent para gerenciar sites. O Director acessa os mesmos dados, além de dados históricos armazenados no banco de dados de monitoramento. Ele também acessa dados HDX do NetScaler Gateway para suporte de help desk e solução de problemas.



Dentro do Controller, o Serviço de Broker relata os dados da sessão para cada sessão na máquina, fornecendo dados em tempo real. O Serviço de Monitor também rastreia os dados em tempo real e os armazena como dados históricos no banco de dados de monitoramento.

O Studio se comunica apenas com o Serviço de Broker. Ele acessa apenas dados em tempo real. O Director se comunica com o Serviço de Broker (através de um plug-in no Broker Agent) para acessar o banco de dados do site.

O Director também pode acessar o Citrix Gateway para obter informações sobre os dados HDX.

Entregar desktops e aplicativos

Você configura as máquinas que entregam aplicativos e desktops com catálogos de máquinas. Em seguida, você cria grupos de entrega que especificam os aplicativos e desktops que estarão disponíveis (usando máquinas nos catálogos) e quais usuários podem acessá-los. Opcionalmente, você pode então criar grupos de aplicativos para gerenciar coleções de aplicativos.

Catálogos de máquinas

Catálogos de máquinas são coleções de máquinas virtuais ou físicas que você gerencia como uma única entidade. Essas máquinas, e os aplicativos ou desktops virtuais nelas, são os recursos que você fornece aos seus usuários. Todas as máquinas em um catálogo têm o mesmo sistema operacional e o mesmo VDA instalados. Elas também têm os mesmos aplicativos ou desktops virtuais.

Normalmente, você cria uma imagem mestre e a usa para criar VMs idênticas no catálogo. Para VMs, você pode especificar o método de provisionamento para as máquinas nesse catálogo: ferramentas Citrix (Citrix Provisioning ou MCS) ou outras ferramentas. Alternativamente, você pode usar suas próprias imagens existentes. Nesse caso, você deve gerenciar os dispositivos de destino individualmente ou coletivamente usando ferramentas de distribuição eletrônica de software (ESD) de terceiros.

Os tipos de máquina válidos são:

- **SO multi-sessão:** Máquinas virtuais ou físicas com um sistema operacional multi-sessão. Usadas para entregar aplicativos publicados do Citrix Virtual Apps (também conhecidos como aplicativos hospedados baseados em servidor) e desktops publicados do Citrix Virtual Apps (também conhecidos como desktops hospedados em servidor). Essas máquinas permitem que vários usuários se conectem a elas ao mesmo tempo.
- **SO de sessão única:** Máquinas virtuais ou físicas com um sistema operacional de sessão única. Usadas para entregar desktops VDI (desktops executando SOs de sessão única que podem ser opcionalmente personalizados), aplicativos hospedados em VM (aplicativos de SOs de sessão única) e desktops físicos hospedados. Apenas um usuário por vez pode se conectar a cada um desses desktops.
- **Acesso Remoto a PC:** Permite que usuários remotos acessem seus PCs físicos de escritório de qualquer dispositivo executando o aplicativo Citrix Workspace. Os PCs de escritório são gerenciados através da implantação do Citrix Virtual Desktops e exigem que os dispositivos do usuário sejam especificados em uma lista de permissões.

Para mais informações, consulte Gerenciamento de Imagens do Citrix Virtual Apps and Desktops e Criar catálogos de máquinas.

Grupos de entrega

Os grupos de entrega especificam quais usuários podem acessar quais aplicativos, desktops ou ambos em quais máquinas. Os grupos de entrega contêm máquinas de seus catálogos de máquinas e usuários do Active Directory que têm acesso ao seu site. Você pode atribuir usuários aos seus grupos de entrega por seu grupo do Active Directory, porque os grupos do Active Directory e os grupos de entrega são maneiras de agrupar usuários com requisitos semelhantes.

Cada grupo de entrega pode conter máquinas de mais de um catálogo, e cada catálogo pode contribuir com máquinas para mais de um grupo de entrega. No entanto, cada máquina individual só pode pertencer a um grupo de entrega por vez.

Você define quais recursos os usuários no grupo de entrega podem acessar. Por exemplo, para entregar diferentes aplicativos a diferentes usuários, você pode instalar todos os aplicativos na imagem mestre para um catálogo e criar máquinas suficientes nesse catálogo para distribuir entre vários grupos de entrega. Você pode então configurar cada grupo de entrega para entregar um subconjunto diferente de aplicativos que estão instalados nas máquinas.

Para obter mais informações, consulte Criar grupos de entrega.

Grupos de aplicativos

Os grupos de aplicativos fornecem vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega. Usando o recurso de restrição de tag, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e ao gerenciamento de mais máquinas. Uma restrição de tag pode ser pensada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Os grupos de aplicativos também podem ser úteis ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Para obter mais informações, consulte Criar grupos de aplicativos.

Mais informações

- Diagramas do Citrix Virtual Apps and Desktops
- Portas de rede
- Bancos de dados
- Hipervisores e outros serviços compatíveis

Bancos de dados

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> Um site do Citrix Virtual Apps ou Citrix Virtual Desktops™ usa três bancos de dados SQL Server:

- **Site:** (também conhecido como configuração do site) armazena a configuração do site em execução, além do estado atual da sessão e informações de conexão.
- **Logging:** (também conhecido como Log de Configuração) armazena informações sobre alterações na configuração do site e atividades administrativas. Este banco de dados é usado quando o recurso de log de configuração está habilitado (padrão = habilitado).
- **Monitoring:** armazena dados usados pelo Director, como informações de sessão e conexão.

Cada Delivery Controller se comunica com o banco de dados do site. A autenticação do Windows é necessária entre o Controller e os bancos de dados. Um Controller pode ser desconectado ou desligado sem afetar outros Controllers no site. Isso significa, no entanto, que o banco de dados do site constitui um único ponto de falha. Se o servidor de banco de dados falhar, as conexões existentes continuarão funcionando até que um usuário faça logoff ou se desconecte. Para obter informações sobre o comportamento da conexão quando o banco de dados do site se torna indisponível, consulte Cache de Host Local.

A Citrix recomenda o seguinte em relação aos bancos de dados:

- **Faça backup regularmente.** Faça backup dos bancos de dados regularmente para que você possa restaurar a partir do backup se o servidor de banco de dados falhar. A estratégia de backup para cada banco de dados pode ser diferente. Para obter mais informações, consulte CTX135207; observe, no entanto, que ele se refere ao CitrixXenDesktopDB, que não é mais suportado ou disponível para clientes.
- **Faça backup e restaure os bancos de dados SQL Server do Site, Monitoring e Logging regularmente.** Para obter informações específicas sobre bancos de dados SQL Server, consulte Criando Backups Completos e Diferenciais de um Banco de Dados SQL Server.

Se o seu site contiver mais de uma zona, certifique-se de que a zona primária sempre contenha o banco de dados do site. Os Controllers em todas as zonas se comunicam com esse banco de dados.

Alta disponibilidade

Existem várias soluções de alta disponibilidade a serem consideradas para garantir o failover automático:

- **Grupos de Disponibilidade AlwaysOn (incluindo Grupos de Disponibilidade Básicos):** Esta solução de alta disponibilidade e recuperação de desastres de nível empresarial

introduzida no SQL Server 2012 permite maximizar a disponibilidade para um ou mais bancos de dados. Os Grupos de Disponibilidade AlwaysOn exigem que as instâncias do SQL Server residam em nós do Windows Server Failover Clustering (WSFC). Para obter mais informações, consulte Windows Server Failover Clustering com SQL Server.

- **Espelhamento de banco de dados SQL Server:** O espelhamento do banco de dados garante que, se você perder o servidor de banco de dados ativo, um processo de failover automático ocorra em questão de segundos, de modo que os usuários geralmente não sejam afetados. Este método é mais caro do que outras soluções porque licenças completas do SQL Server são necessárias em cada servidor de banco de dados. Você não pode usar a edição SQL Server Express em um ambiente espelhado.
- **Clusterização SQL:** A tecnologia de clusterização Microsoft SQL pode ser usada para permitir automaticamente que um servidor assuma as tarefas e responsabilidades de outro servidor que falhou. No entanto, configurar essa solução é mais complicado, e o processo de failover automático é tipicamente mais lento do que alternativas como o espelhamento SQL.
- **Uso dos recursos de alta disponibilidade do hipervisor:** Com este método, você implanta o banco de dados como uma máquina virtual e usa os recursos de alta disponibilidade do seu hipervisor. Esta solução é menos dispendiosa do que o espelhamento porque usa o software de hipervisor existente e você também pode usar a edição SQL Server Express. No entanto, o processo de failover automático é mais lento, pois pode levar tempo para uma nova máquina iniciar para o banco de dados, o que pode interromper o serviço para os usuários.

O recurso Local Host Cache complementa as melhores práticas de alta disponibilidade do SQL Server. O Local Host Cache permite que os usuários se conectem e reconectem a aplicativos e desktops mesmo quando o banco de dados do site não está disponível. Para obter mais informações, consulte Local Host Cache.

Se todos os Controllers em um site falharem, você pode configurar os VDAs para operar em modo de alta disponibilidade, o que permite que os usuários continuem a acessar seus desktops e aplicativos. No modo de alta disponibilidade, o VDA aceita conexões ICA diretas dos usuários, em vez de conexões intermediadas pelo Controller. Use este recurso apenas na rara ocasião em que a comunicação com todos os Controllers falhar. O recurso não é uma alternativa para outras soluções de alta disponibilidade. Para obter mais informações, consulte CTX 127564.

A instalação de um Controller em um nó em uma instalação de clusterização SQL ou espelhamento SQL não é suportada.

Instalar software de banco de dados

Por padrão, a edição SQL Server Express é instalada quando você instala o primeiro Delivery Controller™ se outra instância do SQL Server não for detectada nesse servidor. Essa ação padrão geralmente é suficiente para prova de conceito ou implantações piloto. No entanto, o SQL Server Express não oferece suporte aos recursos de alta disponibilidade da Microsoft.

A instalação padrão usa as contas de serviço e permissões padrão do Windows. Consulte a documentação da Microsoft para obter detalhes sobre esses padrões, incluindo a adição de contas de serviço do Windows à função sysadmin. O Controller usa a conta Network Service nesta configuração. O Controller não requer nenhuma função ou permissão adicional do SQL Server.

Se necessário, você pode selecionar **Ocultar instância** para a instância do banco de dados. Ao configurar o endereço do banco de dados no Web Studio, insira o número da porta estática da instância, em vez de seu nome. Consulte a documentação da Microsoft para obter detalhes sobre como ocultar uma instância do SQL Server Database Engine.

Para a maioria das implantações de produção e qualquer implantação que use recursos de alta disponibilidade da Microsoft, recomendamos usar apenas edições não Express suportadas do SQL Server. Instale o SQL Server em máquinas diferentes do servidor onde o primeiro Controller está instalado. Requisitos do sistema lista as versões suportadas do SQL Server. Os bancos de dados podem residir em uma ou mais máquinas.

Certifique-se de que o software SQL Server esteja instalado antes de criar um site. Você não precisa criar o banco de dados, mas se o fizer, ele deve estar vazio. A configuração de tecnologias de alta disponibilidade da Microsoft também é recomendada.

Use o Windows Update para manter o SQL Server atualizado.

Configurar os bancos de dados a partir do assistente de criação do site

Especifique os nomes e endereços (localização) do banco de dados na página **Bancos de dados** no assistente de criação do site. (Consulte Formatos de endereço de banco de dados.) Para evitar possíveis erros quando o Director consulta o Monitor Service, não use espaços em branco no nome do banco de dados de monitoramento.

A página **Bancos de dados** oferece duas opções para configurar os bancos de dados: automática e usando scripts. Geralmente, você pode usar a opção automática se você (o usuário do Web Studio e o administrador Citrix) tiver os privilégios de banco de dados necessários. (Consulte Permissões necessárias para configurar bancos de dados.)

Você pode alterar o local do banco de dados de log de configuração e monitoramento mais tarde, após criar o site. Consulte Alterar locais do banco de dados.

Para configurar um site para usar um banco de dados espelho, conclua o seguinte e, em seguida, prossiga com os procedimentos de configuração automática ou por script.

1. Instale o software SQL Server em dois servidores, A e B.
2. No Servidor A, crie o banco de dados destinado a ser usado como principal. Faça backup do banco de dados no Servidor A e, em seguida, copie-o para o servidor B.
3. No Servidor B, restaure o arquivo de backup.
4. Inicie o espelhamento no servidor A.

Para verificar o espelhamento após criar o site, execute o cmdlet do PowerShell `get-configdbconnection` para garantir que o Failover Partner tenha sido definido na string de conexão para o espelho.

Se você adicionar, mover ou remover um Delivery Controller em um ambiente de banco de dados espelho posteriormente, consulte Delivery Controllers.

Configuração automática

Se você tiver os privilégios de banco de dados necessários, selecione **Criar e configurar bancos de dados a partir do Studio** na página **Bancos de Dados** do assistente de criação do site. Em seguida, forneça os nomes e endereços dos bancos de dados principais.

Se um banco de dados existir em um endereço especificado, ele deve estar vazio. Se os bancos de dados não existirem em um endereço especificado, você será informado de que um banco de dados não pode ser encontrado e, em seguida, perguntado se deseja que o banco de dados seja criado para você. Ao confirmar essa ação, o Web Studio cria automaticamente os bancos de dados e, em seguida, aplica os scripts de inicialização para os bancos de dados principal e de réplica.

Configuração por script

Se você não tiver os direitos de banco de dados necessários, solicite assistência de alguém que os tenha, como um administrador de banco de dados. Aqui está a sequência:

1. Na página **Bancos de Dados** do assistente de criação do site, selecione **Gerar scripts para configuração manual**. Esta ação gera os três tipos de scripts a seguir para cada um dos seguintes bancos de dados principal e de réplica: bancos de dados de site, monitoramento e log.

- *Script contendo "SysAdmin" em seu nome*. Um script que cria os bancos de dados e o login do Delivery Controller. Essas tarefas exigem direitos de securityadmin.
- *Script contendo "DbOwner" em seu nome*. Um script que cria as funções de usuário no banco de dados, adiciona os logins e, em seguida, cria os esquemas do banco de dados. Essas tarefas exigem direitos de `db_owner`.
- *Script contendo "Mixed" em seu nome*. Todas as tarefas em um único script, independentemente dos direitos necessários.

Você pode indicar onde armazenar os scripts.

> **Observação:**
>
> Em ambientes corporativos, a configuração do banco de dados inclui scripts que podem ser tratados por diferentes equipes com diferentes funções (direitos): `securityadmin` ou `db_owner`. Se aplicável, você primeiro tem scripts "SysAdmin" executados por administradores com a função `securityadmin` e, em seguida, scripts "DbOwner" executados por administradores com direitos `db_owner`. Para gerar esses scripts, você também pode usar o PowerShell. Para obter detalhes, consulte Preferred database rights scripts.

2. Entregue esses scripts ao seu administrador de banco de dados. O assistente de criação do site para automaticamente neste ponto. Você será solicitado quando retornar mais tarde para continuar a criação do site.

O administrador do banco de dados então cria os bancos de dados. Cada banco de dados deve ter as seguintes características:

- Use um agrupamento que termine com `_CI_AS_KS`. Recomendamos usar um agrupamento que termine com `_100_CI_AS_KS`.
- Para um desempenho ideal, habilite o Snapshot Read-Committed do SQL Server. Para obter detalhes, consulte CTX 137161.
- Recursos de alta disponibilidade configurados, se aplicável.
- Para configurar o espelhamento, primeiro defina o banco de dados para usar o modelo de recuperação completa (o modelo simples é o padrão). Faça backup do banco de dados principal em um arquivo e copie-o para o servidor espelho. Em seguida, restaure o arquivo de backup no servidor espelho. Finalmente, inicie o espelhamento no servidor principal.

O administrador do banco de dados usa o utilitário de linha de comando SQLCMD ou o SQL Server Management Studio no modo SQLCMD para:

- Executar cada um dos scripts `xxx_Replica.sql` nas instâncias de banco de dados SQL Server de alta disponibilidade (se a alta disponibilidade estiver configurada)
- Executar cada um dos scripts `xxx\_Principal.sql` nas instâncias de banco de dados SQL Server principais.

Consulte a documentação da Microsoft para obter detalhes sobre o SQLCMD.

Quando todos os scripts forem concluídos com êxito, o administrador do banco de dados fornecerá ao administrador do Citrix os três endereços principais do banco de dados.

O Web Studio solicita que você continue a criação do site. Você é redirecionado para a página **Bancos de Dados**. Insira os endereços. Se algum dos servidores que hospeda um banco de dados não puder ser contatado, uma mensagem de erro será exibida.

Permissões necessárias para configurar bancos de dados

Você deve ser um administrador local e um usuário de domínio para criar e inicializar os bancos de dados (ou alterar o local do banco de dados). Você também deve ter certas permissões do SQL Server. As permissões a seguir podem ser configuradas explicitamente ou adquiridas por meio da associação a um grupo do Active Directory. Se suas credenciais de usuário do Web Studio não incluírem essas permissões, você será solicitado a fornecer as credenciais de usuário do SQL Server.

OPERAÇÃO	PROPÓSITO	FUNÇÃO DO SERVIDOR	FUNÇÃO DO BANCO DE DADOS
Criar um banco de dados	Criar um banco de dados vazio adequado	`dbcreator`	
Criar um esquema	Criar todos os esquemas específicos do serviço e adicionar o primeiro Controller ao site	`securityadmin`*	`db_owner`

OPERAÇÃO	PROPÓSITO	FUNÇÃO DO SERVIDOR	FUNÇÃO DO BANCO DE DADOS
Adicionar um Controller	Adicionar um Controller (diferente do primeiro) ao site	`securityadmin` *	`db_owner`
Adicionar um Controller (servidor espelho)	Adicionar um login de Controller ao servidor de banco de dados atualmente na função de espelho de um banco de dados espelhado	`securityadmin` *	
Remover Controller	Remover controller do site	**	`db_owner`
Atualizar um esquema	Aplicar atualizações de esquema ou hotfixes		`db_owner`

* Embora tecnicamente mais restritivo, na prática, você pode tratar a função de servidor `securityadmin` como equivalente à função de servidor `sysadmin`.

** Quando um Controller é removido de um site, o logon do Controller para o servidor de banco de dados não é removido. Isso é para evitar a remoção potencial de um logon que está sendo usado por outros serviços que não este produto Citrix na mesma máquina. O logon deve ser removido manualmente se não for mais necessário. Esta ação requer a associação à função de servidor `securityadmin`.

Ao usar o Web Studio para realizar essas operações, o usuário do Web Studio deve ter uma conta de servidor de banco de dados que seja explicitamente membro das funções de servidor apropriadas, ou ser capaz de fornecer credenciais de uma conta que seja.

Scripts de direitos de banco de dados preferenciais

Em ambientes corporativos, a configuração do banco de dados inclui scripts que devem ser tratados por diferentes equipes com diferentes funções (direitos): `securityadmin` ou `db_owner`.

Usando o PowerShell, você pode especificar os direitos de banco de dados preferenciais. A especificação de um valor não padrão resulta na criação de scripts separados. Um script contém tarefas que precisam da função `securityadmin`. O outro script requer apenas direitos `db_owner` e pode ser executado por um administrador Citrix, sem a necessidade de contatar um administrador de banco de dados.

Nos cmdlets `get-*DBSchema`, a opção `-DatabaseRights` tem os seguintes valores válidos:

- `SA`: Gera um script que cria os bancos de dados e o login do Delivery Controller. Essas tarefas exigem direitos `securityadmin`.
- `DBO`: Gera um script que cria as funções de usuário no banco de dados, adiciona os logons e, em seguida, cria os esquemas do banco de dados. Essas tarefas exigem direitos `db_owner`.
- `Mixed`: (Padrão) Todas as tarefas em um script, independentemente dos direitos necessários.

Para obter mais informações, consulte a ajuda do cmdlet.

Formatos de endereço de banco de dados

Você pode especificar um endereço de banco de dados em um dos seguintes formatos:

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

Para um Grupo de Disponibilidade AlwaysOn, especifique o ouvinte do grupo no campo de localização.

Alterar locais do banco de dados

Depois de criar um site, você pode alterar o local dos bancos de dados de log de configuração e monitoramento. (Você não pode alterar o local do banco de dados do site.) Ao alterar o local de um banco de dados:

- Os dados do banco de dados anterior não são importados para o novo banco de dados.
- Os logs não podem ser agregados de ambos os bancos de dados ao recuperar logs.
- A primeira entrada de log no novo banco de dados indica que uma alteração no banco de dados ocorreu, mas não identifica o banco de dados anterior.

Você não pode alterar o local do banco de dados de log de configuração quando o log obrigatório está ativado.

Para alterar o local de um banco de dados:

1. Certifique-se de que uma versão compatível do Microsoft SQL Server esteja instalada no servidor onde você deseja que o banco de dados resida. Configure os recursos de alta disponibilidade conforme necessário.
2. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
3. Localize o bloco **Banco de Dados** e selecione **Editar**.
4. Na página **Gerenciar Banco de Dados**, selecione o banco de dados para o qual você deseja especificar um novo local e, em seguida, selecione **Alterar Banco de Dados** na barra de ações.
5. Especifique o novo local e o nome do banco de dados.
6. Se você quiser que o Web Studio crie o banco de dados e tiver as permissões apropriadas, clique em **Concluído**. Quando solicitado, clique em **Concluído**, e então o Web Studio criará o banco de dados automaticamente. O Web Studio tenta acessar o banco de dados usando suas credenciais. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. O Web Studio então carrega o esquema do banco de dados para ele. As credenciais são retidas apenas durante o período de criação do banco de dados.
7. Se você não quiser que o Web Studio crie o banco de dados, ou se não tiver permissões suficientes, clique em **Gerar script do banco de dados**. Os scripts gerados incluem instruções para criar manualmente o banco de dados e um banco de dados espelho, se necessário. Antes de carregar o esquema, certifique-se de que o banco de dados esteja vazio e que pelo menos um usuário tenha permissão para acessar e alterar o banco de dados.

Mais informações

- Ferramenta de dimensionamento de banco de dados.
- Dimensionando o banco de dados do site e configurando cadeias de conexão ao usar soluções de alta disponibilidade do SQL Server.

Métodos de entrega

O Citrix Virtual Apps and Desktops™ oferece vários métodos de entrega. Um único método de entrega provavelmente não atenderá a todos os seus requisitos.

Introdução

Escolher o método de entrega de aplicativo apropriado ajuda a melhorar a escalabilidade, o gerenciamento e a experiência do usuário.

- **Aplicativo instalado:** O aplicativo faz parte da imagem base da área de trabalho. O processo de instalação envolve dll, exe e outros arquivos copiados para a unidade da imagem, além de modificações no registro. Para obter detalhes, consulte Criar catálogos de máquinas.
- **Aplicativo transmitido (Microsoft App-V):** O aplicativo é perfilado e entregue às áreas de trabalho pela rede sob demanda. Os arquivos do aplicativo e as configurações do registro são colocados em um contêiner na área de trabalho virtual e isolados do sistema operacional base e uns dos outros. Esse isolamento ajuda a resolver problemas de compatibilidade. Para obter detalhes, consulte Implantar e entregar aplicativos 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 (VDA, agente de provisionamento Citrix) e muitas camadas de aplicativo, um administrador pode criar facilmente novas imagens implantáveis. O uso de camadas simplifica a manutenção contínua, pois um SO, agente e aplicativo existem em uma única camada. Ao atualizar a camada, todas as imagens implantadas que contêm essa camada são atualizadas. Para obter detalhes, consulte Citrix App Layering.
- **Aplicativo Windows hospedado:** Um aplicativo instalado em um host Citrix Virtual Apps multiusuário e implantado como um aplicativo e não como uma área de trabalho. Um usuário acessa o aplicativo Windows hospedado de forma transparente a partir da área de trabalho VDI ou do dispositivo de endpoint, ocultando o fato de que o aplicativo está sendo executado remotamente. Para obter detalhes, consulte Criar grupos de entrega.
- **Aplicativo local:** Um aplicativo implantado no dispositivo de endpoint. A interface do aplicativo aparece na sessão VDI hospedada do usuário, mesmo que seja executada no endpoint. Para obter detalhes, consulte Acesso a aplicativos locais e redirecionamento de URL.

Para áreas de trabalho, considere áreas de trabalho publicadas ou áreas de trabalho VDI.

Aplicativos e áreas de trabalho publicados do Citrix Virtual Apps™

Use máquinas de SO multi-sessão para entregar aplicativos publicados e áreas de trabalho publicadas do Citrix Virtual Apps and Desktops.

Caso de uso:

- Você deseja uma entrega baseada em servidor de baixo custo 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 realizam tarefas bem definidas e não exigem personalização ou acesso offline a aplicativos. Os usuários podem incluir trabalhadores de tarefas, como operadores de call center e trabalhadores de varejo, ou usuários que compartilham estações de trabalho.
- Tipos de aplicativo: qualquer aplicativo.

Benefícios e considerações:

- Solução gerenciável e escalável dentro do seu data center.
- Solução de entrega de aplicativos mais econômica.
- Os aplicativos hospedados são gerenciados centralmente e os usuários não podem modificar o aplicativo. Isso proporciona uma experiência de usuário consistente, segura e confiável.
- Os usuários devem estar online para acessar seus aplicativos.

Experiência do usuário:

- O usuário solicita um ou mais aplicativos do StoreFront™, do menu **Iniciar** ou de um URL que você fornece.
- Os aplicativos são entregues virtualmente e exibidos perfeitamente em alta definição nos dispositivos do usuário.
- Dependendo das configurações de perfil, as alterações do usuário são salvas quando a sessão do aplicativo do usuário termina. Caso contrário, as alterações são excluídas.

Processar, hospedar e entregar aplicativos:

- O processamento de aplicativos ocorre em máquinas de hospedagem, em vez de nos dispositivos do usuário. A máquina de hospedagem pode ser física ou virtual.
- Aplicativos e desktops residem em uma máquina de SO multi-sessão.
- As máquinas ficam disponíveis por meio de catálogos de máquinas.
- As máquinas dos catálogos de máquinas são organizadas em grupos de entrega que entregam o mesmo conjunto de aplicativos a grupos de usuários.
- Máquinas de SO multi-sessão suportam grupos de entrega que hospedam desktops ou aplicativos, ou ambos.

Gerenciamento e atribuição de sessão:

- Máquinas de SO multissessão executam várias sessões a partir de uma única máquina para entregar múltiplos aplicativos e desktops a múltiplos usuários conectados simultaneamente. Cada usuário requer uma única sessão a partir da qual pode executar todos os seus aplicativos hospedados.

  Por exemplo, um usuário faz logon e solicita um aplicativo. Uma sessão nessa máquina fica indisponível para outros usuários. Um segundo usuário faz logon e solicita um aplicativo que essa máquina hospeda. Uma segunda sessão na mesma máquina agora está indisponível. Se ambos os usuários solicitarem mais aplicativos, nenhuma sessão adicional será necessária porque um usuário pode executar vários aplicativos usando a mesma sessão. Se mais dois usuários fizerem logon e solicitarem desktops, e duas sessões estiverem disponíveis na mesma máquina, essa única máquina estará agora usando quatro sessões para hospedar quatro usuários diferentes.
- Dentro do grupo de entrega ao qual um usuário é atribuído, uma máquina no servidor menos carregado é selecionada. Uma máquina com disponibilidade de sessão é atribuída aleatoriamente para entregar aplicativos a um usuário quando esse usuário faz logon.

Aplicativos hospedados em VM

Use máquinas de SO de sessão única para entregar aplicativos hospedados em VM

Caso de uso:

- Você deseja uma solução de entrega de aplicativos baseada em cliente que seja segura, forneça gerenciamento centralizado e suporte muitos usuários por servidor host. Você deseja fornecer a esses usuários aplicativos que são exibidos perfeitamente em alta definição.
- Seus usuários são internos, contratados externos, colaboradores de terceiros e outros membros provisórios da equipe. Seus usuários não exigem acesso offline a aplicativos hospedados.
- Tipos de aplicativos: Aplicativos que podem não funcionar bem com outros aplicativos ou podem interagir com o sistema operacional, como o Microsoft .NET Framework. Esses tipos de aplicativos são ideais para hospedagem em máquinas virtuais.

Benefícios e considerações:

- Aplicativos e desktops na imagem mestre são gerenciados, hospedados e executados com segurança em máquinas dentro do seu data center, fornecendo 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 cada vez que esse usuário fizer logon. Máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de múltiplas sessões não é suportada em máquinas de SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega ao fazer logon, e os usuários devem estar online para acessar seus aplicativos.
- Este método pode aumentar a quantidade de recursos do servidor para processar aplicativos e aumentar a quantidade de armazenamento para os dados dos usuários.

Experiência do usuário:

- A mesma experiência de aplicativo contínua que a hospedagem de aplicativos compartilhados em máquinas de SO multi-sessão.

Processar, hospedar e entregar aplicativos:

- O mesmo que máquinas de SO multi-sessão, exceto que são máquinas de SO virtuais de sessão única.

Gerenciamento e atribuição de sessão:

- Máquinas de SO de sessão única executam uma única sessão de desktop a partir de uma única máquina. Ao acessar apenas aplicativos, um único usuário pode usar vários aplicativos (e não está limitado a um único aplicativo) porque o sistema operacional vê cada aplicativo como uma nova sessão.
- Dentro de um grupo de entrega, quando os usuários fazem logon, eles podem acessar uma máquina atribuída estaticamente (cada vez que o usuário faz logon na mesma máquina) ou uma máquina atribuída aleatoriamente que é selecionada com base na disponibilidade da sessão.

Desktops VDI

Use máquinas de SO de sessão única para entregar desktops VDI do Citrix Virtual Apps and Desktops.

Desktops VDI são hospedados em máquinas virtuais e fornecem a cada usuário um sistema operacional de desktop.

Desktops VDI exigem mais recursos do que desktops publicados, mas não exigem que os aplicativos instalados neles suportem sistemas operacionais baseados em servidor. Além disso, dependendo do tipo de desktop VDI que você escolher, esses desktops podem ser atribuídos a usuários individuais. Isso permite aos usuários um alto nível de personalização.

Ao criar um catálogo de máquinas para desktops VDI, você cria um destes tipos de desktops:

- **Desktop aleatório não persistente, também conhecido como desktop VDI agrupado:** Cada vez que um usuário faz logon em um desses desktops, esse usuário se conecta a um desktop selecionado de um pool de desktops. Esse pool é baseado em uma única imagem mestre. Todas as alterações no desktop são perdidas quando a máquina é reiniciada.
- **Desktop estático não persistente:** Durante o primeiro logon, um usuário é atribuído a um desktop de um pool de desktops. (Cada máquina no pool é baseada em uma única imagem mestre.) Após o primeiro uso, cada vez que um usuário faz logon para usar um desktop, esse usuário se conecta ao mesmo desktop que foi atribuído no primeiro uso. Todas as alterações no desktop são perdidas quando a máquina é reiniciada.
- **Desktop estático persistente:** Ao contrário de outros tipos de desktops VDI, os usuários podem personalizar totalmente esses desktops. Durante o primeiro logon, um usuário é atribuído a um desktop de um pool de desktops. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso. As alterações no desktop são retidas quando a máquina é reiniciada.

Acesso Remoto ao PC

O Acesso Remoto a PC é um recurso do Citrix Virtual Apps and Desktops que permite às organizações permitir facilmente que seus funcionários acessem recursos corporativos remotamente de forma segura. A plataforma Citrix torna esse acesso seguro possível, dando aos usuários acesso aos seus PCs físicos do escritório. Se os usuários puderem acessar seus PCs do escritório, eles poderão acessar todos os aplicativos, dados e recursos de que precisam para realizar seu trabalho. O Acesso Remoto a PC elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, desktops virtuais ou aplicativos e sua infraestrutura associada.

O Acesso Remoto a PC usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam desktops e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Acesso Remoto a PC são os mesmos exigidos para a implantação do Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários recebem a

melhor experiência de usuário usando o Citrix HDX™ para entregar sua sessão de PC do escritório.

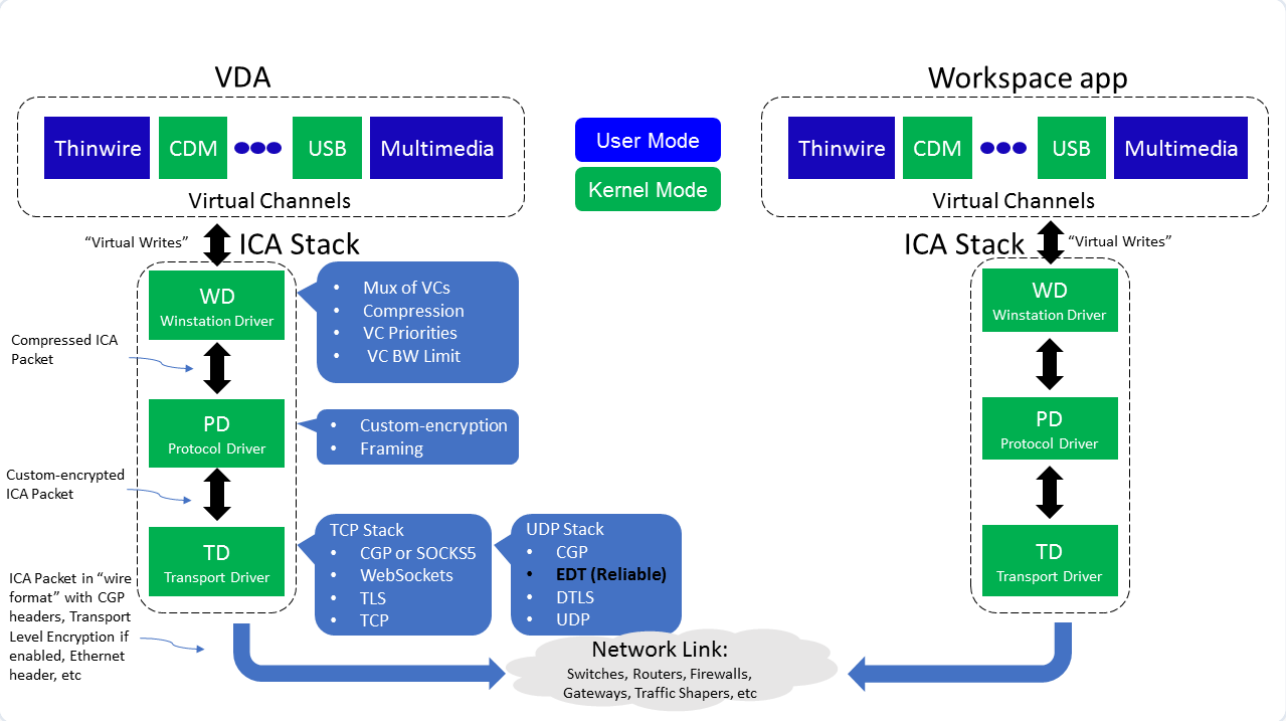
Para obter mais informações, Acesso Remoto a PC.

HDX™

Aviso:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Citrix HDX representa um amplo conjunto de tecnologias que oferecem uma experiência de alta definição aos usuários de aplicativos e desktops centralizados, em qualquer dispositivo e em qualquer rede.

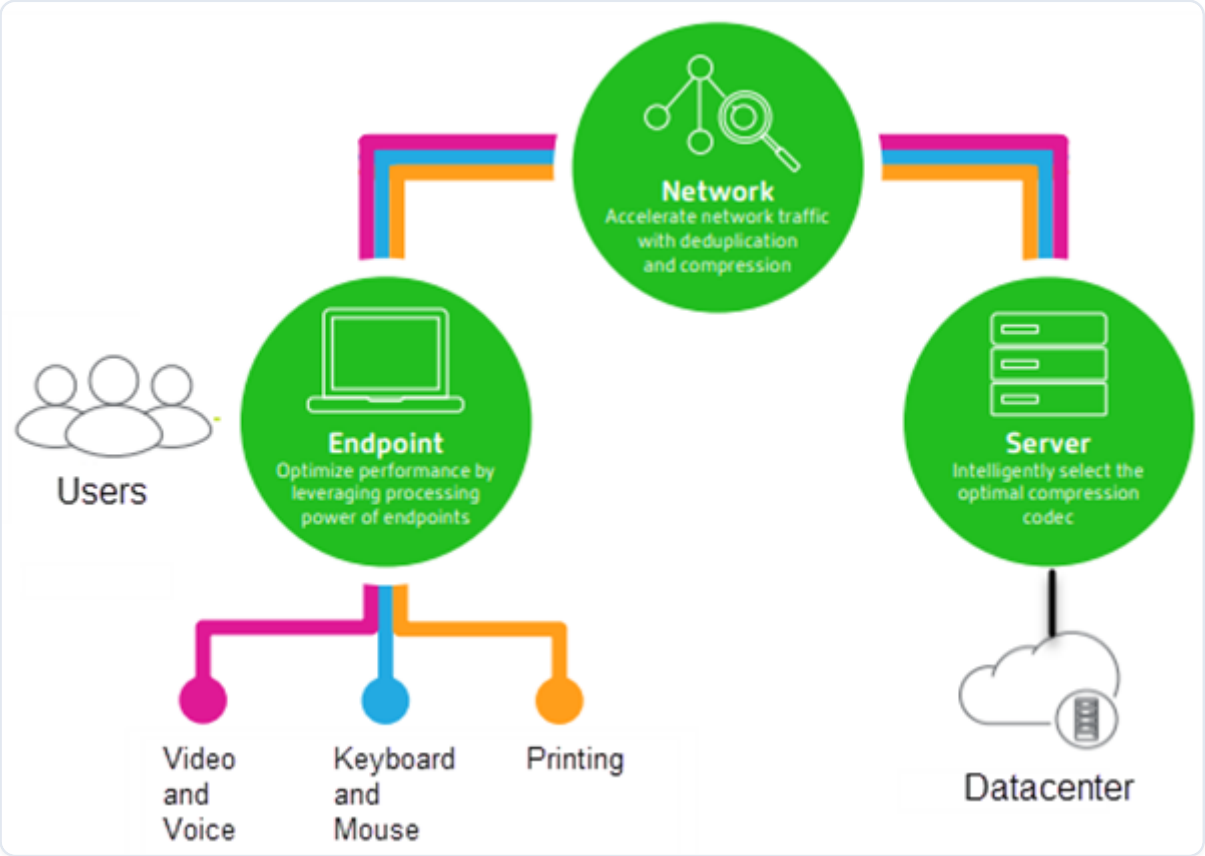


O HDX é projetado com base em três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência de TI e do usuário, diminuem o consumo de largura de banda e aumentam a densidade de usuários por servidor de hospedagem.

- **Redirecionamento inteligente** - O redirecionamento inteligente examina a atividade da tela, os comandos do aplicativo, o dispositivo de endpoint e os recursos de rede e servidor para determinar instantaneamente como e onde renderizar uma atividade de aplicativo ou desktop. A renderização pode ocorrer no dispositivo de endpoint ou no servidor de hospedagem.
- **Compressão adaptativa** - A compressão adaptativa permite que exibições multimídia ricas sejam entregues em conexões de rede finas. O HDX primeiro avalia várias variáveis, como o tipo de entrada, dispositivo e exibição (texto, vídeo, voz e multimídia). Ele escolhe o codec de compressão ideal e a melhor proporção de uso de CPU e GPU. Em seguida, ele se adapta inteligentemente com base em cada usuário e base únicos. Essa adaptação inteligente é por usuário, ou mesmo por sessão.



- **Desduplicação de dados** - A desduplicação do tráfego de rede reduz o volume total de dados enviados entre cliente e servidor. Isso é feito aproveitando padrões repetidos em dados comumente acessados, como gráficos de bitmap, documentos, trabalhos de impressão e mídia transmitida. O cache desses padrões permite que apenas as alterações sejam transmitidas pela rede, eliminando o tráfego duplicado. O HDX também suporta a transmissão multicast de fluxos multimídia, onde uma única transmissão da fonte é visualizada por vários assinantes em um local, em vez de uma conexão um-para-um para cada usuário.

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 aprimorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários recebam uma experiência suave e contínua com conteúdo multimídia em seus desktops ou aplicativos virtuais. O controle de espaço de trabalho permite que os usuários pausem desktops e aplicativos virtuais e retomem o trabalho 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 do HDX se adaptam às mudanças no ambiente. Os recursos equilibram desempenho e largura de banda. Eles aplicam as melhores tecnologias para cada cenário de usuário, seja o desktop ou aplicativo acessado localmente na rede corporativa ou remotamente de fora do firewall corporativo.

No data center

O HDX usa o poder de processamento e a escalabilidade dos servidores para oferecer desempenho gráfico avançado, independentemente dos recursos do dispositivo cliente.

O monitoramento de canal HDX fornecido pelo Citrix Director exibe o status dos canais HDX conectados nos dispositivos do usuário.

HDX Insight

O HDX Insight é a integração do NetScaler® Network Inspector e Performance Manager com o Director. Ele captura dados sobre o tráfego ICA e fornece uma visualização em painel de detalhes em tempo real e históricos. Esses dados incluem latência de sessão ICA do lado do cliente e do lado do servidor, uso de largura de banda dos canais ICA e o valor do tempo de ida e volta do ICA de cada sessão.

Você pode habilitar o NetScaler para usar o canal virtual HDX Insight para mover todos os pontos de dados necessários em um formato não compactado. Se você desabilitar esse recurso, o dispositivo NetScaler descriptografa e descompacta o tráfego ICA® espalhado por vários canais

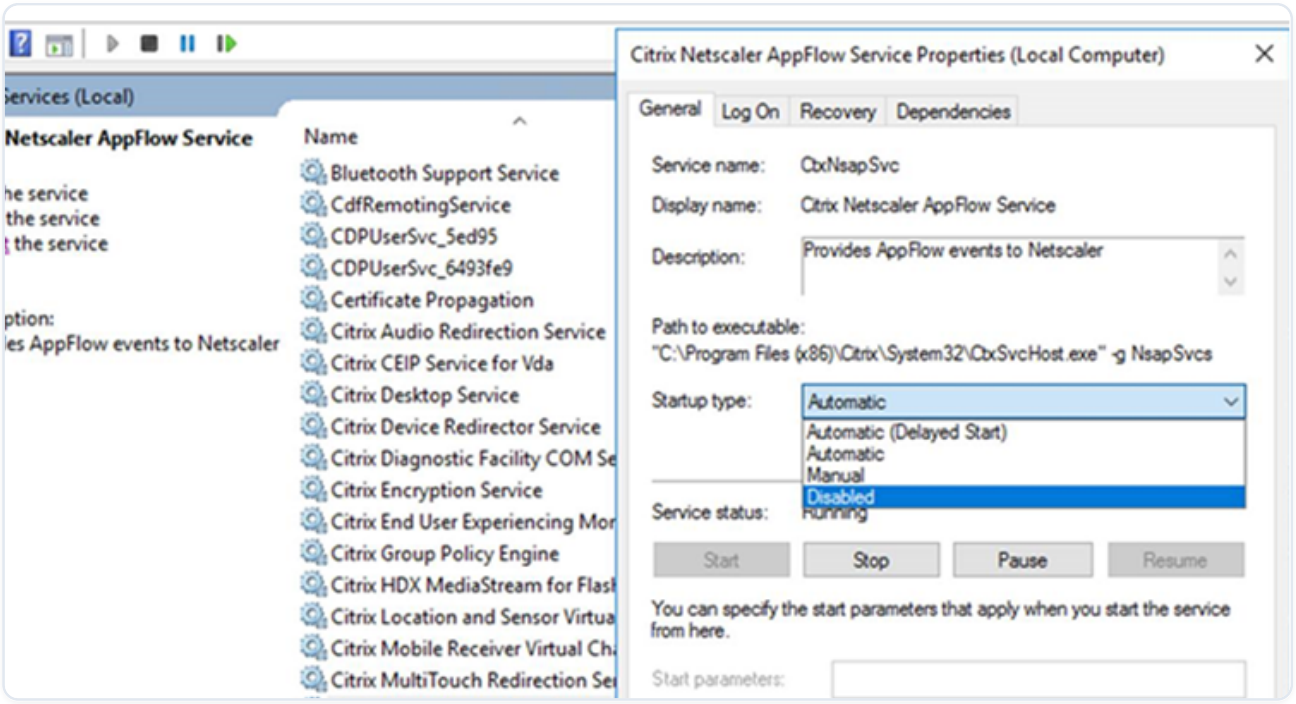
virtuais. Usar o único canal virtual diminui a complexidade, aumenta a escalabilidade e é mais econômico.

Requisitos mínimos:

- NetScaler versão 12.0 Build 57.x
- Citrix Workspace™ app para Windows 1808
- Citrix Receiver para Windows 4.10
- Citrix Workspace app para Mac 1808
- Citrix Receiver para Mac 12.8

Ativar ou desativar o canal virtual HDX Insight

Para desativar este 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 após alterar essas propriedades. Por padrão, este serviço está ativado (Automático).



Experimente os recursos do HDX a partir do seu desktop virtual

- Para ver como o redirecionamento de conteúdo do navegador, uma das quatro tecnologias de redirecionamento multimídia HDX, acelera a entrega de conteúdo multimídia HTML5 e WebRTC:

  a. Baixe a extensão do navegador Chrome e instale-a no desktop virtual.

b. Para experimentar como o redirecionamento de conteúdo do navegador acelera a entrega de conteúdo multimídia para desktops virtuais, assista a um vídeo em seu desktop a partir de um site que contenha vídeos HTML5, como o YouTube. Os usuários não sabem quando o redirecionamento de conteúdo do navegador está em execução. Para ver se o redirecionamento de conteúdo do navegador está sendo usado, arraste a janela do navegador rapidamente. Você verá um atraso ou fora do quadro entre a área de visualização e a interface do usuário. Você também pode clicar com o botão direito do mouse na página da web e procurar por **Sobre o Redirecionamento de Navegador HDX** no menu.

- Para ver como o HDX oferece áudio de alta definição:

  a. Configure seu cliente Citrix para máxima qualidade de áudio; consulte a documentação do aplicativo Citrix Workspace para obter detalhes.

  b. Reproduza arquivos de música usando um reprodutor de áudio digital (como o iTunes) em seu desktop.

O HDX oferece uma experiência superior de gráficos e vídeo para a maioria dos usuários por padrão, e a configuração não é necessária. As configurações de política do Citrix que fornecem a melhor experiência para a maioria dos casos de uso estão ativadas por padrão.

- O HDX seleciona automaticamente o melhor método de entrega com base no cliente, plataforma, aplicativo e largura de banda da rede, e então se autoajusta com base nas condições em mudança.
- O HDX otimiza o desempenho de gráficos e vídeo 2D e 3D.
- O HDX permite que os dispositivos do usuário transmitam arquivos multimídia diretamente do provedor de origem na internet ou intranet, em vez de através do servidor host. Se os requisitos para esta busca de conteúdo do lado do cliente não forem atendidos, a entrega de mídia retorna à busca de conteúdo do lado do servidor e ao redirecionamento multimídia. Geralmente, ajustes nas políticas de recursos de redirecionamento multimídia não são necessários.
- O HDX entrega conteúdo de vídeo rico renderizado pelo servidor para desktops virtuais quando o redirecionamento multimídia não está disponível: Assista a um vídeo em um site que contenha vídeos de alta definição, como `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`.

É bom saber:

- Para obter informações de suporte e requisitos para recursos HDX, consulte o artigo Requisitos do sistema. Salvo indicação em contrário, os recursos HDX estão disponíveis para máquinas Windows Multi-session OS e Windows Single-session OS compatíveis, além de desktops de Acesso Remoto para PC.
- Este conteúdo descreve como otimizar a experiência do usuário, melhorar a escalabilidade do servidor ou reduzir os requisitos de largura de banda. Para obter informações sobre como usar as políticas e configurações de política do Citrix, consulte a documentação Políticas do Citrix para esta versão.
- Para instruções que incluem a edição do registro, use com cautela: editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Reconexão automática do cliente e confiabilidade da sessão

Ao acessar aplicativos ou desktops hospedados, pode ocorrer interrupção da rede. Para ter uma reconexão mais suave, oferecemos reconexão automática do cliente e confiabilidade da sessão. Em uma configuração padrão, a confiabilidade da sessão é iniciada e, em seguida, a reconexão automática do cliente é acionada.

Reconexão automática do cliente:

A reconexão automática do cliente reinicia o mecanismo do cliente para reconectar a uma sessão desconectada. A reconexão automática do cliente fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Se a reconexão automática do cliente estiver em andamento, o sistema envia uma notificação de interrupção de rede de aplicativo e desktops ao usuário da seguinte forma:

- **Desktops.** A janela da sessão fica esmaecida e um cronômetro de contagem regressiva exibe o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela da sessão é fechada e uma caixa de diálogo aparece para o usuário contendo um cronômetro de contagem regressiva mostrando o tempo até que as reconexões sejam tentadas.

Durante a reconexão automática do cliente, as sessões são reiniciadas esperando conectividade de rede. O usuário não pode interagir com as sessões enquanto uma reconexão automática do cliente estiver em andamento.

Na reconexão, as sessões desconectadas se reconectam usando as informações de conexão salvas. O usuário pode interagir com os aplicativos e desktops normalmente.

Configurações padrão de reconexão automática do cliente:

- Tempo limite de reconexão automática do cliente: 120 segundos
- Reconexão automática do cliente: Habilitado
- Autenticação de reconexão automática do cliente: Desabilitado
- Registro de reconexão automática do cliente: Desativado

Para obter mais informações, consulte Configurações da política de reconexão automática do cliente.

Confiabilidade da sessão:

A confiabilidade da sessão reconecta as sessões ICA de forma contínua em caso de interrupções de rede. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Após o tempo limite de confiabilidade da sessão, as configurações de reconexão automática do cliente entram em vigor, tentando reconectar o usuário à sessão desconectada. Quando a confiabilidade da sessão está em andamento, as notificações de interrupção de rede de aplicativos e desktops são enviadas ao usuário da seguinte forma:

- **Desktops.** A janela da sessão torna-se translúcida e um cronômetro de contagem regressiva exibe o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela torna-se translúcida, juntamente com pop-ups de conexão interrompida da área de notificação.

Enquanto a confiabilidade da sessão está ativa, o usuário não pode interagir com as sessões ICA. No entanto, as ações do usuário, como pressionamentos de tecla, são armazenadas em buffer por alguns segundos imediatamente após a interrupção da rede e retransmitidas quando a rede está disponível.

Na reconexão, o cliente e o servidor retomam no mesmo ponto em que estavam em sua troca de protocolo. As janelas da sessão perdem a translucidez e pop-ups apropriados da área de notificação são exibidos para os aplicativos.

Configurações padrão de confiabilidade da sessão

- Tempo limite de confiabilidade da sessão: 180 segundos
- Nível de opacidade da interface do usuário de reconexão: 80%

- Conexão de confiabilidade da sessão: Habilitada
- Número da porta de confiabilidade da sessão: 2598

Para obter mais informações, consulte Configurações da política de confiabilidade da sessão.

NetScaler com reconexão automática do cliente e confiabilidade da sessão:

Se as políticas Multistream e Multiport estiverem habilitadas no servidor e qualquer ou todas estas condições forem verdadeiras, a reconexão automática do cliente não funciona:

- A confiabilidade da sessão está desabilitada no NetScaler Gateway.
- Ocorre um failover no appliance NetScaler.
- O NetScaler SD-WAN é usado com o NetScaler Gateway.

Taxa de transferência adaptativa HDX

A taxa de transferência adaptativa HDX ajusta inteligentemente a taxa de transferência máxima da sessão ICA, ajustando os buffers de saída. O número de buffers de saída é inicialmente definido com um valor alto. Esse valor alto permite que os dados sejam transmitidos ao cliente de forma mais rápida e eficiente, especialmente em redes com alta latência. Proporcionar melhor interatividade, transferências de arquivos mais rápidas, reprodução de vídeo mais suave, maior taxa de quadros e resolução resulta em uma experiência de usuário aprimorada.

A interatividade da sessão é constantemente medida para determinar se algum fluxo de dados dentro da sessão ICA está afetando negativamente a interatividade. Se isso ocorrer, a taxa de transferência é diminuída para reduzir o impacto do grande fluxo de dados na sessão e permitir que a interatividade se recupere.

> **Importante:**

> A taxa de transferência adaptativa HDX altera a forma como os buffers de saída são definidos, movendo esse mecanismo do cliente para o VDA, e nenhuma configuração manual é necessária.

> Este recurso tem os seguintes requisitos:

- VDA versão 1811 ou posterior
- Workspace app para Windows 1811 ou posterior

Melhorar a qualidade da imagem enviada para os dispositivos do usuário

As seguintes configurações de política de exibição visual controlam a qualidade das imagens enviadas de desktops virtuais para dispositivos de usuário.

- Qualidade visual. Controla a qualidade visual das imagens exibidas no dispositivo do usuário: média, alta, sempre sem perdas, construir para sem perdas (padrão = média). A qualidade real do vídeo usando a configuração padrão de média depende da largura de banda disponível.
- Taxa de quadros alvo. Especifica o número máximo de quadros por segundo que são enviados do desktop virtual para o dispositivo do usuário (padrão = 30). Para dispositivos com CPUs mais lentas, especificar um valor menor pode melhorar a experiência do usuário. A taxa de quadros máxima suportada por segundo é 60.
- Limite de memória de exibição. Especifica o tamanho máximo do buffer de vídeo para a sessão em kilobytes (padrão = 65536 KB). Para conexões que exigem maior profundidade de cor e resolução mais alta, aumente o limite. Você pode calcular a memória máxima necessária.

> **Observação:**
>
> A configuração **Limite de Memória de Exibição** foi descontinuada. Com essa alteração, a Citrix não limita mais a memória de exibição. Em vez disso, a quantidade mínima de memória necessária é alocada para garantir que o layout de exibição do cliente seja totalmente acomodado.

Melhorar o desempenho da videoconferência

Vários aplicativos populares de videoconferência são otimizados para entrega a partir do Citrix Virtual Apps and Desktops por meio de redirecionamento multimídia (veja, por exemplo, HDX RealTime Optimization Pack). Para aplicativos que não são otimizados, a compactação de vídeo da webcam HDX melhora a eficiência da largura de banda e a tolerância à latência para webcams durante videoconferências em uma sessão. Essa tecnologia transmite o tráfego da webcam por um canal virtual multimídia dedicado. Essa tecnologia usa menos largura de banda em comparação com o suporte de redirecionamento USB isócrono HDX Plug-n-Play e funciona bem em conexões WAN.

Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**. Para evitar que os usuários alternem da compactação de vídeo da webcam HDX,

desative o redirecionamento de dispositivo USB usando as configurações de política em Configurações de política ICA > Configurações de política de dispositivos USB.

A compactação de vídeo da webcam HDX exige que as seguintes configurações de política estejam habilitadas (todas estão habilitadas por padrão).

- Redirecionamento de áudio do cliente
- Redirecionamento de microfone do cliente
- Conferência multimídia

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

Prioridades são atribuídas ao tráfego de rede em várias conexões para uma sessão usando roteadores compatíveis com Qualidade de Serviço. Quatro fluxos TCP e dois fluxos de User Datagram Protocol (UDP) estão disponíveis para transportar o tráfego ICA entre o dispositivo do usuário e o servidor:

- Fluxos TCP - em tempo real, interativo, em segundo plano e em massa
- Fluxos UDP - voz e acesso remoto de exibição Framehawk

Cada canal virtual é associado a uma prioridade específica e transportado na conexão correspondente. Você pode configurar os canais independentemente, com base no número da porta TCP usada para a conexão.

Conexões de streaming de múltiplos canais são suportadas para Virtual Delivery Agents (VDAs) instalados em máquinas Windows 10, Windows 8 e Windows 7. Trabalhe com seu administrador de rede para garantir que as portas do Common Gateway Protocol (CGP) configuradas na configuração **Política de Múltiplas Portas** sejam atribuídas corretamente nos roteadores de rede.

A Qualidade de Serviço é suportada apenas quando várias portas de confiabilidade de sessão, ou as portas CGP, estão configuradas.

> **Aviso:**

> Use segurança de transporte ao usar este recurso. A Citrix recomenda usar Segurança de Protocolo de Internet (IPsec) ou Segurança da Camada de Transporte (TLS). As conexões TLS são suportadas apenas quando as conexões atravessam um NetScaler Gateway que suporta ICA multi-stream. Em uma rede corporativa interna, conexões multi-stream com TLS não são suportadas.

> Para definir a Qualidade de Serviço para múltiplas conexões de streaming, adicione as seguintes configurações de política da Citrix a uma política (consulte Configurações de política de conexões multi-stream para obter detalhes):

- Política Multi-Porta - Esta configuração especifica portas para o tráfego ICA em múltiplas conexões e estabelece prioridades de rede.
  - Selecione uma prioridade na lista de prioridades de porta padrão do CGP. Por padrão, a porta primária (2598) tem prioridade Alta.
  - Digite mais portas CGP em CGP port1, CGP port2 e CGP port3 conforme necessário, e identifique as prioridades para cada uma. Cada porta deve ter uma prioridade única.

  Configure explicitamente os firewalls nos VDAs para permitir o tráfego TCP adicional.
- Configuração de computador Multi-Stream - Esta configuração está desabilitada por padrão. Se você usa Citrix NetScaler SD-WAN com suporte Multi-Stream em seu ambiente, não precisa configurar esta opção. Configure esta configuração de política ao usar roteadores de terceiros ou NetScaler SD-WAN legado para alcançar a Qualidade de Serviço desejada.
- Configuração de usuário Multi-Stream - Esta configuração está desabilitada por padrão.

Para que as políticas que contêm essas configurações entrem em vigor, os usuários devem fazer logoff e, em seguida, logon na rede.

Mostrar ou ocultar a barra de idiomas remota

A barra de idiomas exibe o idioma de entrada preferencial em uma sessão de aplicativo. Se este recurso estiver habilitado (padrão), você pode mostrar ou ocultar a barra de idiomas na interface do usuário **Preferências Avançadas > Barra de idiomas** no aplicativo Citrix Workspace para Windows. Usando uma configuração de registro no lado do VDA, você pode desabilitar o controle do cliente sobre o recurso da barra de idiomas. Se este recurso estiver desabilitado, a configuração da interface do usuário do cliente não terá efeito, e a configuração atual por usuário determinará o estado da barra de idiomas. Para mais informações, consulte Melhorar a experiência do usuário.

Para desabilitar o controle do cliente sobre o recurso da barra de idiomas a partir do VDA:

1. No editor de registro, navegar para HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI.
2. Crie uma chave de valor DWORD, SeamlessFlags, e defina-a como 0x40000.

Mapeamento de teclado Unicode

Os Citrix Receivers que não são Windows usam o layout de teclado local (Unicode). Se um usuário alterar o layout de teclado local e o layout de teclado do servidor (código de varredura), eles podem não estar sincronizados e a saída estará incorreta. Por exemplo, o Usuário1 altera o layout de teclado local de inglês para alemão. O Usuário1 então altera o teclado do lado do servidor para alemão. Mesmo que ambos os layouts de teclado sejam alemães, eles podem não estar sincronizados, causando uma saída de caracteres incorreta.

Habilitar ou desabilitar o mapeamento de layout de teclado Unicode

Por padrão, o recurso está desabilitado no lado do VDA. Para habilitar o recurso, ative-o usando o editor de registro regedit no VDA. Adicione a seguinte chave de registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

Para desabilitar este recurso, defina **EnableKlMap** como 0 ou exclua a chave **CtxKlMap**.

Habilitar o modo compatível de mapeamento de layout de teclado Unicode

Por padrão, o mapeamento de layout de teclado Unicode automaticamente "engancha" (hooks) algumas APIs do Windows para recarregar o novo mapa de layout de teclado Unicode quando você altera o layout de teclado no lado do servidor. Algumas aplicações não podem ser "enganchadas". Para manter a compatibilidade, você pode alterar o recurso para o modo compatível para suportar essas aplicações não "enganchadas". Adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valor: 1

Para usar o mapeamento normal de layout de teclado Unicode, defina **DisableWindowHook** como 0.

Canais virtuais Citrix ICA®

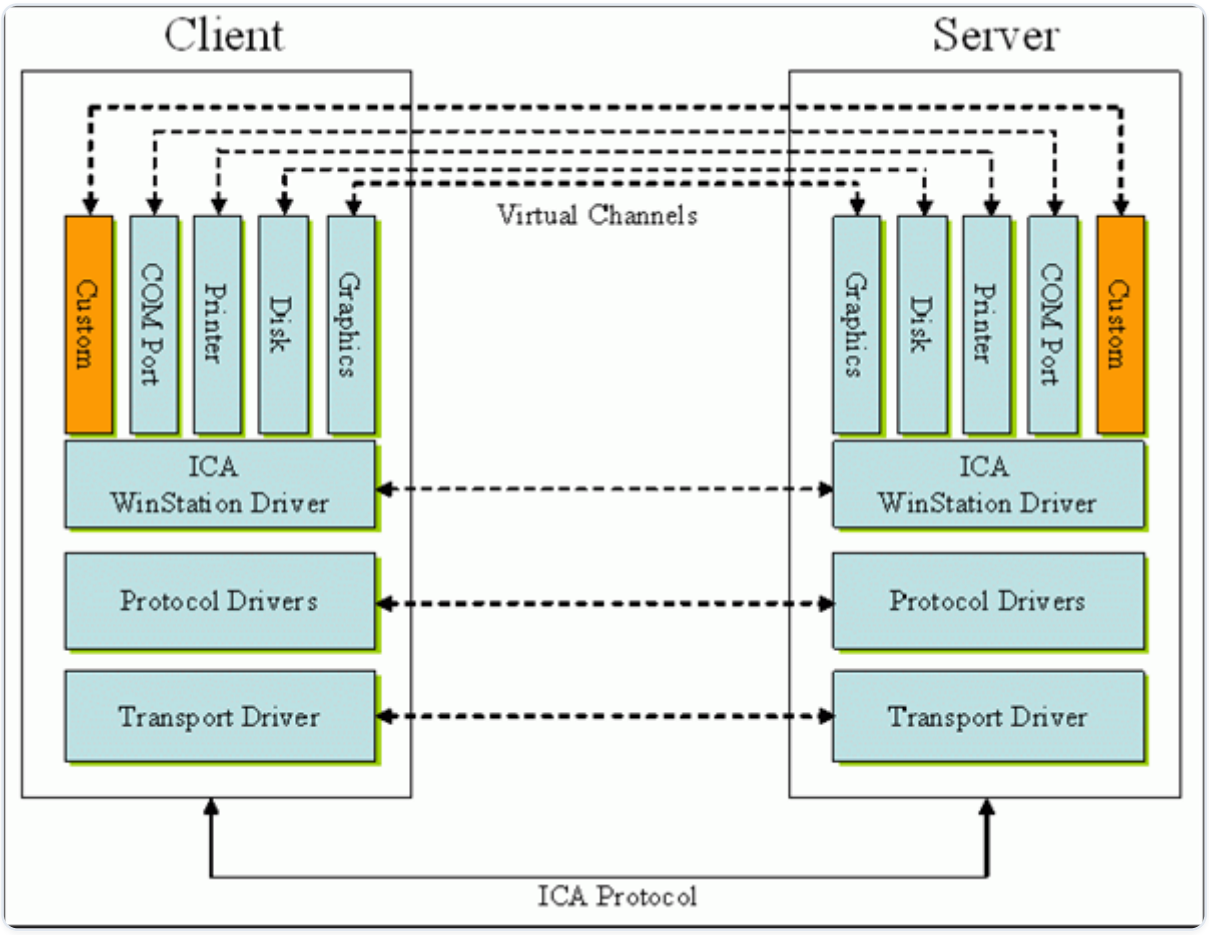
> **Aviso:**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

O que são canais virtuais ICA?

Uma grande parte da funcionalidade e comunicação entre o aplicativo Citrix Workspace™ e os servidores Citrix Virtual Apps and Desktops™ ocorre por meio de canais virtuais. Os canais virtuais são uma parte necessária da experiência de computação remota com os servidores Citrix Virtual Apps and Desktops. Os canais virtuais são usados para:

- Áudio
- Portas COM
- Discos
- Gráficos
- Portas LPT
- Impressoras
- Cartões inteligentes
- Canais virtuais personalizados de terceiros
- Vídeo

Novos canais virtuais são, às vezes, lançados com novas versões dos servidores Citrix Virtual Apps and Desktops e produtos do aplicativo Citrix Workspace para fornecer mais funcionalidade.



Um canal virtual consiste em um driver virtual do lado do cliente que se comunica com um aplicativo do lado do servidor. O Citrix Virtual Apps and Desktops é fornecido com vários canais virtuais incluídos. Eles são projetados para permitir que clientes e fornecedores terceirizados criem seus próprios canais virtuais usando um dos Kits de Desenvolvimento de Software (SDKs) fornecidos.

Os canais virtuais fornecem uma maneira segura de realizar várias tarefas. Por exemplo, um aplicativo que está sendo executado em um servidor Citrix Virtual Apps que se comunica com um dispositivo do lado do cliente ou um aplicativo que se comunica com o ambiente do lado do cliente.

No lado do cliente, os canais virtuais correspondem a drivers virtuais. Cada driver virtual fornece uma função específica. Alguns são necessários para a operação normal, e outros são opcionais. Os drivers virtuais operam no nível do protocolo da camada de apresentação. Pode haver vários protocolos ativos a qualquer momento, multiplexando canais fornecidos pela camada de protocolo 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
- Clipboard
- ClientComm
- ClientAudio
- LicenseHandler (Obrigatório)
- TWI (Obrigatório)
- SmartCard
- ICACTL (Obrigatório)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Observação:**

> Você pode desabilitar funcionalidades específicas do cliente removendo um ou mais desses valores da chave de registro. Por exemplo, se você quiser remover a Área de Transferência do Cliente, remova a palavra **Clipboard**.

> Esta lista contém os arquivos de driver virtual do cliente e suas respectivas funções. O Citrix Virtual Apps e o Citrix Workspace app para Windows usam esses arquivos. Eles estão na forma de Bibliotecas de Vínculo Dinâmico (modo de usuário) e não de drivers do Windows

> (modo kernel), exceto para o USB Genérico, conforme descrito no canal virtual USB Genérico.

- vd3dn.dll – Canal virtual Direct3D usado para redirecionamento de composição da área de trabalho
- vdcamN.dll – Áudio bidirecional
- vdcdm30n.dll – Mapeamento de unidade do cliente
- vdcom30N.dll - Mapeamento de porta COM do cliente
- vdcpm30N.dll – Mapeamento de impressora do cliente
- vdctln.dll – Canal de controles ICA
- vddvc0n.dll – Canal virtual dinâmico
- vdeuemn.dll - Monitoramento da experiência do usuário final
- vdgusbn.dll – Canal virtual USB Genérico
- vdkbhook.dll – Passagem transparente de teclas
- vdlfpn.dll – Canal de exibição Framehawk sobre transporte tipo UDP
- vdmmn.dll – Suporte multimídia
- vdmrvc.dll – Canal virtual do Mobile Receiver
- vdmtchn.dll - Suporte multitoque
- vdscardn.dll – Suporte a smartcard
- vdsens.dll – Canal virtual de sensores
- vdspl30n.dll – UPD do cliente
- vdsspin.dll – Kerberos
- vdtuin.dll – UI transparente
- vdtw30n.dll – Thinwire do cliente
- vdtwin.dll – Seamless
- vdtwn.dll – Twain

Alguns canais virtuais são compilados em outros arquivos. Por exemplo, o Mapeamento da Área de Transferência está disponível em wfica32.exe

Compatibilidade de 64 bits

O aplicativo Citrix Workspace para Windows é compatível com 64 bits. Assim como a maioria dos binários compilados para 32 bits, esses arquivos de cliente têm equivalentes compilados para 64 bits:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Canal virtual USB genérico

A implementação do canal virtual USB genérico usa dois drivers de modo kernel juntamente com o driver de canal virtual vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

Como os canais virtuais ICA funcionam

Os canais virtuais são carregados de várias maneiras. O Shell (WfShell para o servidor e PicaShell para a estação de trabalho) carrega alguns canais virtuais. Alguns canais virtuais são hospedados como serviços do Windows.

Módulos de canal virtual carregados pelo Shell, por exemplo:

- EUEM
- Twain
- Área de Transferência

- Multimídia
- Compartilhamento de sessão contínuo
- Fuso Horário

Alguns são carregados como modo kernel, por exemplo:

- CtxDvcs.sys – Canal virtual dinâmico
- Icausbb.sys – Redirecionamento USB genérico
- Picadm.sys – Mapeamento de unidade cliente
- Picaser.sys – Redirecionamento de porta COM
- Picapar.sys – Redirecionamento de porta LPT

Canal virtual gráfico no lado do servidor

O `ctxgfx.exe` hospeda o canal virtual gráfico para sessões baseadas em estação de trabalho e servidor de terminal. O `Ctxgfx` hospeda módulos específicos da plataforma que interagem com o driver correspondente (`Icardd.dll` para RDSH e `vdod.dll` e `vidd.dll` para estação de trabalho).

Para implantações do XenDesktop® 3D Pro, um driver gráfico OEM é instalado para a GPU correspondente no VDA. `Ctxgfx` carrega módulos adaptadores especializados para interagir com o driver gráfico OEM.

Hospedando canais especializados em serviços do Windows

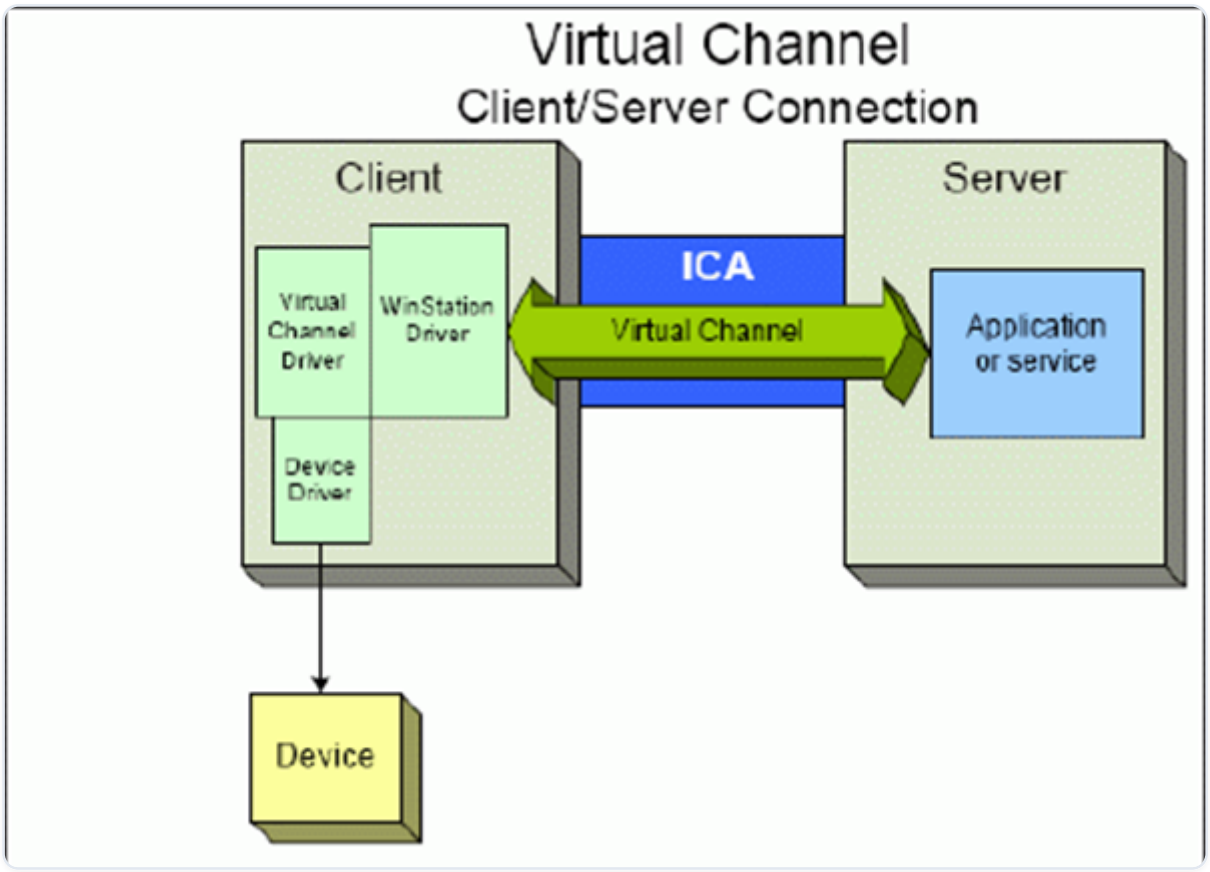
Nos servidores Citrix Virtual Apps and Desktops, vários canais são hospedados como serviços do Windows. Essa hospedagem oferece semântica de um para muitos para vários aplicativos em uma sessão e várias sessões no servidor. Exemplos de tais serviços incluem:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Serviço de Canal Virtual de Localização e Sensor Citrix
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops™ apenas)

- Citrix ICA Status Channel Service

O canal virtual de áudio no Citrix Virtual Apps é hospedado usando o serviço de Áudio do Windows.

No lado do servidor, todos os canais virtuais do cliente são roteados através do driver WinStation, Wdica.sys. No lado do cliente, o driver WinStation correspondente, integrado ao wfica32.exe, pesquisa os canais virtuais do cliente. Esta imagem ilustra a conexão cliente-servidor do canal virtual.



Esta visão geral contém uma troca de dados cliente-servidor usando um canal virtual.

1. O cliente se conecta ao servidor Citrix Virtual Apps and Desktops. O cliente passa informações sobre os canais virtuais que ele suporta para o servidor.
2. O aplicativo do lado do servidor inicia, obtém um manipular para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.
3. O driver virtual do cliente e o aplicativo do lado do servidor passam dados usando os dois métodos a seguir:

    - Se o aplicativo do servidor tiver dados para enviar ao cliente, os dados serão enviados ao cliente imediatamente. Quando o cliente recebe os dados, o driver WinStation

desmultiplexa os dados do canal virtual do fluxo ICA e os passa imediatamente para o driver virtual do cliente.

- Se o driver virtual do cliente tiver dados para enviar ao servidor, os dados serão enviados na próxima vez que o driver WinStation o sondar. Quando o servidor recebe os dados, eles são enfileirados até que o aplicativo do canal virtual os leia. Não há como alertar o aplicativo do canal virtual do servidor de que os dados foram recebidos.

4. Quando o aplicativo do canal virtual do servidor é concluído, ele fecha o canal virtual e libera quaisquer recursos alocados.

Criando seu próprio canal virtual usando o SDK do Canal Virtual

Observação:

Os SDKs da Citrix estão disponíveis no portal do Desenvolvedor Citrix em `<https://developer.cloud.com>`.

A criação de um canal virtual usando o SDK do Canal Virtual requer conhecimento de programação intermediário. Use este método para fornecer um caminho de comunicação principal entre o cliente e o servidor. Por exemplo, se você estiver implementando o uso de um dispositivo no lado do cliente, como um scanner, para ser usado com um processo na sessão.

Observação:

- O SDK do Canal Virtual requer o SDK WFAPI para escrever o lado do servidor do canal virtual.
- Devido à segurança aprimorada para Citrix Virtual Apps and Desktops, você deve especificar quais canais virtuais podem ser abertos em uma sessão ICA. Para obter mais informações, consulte Configurações de política da lista de permissões de canais virtuais.

Criando seu próprio canal virtual usando o SDK do Objeto Cliente ICA

Criar um canal virtual usando o Objeto Cliente ICA (ICO) é mais fácil do que usar o SDK do Canal Virtual. Use o ICO criando um objeto nomeado em seu programa usando o método **CreateChannels**.

> **Importante:**
>
> Devido à segurança aprimorada a partir da versão 10.00 do Citrix Receiver para Windows e posterior (e aplicativos Citrix Workspace para Windows), você deve dar um passo extra ao criar um canal virtual ICO.

Funcionalidade de pass-through de canais virtuais

A maioria dos canais virtuais que a Citrix fornece opera sem modificações quando você usa o aplicativo Citrix Workspace para Windows dentro de uma sessão ICA (também conhecida como sessão de pass-through). Há considerações ao usar o cliente em saltos extras.

As seguintes funções operam da mesma forma em saltos únicos ou múltiplos:

- Mapeamento de porta COM do cliente
- Mapeamento de unidade cliente
- Mapeamento de impressora do cliente
- UPD do cliente
- Monitoramento da experiência do usuário final
- USB genérico
- Kerberos
- Suporte multimídia
- Suporte a smartcard
- Pass-through de chave transparente
- Twain

Devido à natureza inerente da latência e a fatores como compressão e descompressão e renderização sendo realizadas em cada salto, o desempenho pode ser afetado a cada salto adicional que o cliente sofre. As áreas afetadas são:

- Áudio bidirecional

- Transferências de arquivos
- Redirecionamento USB genérico
- Seamless
- Thinwire

> **Importante:**
>
> Por padrão, as unidades de cliente mapeadas por uma instância do cliente em execução em uma sessão de passagem são restritas às unidades de cliente do cliente de conexão.

Funcionalidade de passagem de canais virtuais entre uma sessão do Citrix Virtual Desktop e uma sessão do Citrix Virtual App

A maioria dos canais virtuais fornecidos pela Citrix opera sem modificações quando você usa o aplicativo Citrix Workspace para Windows dentro de uma sessão ICA em um servidor Citrix Virtual Desktops (também conhecida como sessão de passagem).

Especificamente, no servidor Citrix Virtual Desktops, há um hook VDA que executa **picaPassthruHook**. Este hook faz com que o cliente pense que está sendo executado em um servidor CPS, colocando o cliente em seu modo de passagem tradicional.

Oferecemos suporte aos seguintes canais virtuais tradicionais e suas funcionalidades:

- Cliente
- Mapeamento de porta COM do cliente
- Mapeamento de unidade cliente
- Mapeamento de impressora do cliente
- USB genérico (limitado devido ao desempenho)
- Suporte multimídia
- Suporte a smartcard
- SSON
- Passagem transparente de chave

Segurança e canais virtuais ICA

Proteger o uso é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança ao longo deste documento.

Melhores práticas

Abra os canais virtuais ao **Conectar** e **Reconectar**. Feche os canais virtuais ao fazer logoff e **Desconectar**.

Tenha as seguintes diretrizes em mente ao criar scripts que usam funções de canal virtual.

Nomeando os Canais Virtuais:

Você pode criar um máximo de 32 canais virtuais. Dezessete dos 32 canais são reservados para fins especiais.

- Os nomes dos canais virtuais não devem ter mais de sete caracteres.
- Os três primeiros caracteres são reservados para o nome do fornecedor, e os quatro seguintes para o tipo de canal. Por exemplo, **CTXAUD** representa o canal virtual de áudio da Citrix.

Os canais virtuais são referenciados por um nome ASCII de sete caracteres (ou menos). Em algumas versões anteriores do protocolo ICA, os canais virtuais eram numerados. Os números agora são atribuídos dinamicamente com base no nome ASCII, facilitando a implementação. Usuários que estão desenvolvendo código de canal virtual apenas para uso interno podem usar qualquer nome de sete caracteres que não entre em conflito com os canais virtuais existentes. Use apenas números e ASCII maiúsculas e minúsculas. Siga a convenção de nomenclatura existente ao adicionar seus próprios canais virtuais. Existem vários canais predefinidos. Os canais predefinidos começam com o identificador OEM CTX e são para uso exclusivo da Citrix.

Suporte a Double-Hop:

CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
Áudio	Não
Redirecionamento de Conteúdo do Navegador	Não
CDM	Sim
CEIP	Não

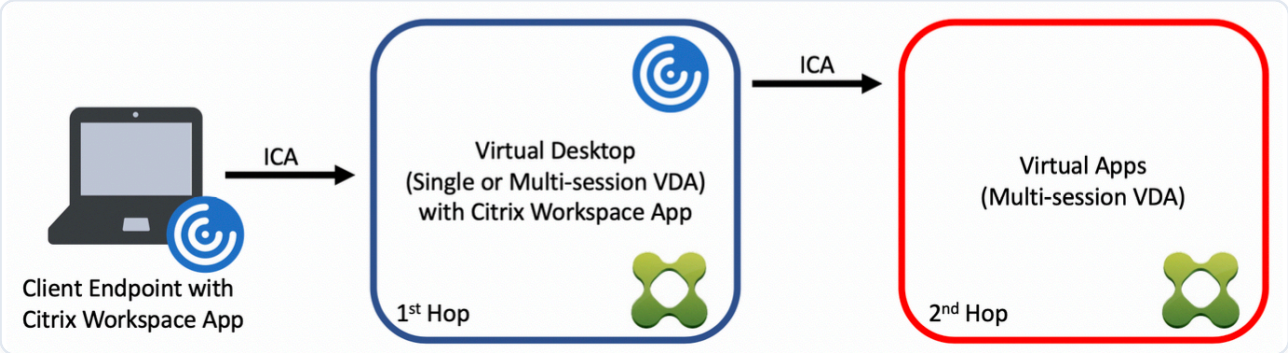
CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
Área de Transferência	Sim
Continuum (MRVC)	Não
VC de Controle	Sim
Redirecionamento de Vídeo HTML5 (v1)	Sim
Teclado, Mouse	Sim
Multitoque	Não
NSAPVC	Não
Impressão	Sim
SensVC	Não
Smartcard	Sim
Twain	Sim
VC USB	Sim
Dispositivos WAYCOM -K2M usando VC USB	Sim
Compressão de Vídeo da Webcam	Sim
Redirecionamento de Mídia do Windows	Sim

Consulte também

- SDK de Canal Virtual ICA
- A Citrix Developer Network é o lar de todos os recursos técnicos e discussões envolvendo o uso de SDKs da Citrix. Nesta rede, você pode encontrar acesso a SDKs, código de exemplo e scripts, extensões e plug-ins, e documentação do SDK. Também estão incluídos os fóruns da Citrix Developer Network, onde discussões técnicas ocorrem sobre cada um dos SDKs da Citrix.

Salto duplo no Citrix Virtual Apps and Desktops™

No contexto de uma sessão de cliente Citrix, o termo “salto duplo” refere-se a uma sessão do Citrix Virtual App que está sendo executada dentro de uma sessão do Citrix Virtual Desktop. O diagrama a seguir ilustra um salto duplo.



Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktop executado em um VDA de SO de sessão única (conhecido como VDI) ou em um VDA de SO de múltiplas sessões (conhecido como desktop publicado), isso é considerado o primeiro salto. Depois que o usuário se conecta ao desktop virtual, o usuário pode iniciar uma sessão do Citrix Virtual Apps™. Isso é considerado o segundo salto.

Você pode usar um modelo de implantação de salto duplo para oferecer suporte a vários casos de uso. O caso em que os ambientes Citrix Virtual Desktop 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 Virtual Apps and Desktops, incluindo o serviço Citrix Cloud™, suportam salto duplo.

O primeiro salto deve usar uma versão compatível do VDA de SO de sessão única ou de múltiplas sessões e do Citrix Workspace App. O segundo salto deve usar uma versão compatível do VDA de SO de múltiplas sessões. Consulte a página Matriz de Produtos para ver as versões compatíveis.

Para melhor desempenho e compatibilidade, a Citrix recomenda usar um cliente Citrix da mesma versão ou mais recente do que as versões do VDA em uso.

Em ambientes onde o primeiro salto envolve uma solução de desktop virtual de terceiros (não Citrix) em combinação com uma sessão do Citrix Virtual Apps, o suporte é limitado ao ambiente do Citrix Virtual Apps. No caso de quaisquer problemas relacionados ao desktop virtual de terceiros, incluindo — mas não se limitando a — compatibilidade do aplicativo Citrix Workspace™,

redirecionamento de dispositivos de hardware e desempenho da sessão, a Citrix pode fornecer suporte técnico em capacidade limitada. Um Citrix Virtual Desktop no primeiro salto pode ser necessário como parte da solução de problemas.

Considerações de implantação para HDX™ em salto duplo

Em geral, cada sessão em um salto duplo é única e as funções cliente-servidor são isoladas para um determinado salto. Esta seção inclui áreas que exigem consideração especial pelos administradores Citrix. A Citrix recomenda que os clientes realizem testes completos dos recursos HDX necessários para garantir que a experiência do usuário e o desempenho sejam adequados para uma determinada configuração de ambiente.

Gráficos

Use as configurações gráficas padrão (codificação seletiva) nos primeiros e segundos saltos. No caso do HDX 3D Pro, a Citrix recomenda fortemente que todos os aplicativos que exigem aceleração gráfica sejam executados localmente no primeiro salto com os recursos de GPU apropriados disponíveis para o VDA.

Latência

A latência de ponta a ponta pode impactar a experiência geral do usuário. Considere a latência adicionada entre o primeiro e o segundo saltos. Isso é especialmente importante com o redirecionamento de dispositivos de hardware.

Multimídia

A renderização de conteúdo de áudio e vídeo no lado do servidor (na sessão) tem o melhor desempenho no primeiro salto. A reprodução de vídeo no segundo salto requer decodificação e recodificação no primeiro salto, aumentando o uso de largura de banda e recursos de hardware como resultado. O conteúdo de áudio e vídeo deve ser limitado ao primeiro salto sempre que possível.

Redirecionamento de dispositivo USB

O HDX inclui modos de redirecionamento genéricos e otimizados para suportar uma ampla gama de tipos de dispositivos USB. Preste atenção especial ao modo em uso em cada salto e use a tabela a seguir como referência para obter os melhores resultados. Para obter mais informações sobre os modos de redirecionamento genéricos e otimizados, consulte Dispositivos USB genéricos.

PRIMEIRO SALTO (VDI OU ÁREA DE TRABALHO PUBLICADA)	SEGUNDO SALTO (APLICATIVOS VIRTUAIS)	NOTAS DE SUPORTE
Otimizado	Otimizado	Recomendado (com base no suporte ao dispositivo). Por exemplo, armazenamento em massa USB, scanners TWAIN, webcam, áudio.
Genérico	Genérico	Para dispositivos onde a opção otimizada não está disponível.
Genérico	Otimizado	Embora tecnicamente possível, recomenda-se usar o modo otimizado em ambos os saltos quando o suporte ao dispositivo estiver disponível.
Otimizado	Genérico	Não suportado

Observação:

Devido à verbosidade inerente dos protocolos USB, o desempenho pode diminuir entre os saltos. A funcionalidade e os resultados variam dependendo dos requisitos específicos do dispositivo e do aplicativo. O teste de validação é altamente recomendado em todos os casos de redirecionamento de dispositivo e especialmente importante em cenários de salto duplo.

Exceções de suporte

As sessões de salto duplo suportam a maioria dos recursos e capacidades HDX, exceto pelos seguintes:

- Redirecionamento de conteúdo do navegador(/pt-br/citrix-virtual-apps-desktops/2407/multimedia/browser-content-redirection.html)
- Acesso a Aplicativos Locais

- Pacote de Otimização em Tempo Real para Skype for Business
- Otimização para Microsoft Teams

Instalar e configurar

Revise os artigos referenciados antes de iniciar cada etapa de implantação, para saber o que você verá e especificará durante a implantação.

Use a seguinte sequência para implantar o Citrix Virtual Apps and Desktops.

Preparar

Revise Preparar para instalar e conclua todas as tarefas necessárias.

- Onde encontrar informações sobre conceitos, recursos, diferenças em relação a versões anteriores, requisitos de sistema e bancos de dados.
- Considerações ao decidir onde instalar os componentes principais.
- Requisitos de permissão e do Active Directory.
- Informações sobre os instaladores, ferramentas e interfaces disponíveis.

Instalar componentes principais

Instale o Delivery Controller, Web Studio, Citrix Director e Citrix License Server. Você também pode instalar o Citrix StoreFront. Para obter detalhes, consulte Instalar componentes principais ou Instalar usando a linha de comando.

Criar um site

Depois de instalar os componentes principais e iniciar o Studio, você será solicitado a criar um site.

Instalar um ou mais Virtual Delivery Agents (VDAs)

Instale um VDA em uma máquina executando um sistema operacional Windows, seja em uma imagem mestre ou diretamente em cada máquina. Consulte Instalar VDAs ou Instalar usando a linha de comando. Scripts de exemplo são fornecidos se você quiser instalar VDAs através do Active Directory.

Para máquinas com sistema operacional Linux, siga as orientações em Linux Virtual Delivery Agent.

Para uma implantação de Acesso Remoto a PC, instale um VDA para um SO de sessão única em cada PC de escritório. Se você precisar apenas dos serviços VDA principais, use o instalador autônomo `VDAWorkstationCoreSetup.exe` e seus métodos existentes de Distribuição Eletrônica de Software (ESD). (Prepare-se para instalar descreve os instaladores VDA disponíveis.)

Instalar componentes opcionais

Se você planeja usar o Citrix Universal Print Server, instale seu componente de servidor em seus servidores de impressão. Consulte Instalar componentes principais ou Instalar usando a linha de comando.

Para permitir que o StoreFront use opções de autenticação como asserções SAML, instale o Citrix Federated Authentication Service.

Para permitir que os usuários finais tenham maior controle sobre suas contas de usuário, instale o Self-Service Password Reset.

Opcionalmente, integre mais componentes Citrix à sua implantação do Citrix Virtual Apps and Desktops.

- Citrix Provisioning é um componente opcional que provisiona máquinas transmitindo uma imagem mestre para dispositivos de destino.
- Citrix Gateway é uma solução segura de acesso a aplicativos que fornece aos administradores políticas granulares de nível de aplicativo e controles de ação para proteger o acesso a aplicativos e dados.
- Citrix SD-WAN é um conjunto de appliances que otimizam o desempenho da WAN.

Criar um catálogo de máquinas

Depois de criar um site no Studio, você será guiado para criar um catálogo de máquinas.

Um catálogo pode conter máquinas físicas ou virtuais (VMs). As máquinas virtuais podem ser criadas a partir de uma imagem mestre. Ao usar um hipervisor ou outro serviço para fornecer VMs, você primeiro cria uma imagem mestre nesse host. Em seguida, ao criar o catálogo, você especifica essa imagem, que é usada ao criar VMs.

Criar um grupo de entrega

Depois de criar seu primeiro catálogo de máquinas no Web Studio, você será guiado para criar um grupo de entrega.

Um grupo de entrega especifica quais usuários podem acessar máquinas em um catálogo selecionado e os aplicativos disponíveis para esses usuários.

Criar um grupo de aplicativos (opcional)

Depois de criar um grupo de entrega, você pode opcionalmente criar um grupo 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 dos grupos de entrega.

Limitação conhecida

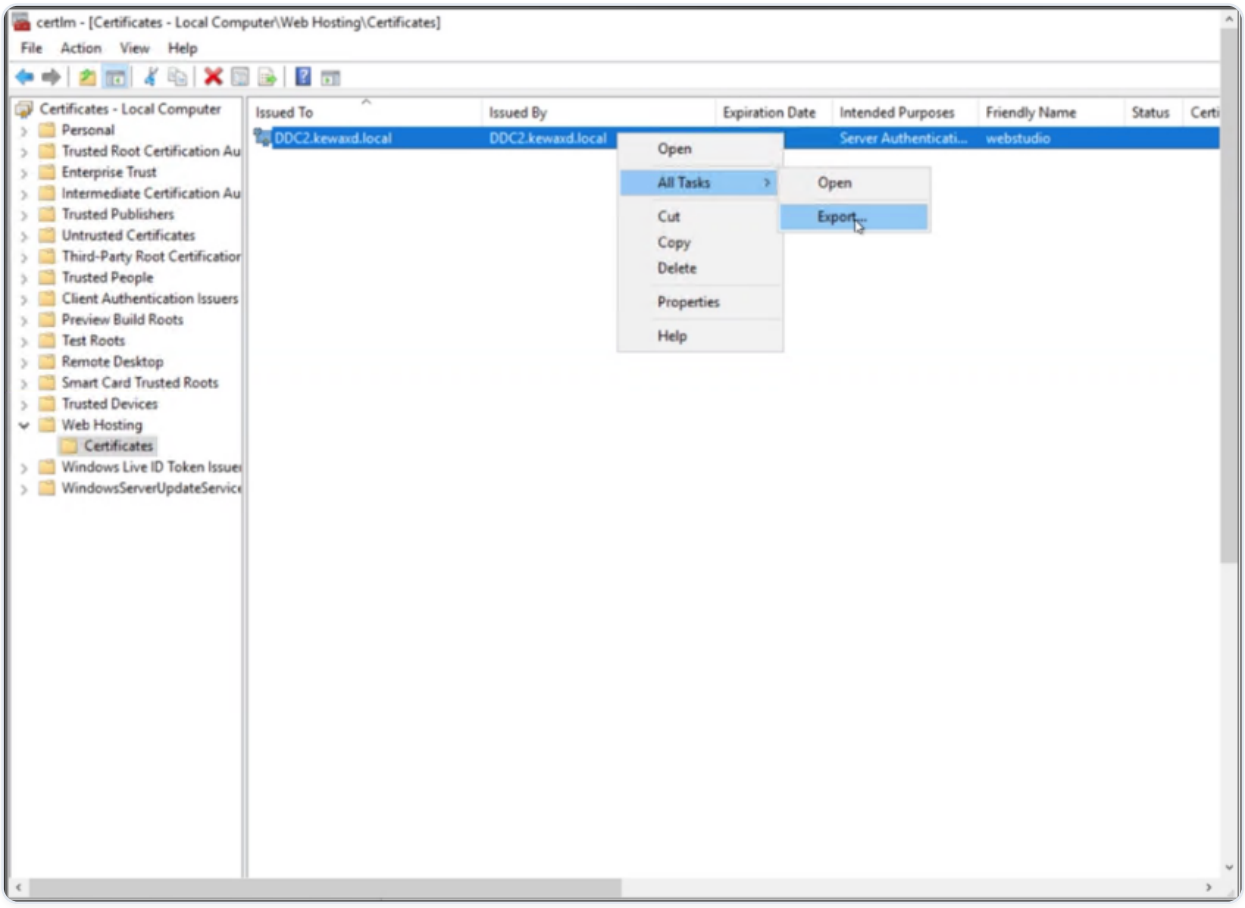
Ao usar o aplicativo Citrix Workspace™ para Windows versão 1912 ou anterior, a sessão é encerrada após um tempo. Esse problema foi corrigido nas versões LTSR e CR mais recentes do aplicativo Citrix Workspace. Para obter mais informações sobre as versões de lançamento suportadas, consulte Citrix Workspace app for Windows / Citrix Receiver for Windows Long Term Service Releases.

Proteger uma implantação do Web Studio (opcional)

Quando você instala o Web Studio junto com um Delivery Controller™, o instalador cria um certificado autoassinado, vinculado à porta `443` do servidor atual. O Web Studio e o Delivery Controller usarão o certificado como certificado TLS. Ao acessar de uma máquina diferente, você pode não conseguir acessar o Web Studio ou pode ver um erro na tela de logon do Web Studio.

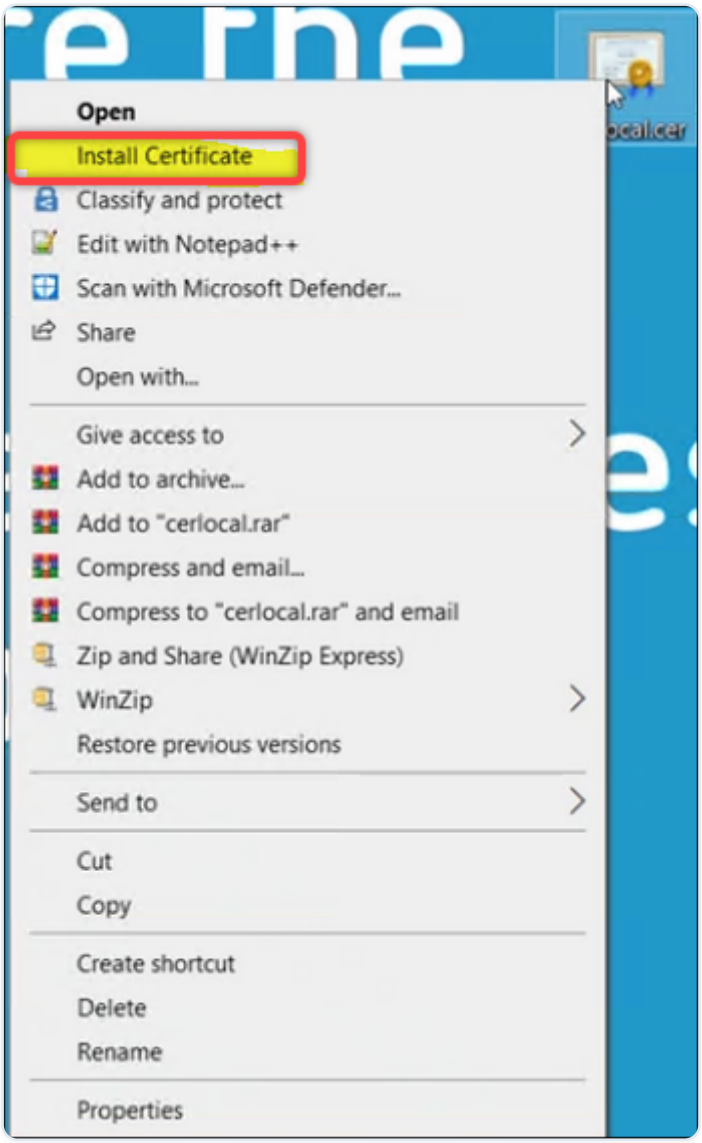
Se você quiser acessar o Web Studio de uma máquina diferente, pode fazer o seguinte:

1. Exporte o certificado autoassinado do Delivery Controller.



- Para **Exportar Chave Privada**, selecione **Não, não exportar a chave privada**.
- Para **Formato de Arquivo de Exportação**, selecione **X.509 binário codificado em DER (.CER)**.

2. Vá para a máquina onde você deseja acessar o Web Studio e, em seguida, instale o certificado.



- Para **Local de Armazenamento**, selecione **Máquina Local**.

Se você optar por instalar o Web Studio em um servidor dedicado que esteja remoto do Delivery Controller, precisará executar duas tarefas:

- **Tarefa 1**: Exporte os certificados do servidor Web Studio e do Delivery Controller, respectivamente.
- **Tarefa 2**: Instale os dois certificados na máquina onde você deseja acessar o Web Studio.

> **Observação:**
>
> Como prática recomendada, recomendamos que você proteja sua implantação do Web Studio usando um certificado de confiança pública externo ou um certificado de uma CA corporativa.

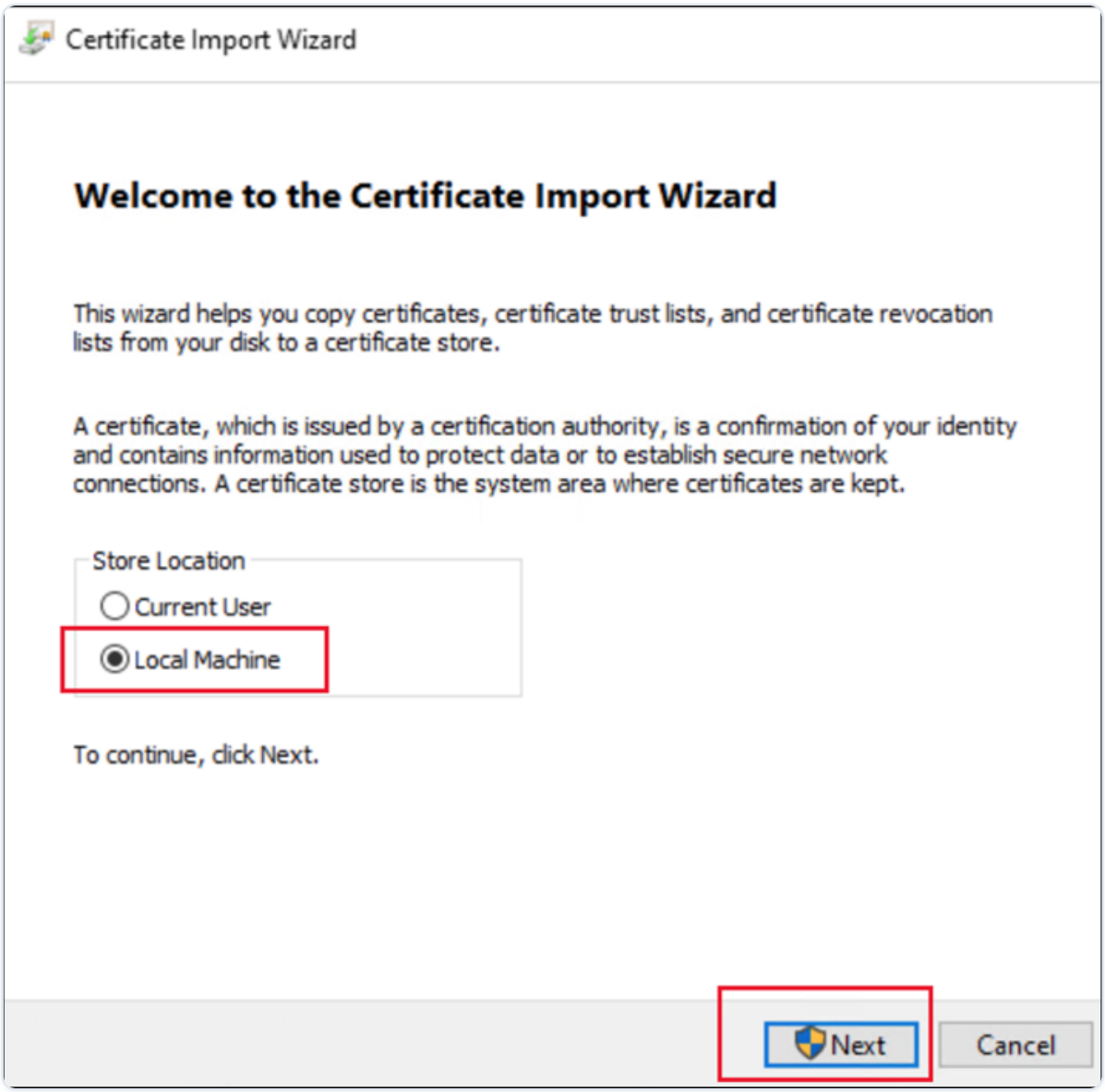
Usar um certificado de confiança pública externo

Você pode importar um certificado de confiança pública externo para o servidor Web Studio usando qualquer um dos três métodos a seguir:

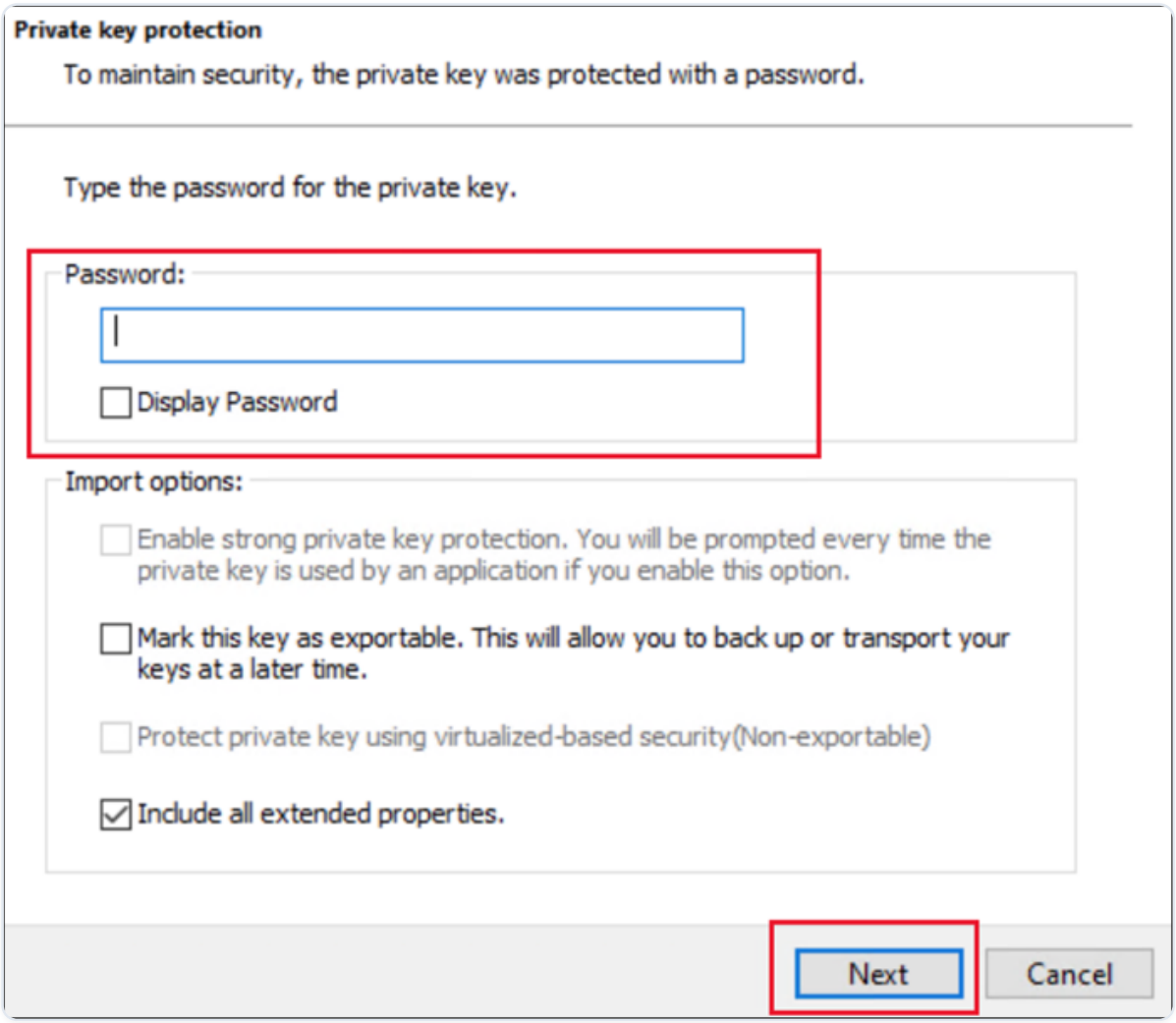
- **Instalar o arquivo PFX**.

  a. Clique duas vezes no arquivo PFX.

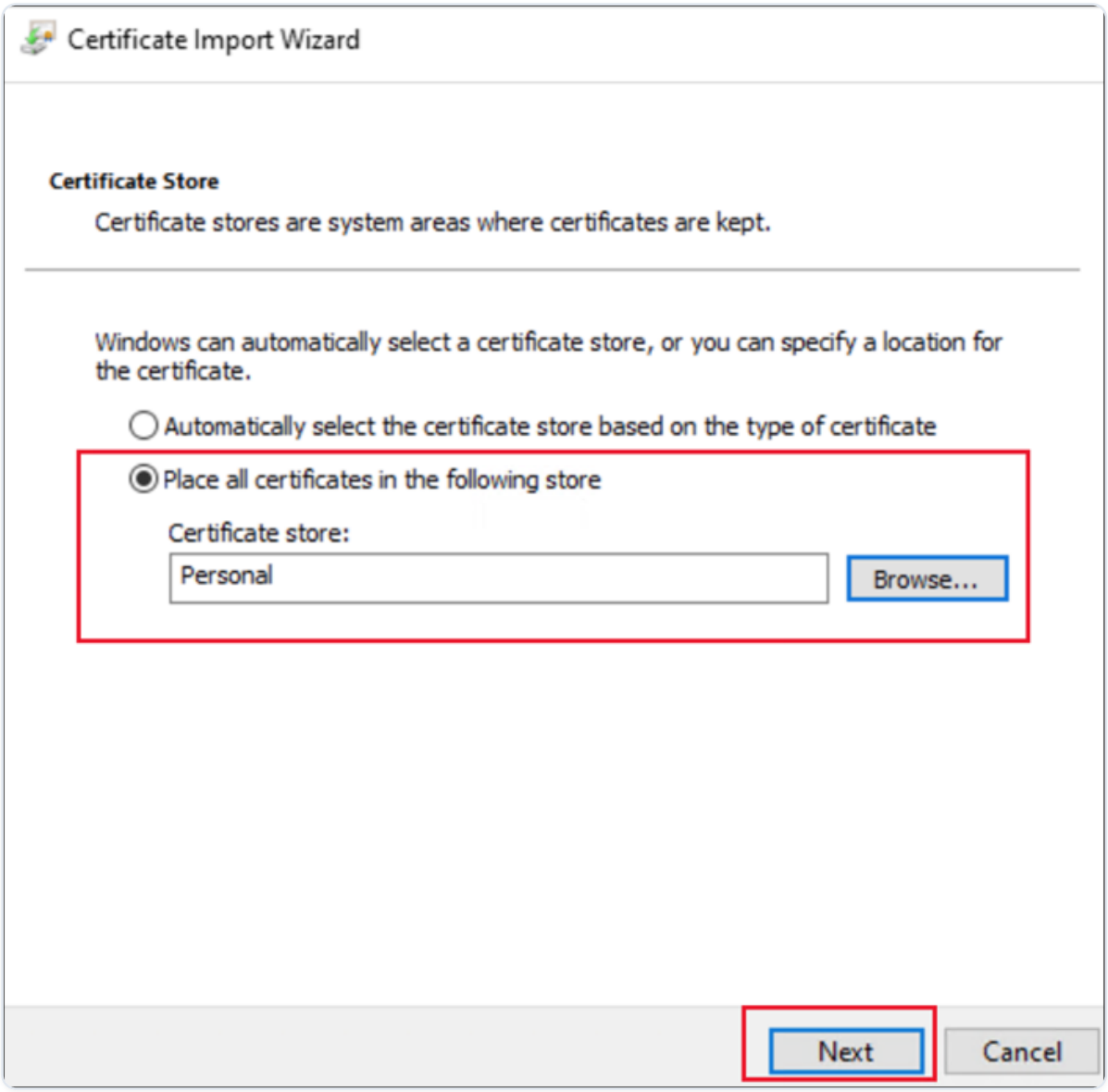
  b. Para **Local do Repositório**, selecione **Máquina Local**.



  c. Insira a senha, se necessário.

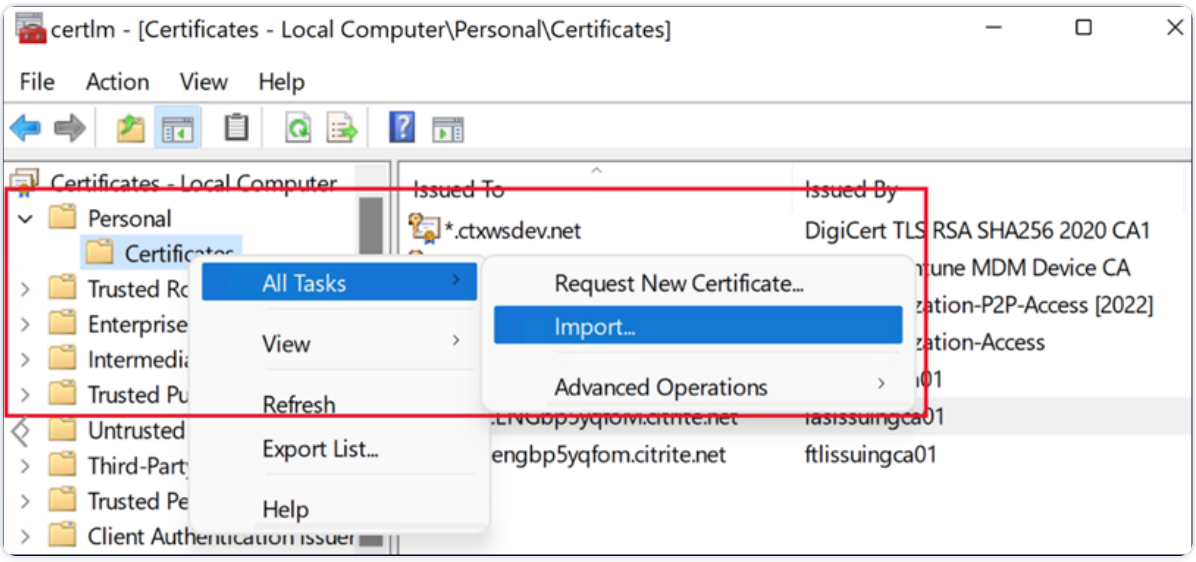


d. Para **Repositório de Certificados**, selecione **Pessoal**.



- **Usar o console Gerenciar certificados do computador**.

  a. Abra o console Gerenciar Certificados do Computador e vá para **Pessoal > Certificados > Todas as Tarefas > Importar**.



b. Selecione o arquivo PFX e insira a senha, se necessário.

- **Usar o PowerShell**.

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String
"123456" -AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\
-FilePath .\Desktop\certificate.pfx
```

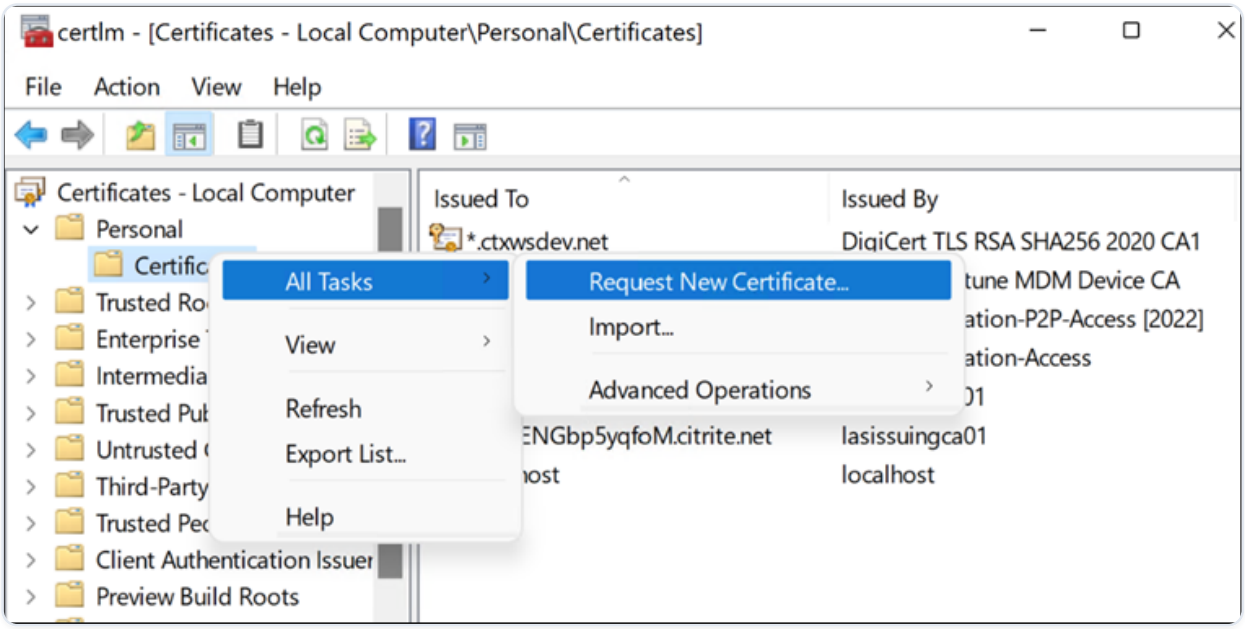
Em seguida, você vincula o certificado à porta `443`. Você pode fazer isso antes da instalação ou atualização, ou após a instalação ou atualização. O instalador não faz nada se a vinculação do certificado estiver configurada para a porta `443`. Para obter mais informações, consulte Antes da instalação ou atualização.

Usar um certificado de uma CA corporativa

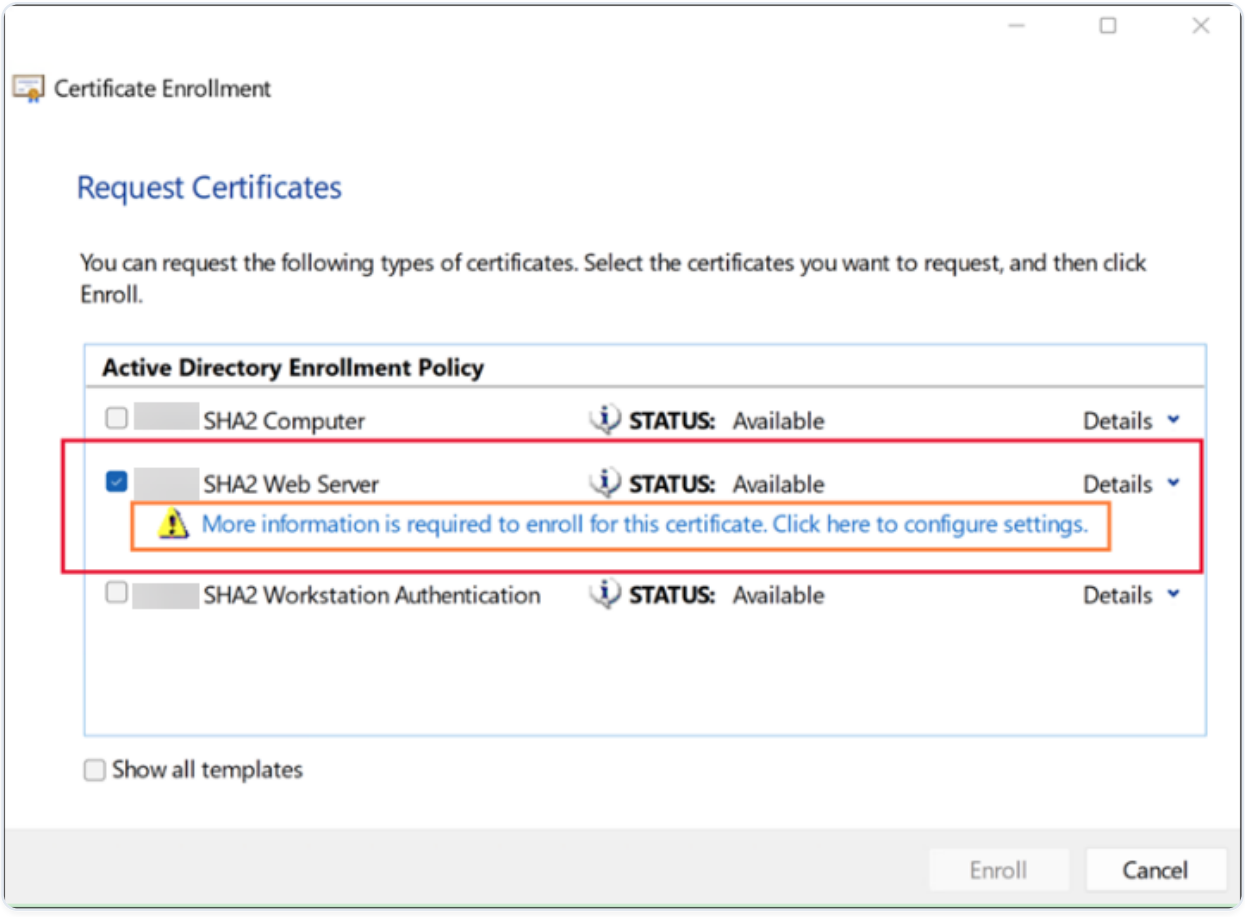
Antes de começar, certifique-se de ter o servidor da Autoridade de Certificação (CA) corporativa implantado em seu domínio.

Para solicitar um certificado, execute as seguintes etapas:

1. No servidor, abra o console **Gerenciar Certificados do Computador**.
2. Vá para **Pessoal > Certificados > Todas as Tarefas > Solicitar Novo Certificado**.



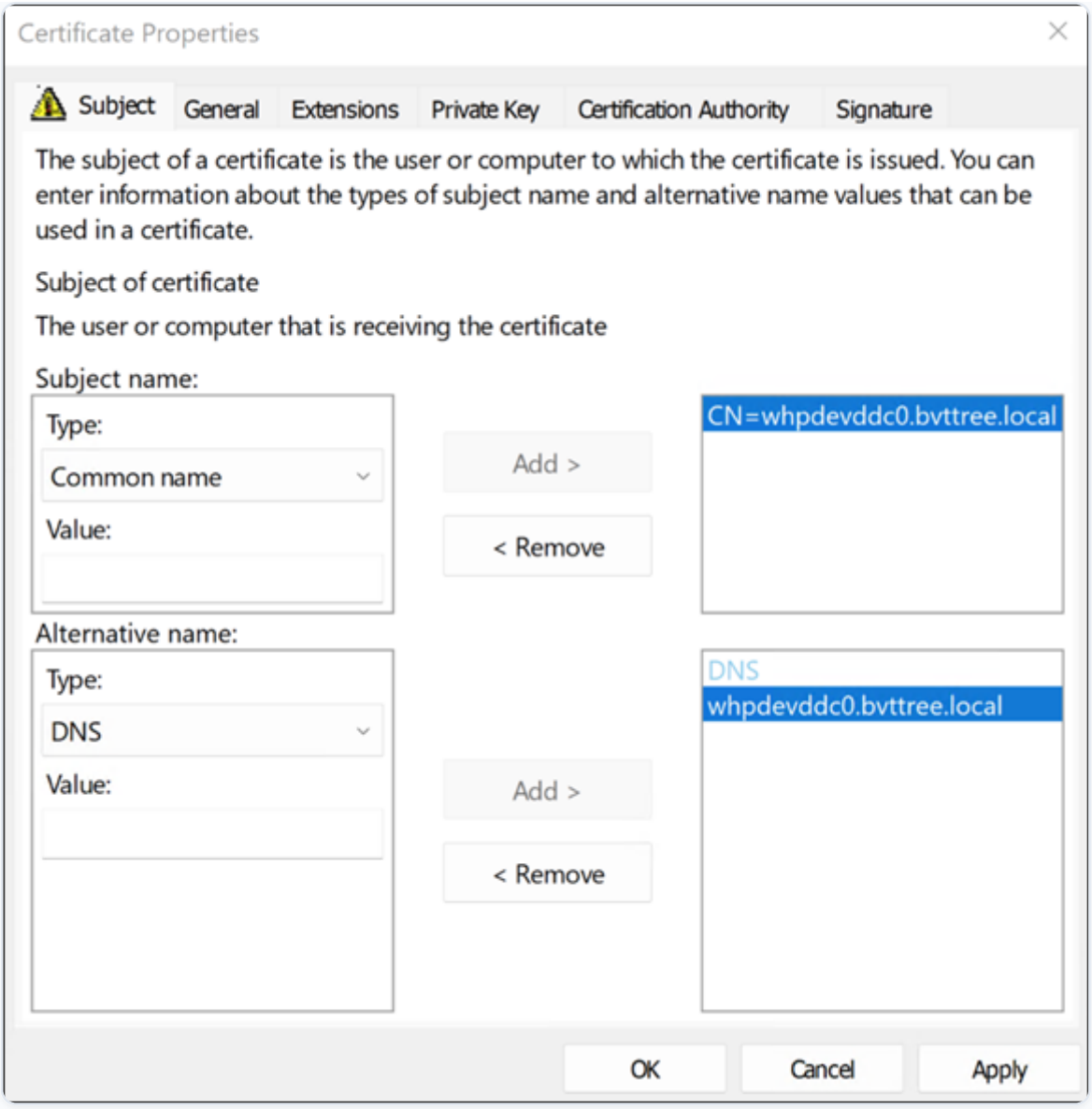
3. Vá para **Registro de Certificado**, selecione o Servidor Web e clique na mensagem de aviso para preencher as informações necessárias.



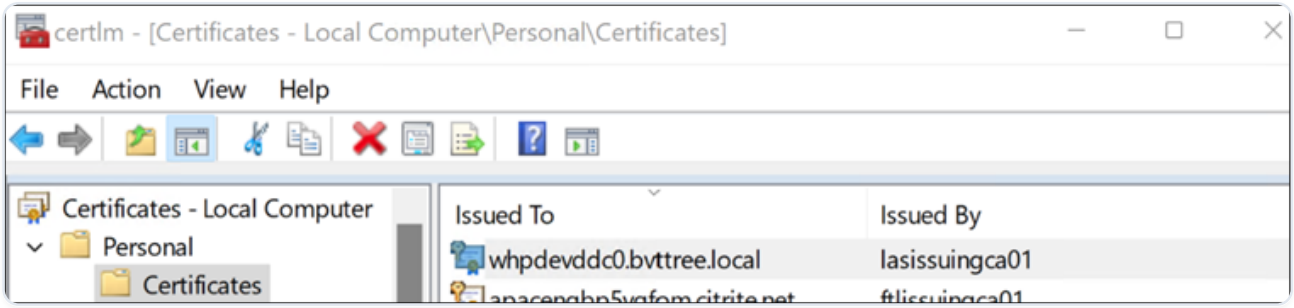
4. Selecione **Nome comum** como o tipo de nome do assunto e insira seu FQDN ou DNS. Além disso, insira o nome alternativo.

> **Observação:**

> Se você precisar de um certificado curinga, poderá inserir `CN=*.bvttree.local` para o nome do assunto e `*.bvttree.local and bvttree.local` para o nome DNS alternativo.



O certificado está disponível em **Pessoal > Certificados**.

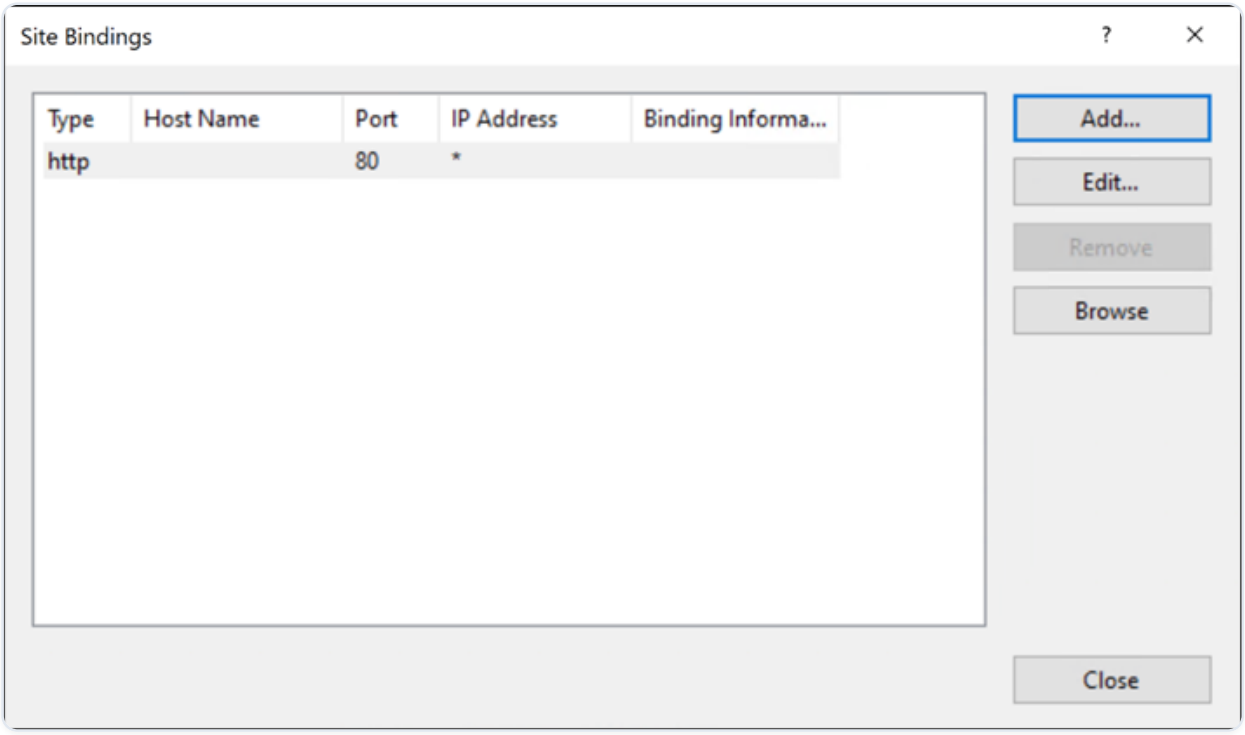


Em seguida, você vincula o certificado à porta `443`. Você pode fazer isso antes da instalação ou atualização, ou após a instalação ou atualização. O instalador não faz nada se a vinculação do certificado estiver configurada para a porta `443`.

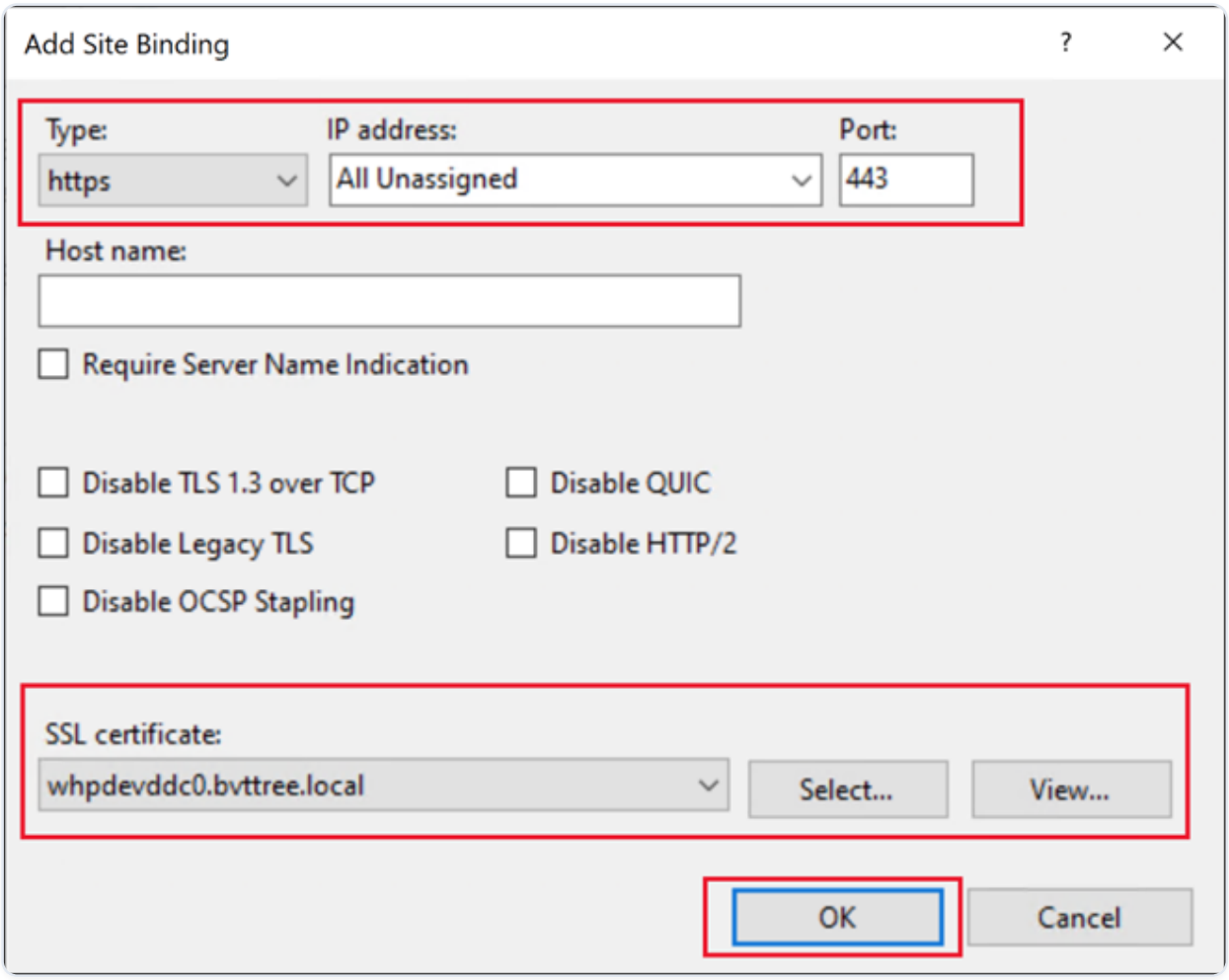
Antes da instalação ou atualização

Para vincular o certificado à porta `443`, execute as seguintes etapas (desde que a vinculação do certificado ainda não esteja configurada para `443` e o IIS esteja habilitado no servidor):

1. Faça logon no servidor do Web Studio como administrador.
2. Abra o Gerenciador do IIS, navegue até **Sites > Default Web Site > Bindings**.
3. Em **Site Bindings**, clique em **Adicionar**.



4. Em **Adicionar Associação de Site**, defina o tipo como `https` e a porta como 443, selecione o certificado SSL que você solicitou da CA e, em seguida, clique em **OK**.



Depois de instalar o Web Studio, o Web Studio e o Delivery Controller são configurados automaticamente para usar o certificado para proteger as conexões.

Alternativamente, você pode alterar o certificado usando o PowerShell.

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="$($(New-
Guid).ToString("B"))"
```

Após a instalação ou atualização

Vá para o servidor Web Studio e altere o certificado usando o Gerenciador do IIS.

Alternativamente, você pode alterar o certificado usando o PowerShell.

```
$certSName = 'CN=whpdevddc0.bvttree.local' # The Enterprise CA certificate
subject.

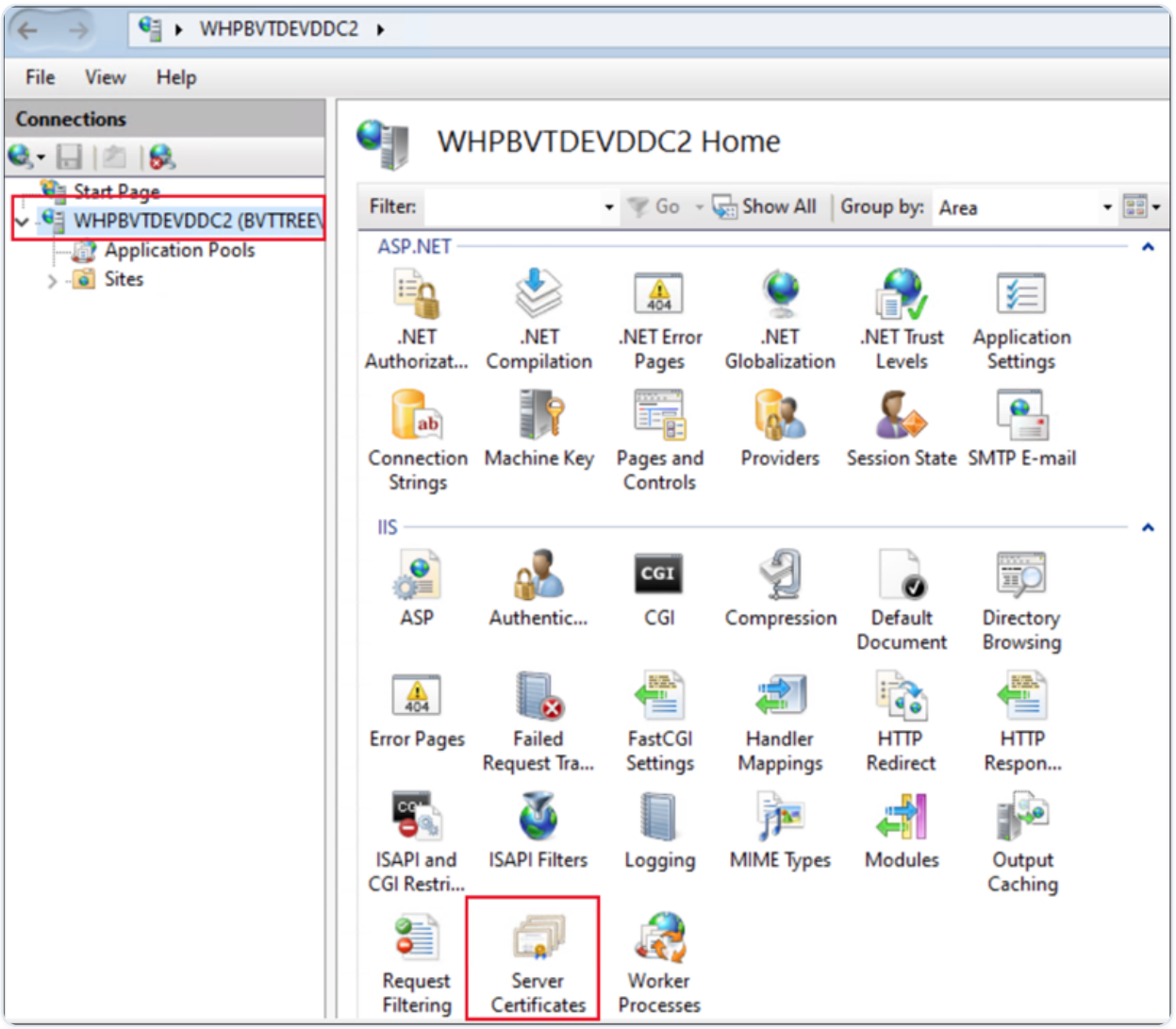
$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http update sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint)
```

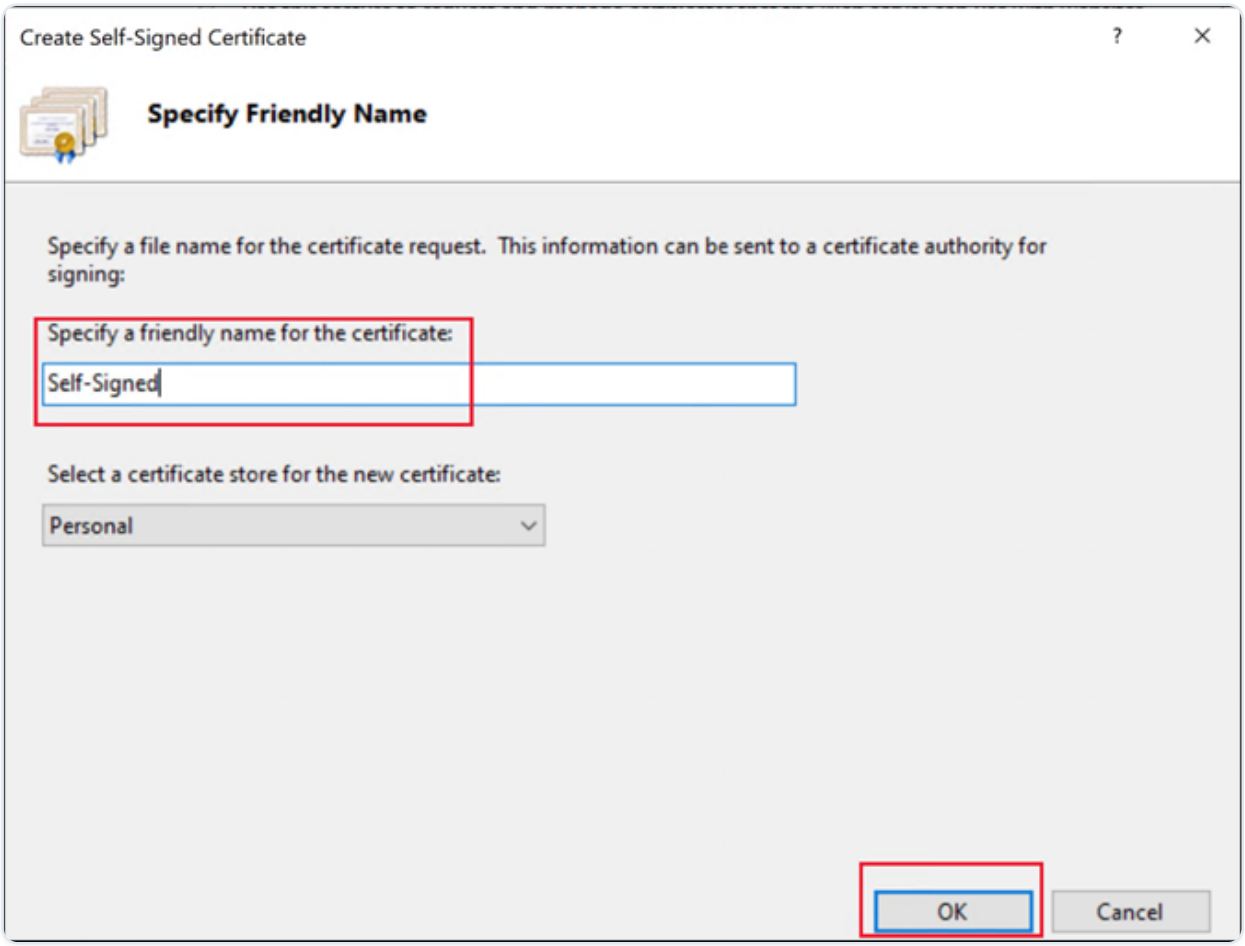
Usar um novo certificado autoassinado

Você pode gerar um novo certificado autoassinado e usá-lo para substituir o existente. Execute as seguintes etapas:

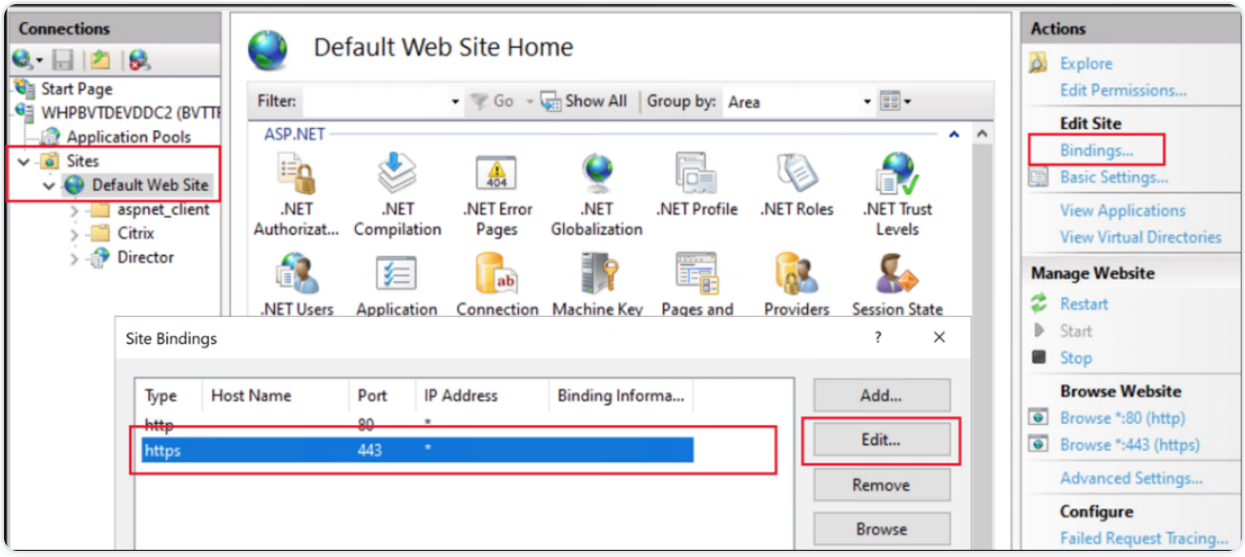
1. Faça logon no servidor Web Studio como administrador.
2. Abra o Gerenciador do IIS, navegue até **Certificados de Servidor** e selecione **Criar Certificado Autoassinado** no painel **Ações**.



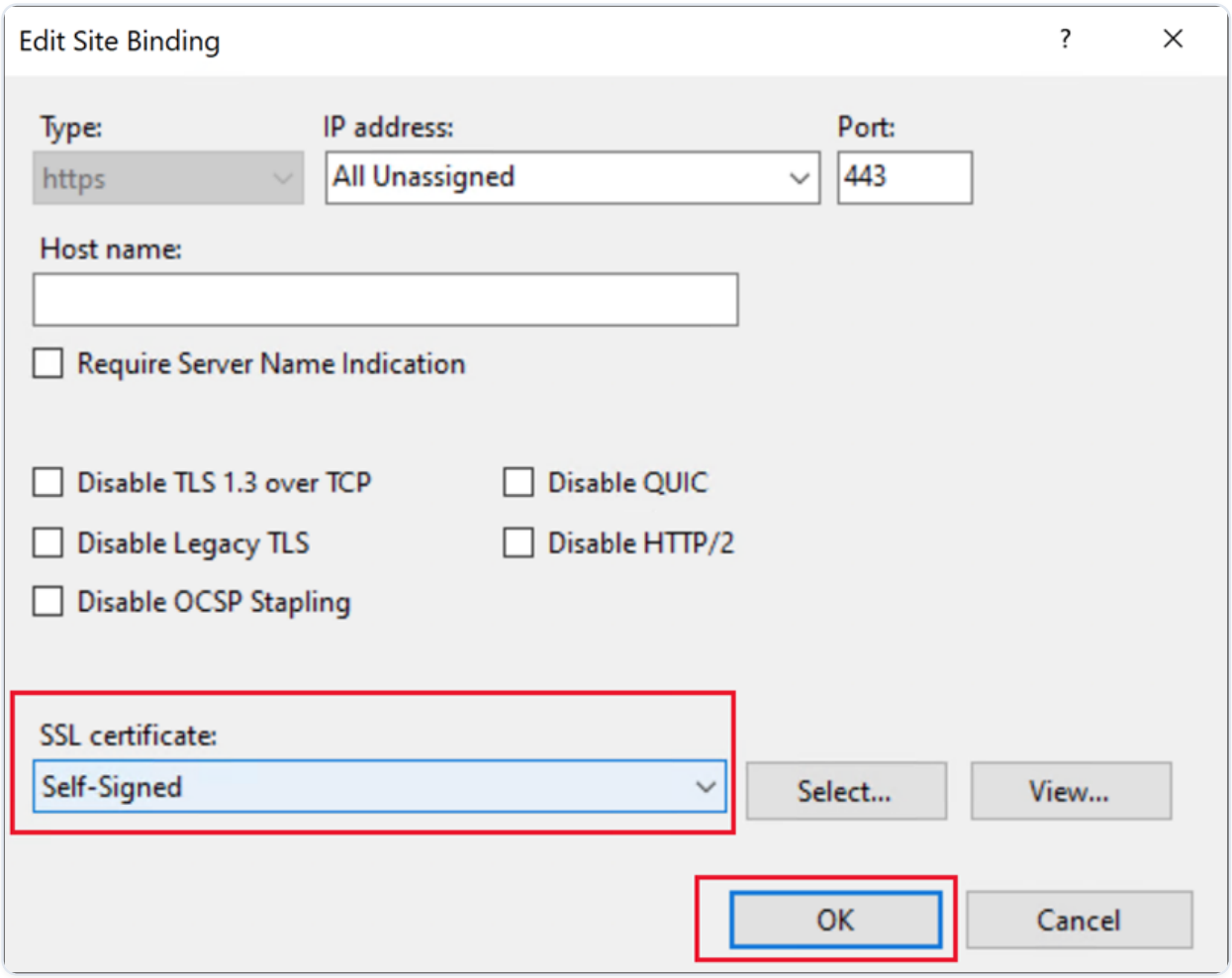
3. Em **Criar Certificado Autoassinado**, insira um nome para o certificado e clique em **OK**. O certificado autoassinado é então criado.



4. Navegue até **Sites > Default Web Site**, selecione **Associações** no painel **Ações**, selecione a entrada `https` e selecione **Editar**.



5. Em **Editar Associação do Site**, selecione o certificado da lista e clique em **OK**.



Isso conclui a alteração do certificado.

Alternativamente, você pode alterar o certificado usando o PowerShell.

```
$certSubject = "CN=WHPBVTDEVDDC2.BVTTREE.LOCAL" # The FQDN of the server.

$frindlyName = "Self-Signed-3"

$expireYears = 5



## new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $frindlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))
```

```
Remove-Item -Path $Env:TEMP\tempCertificate.cer -Force -ErrorAction
SilentlyContinue



## Import this certificate into LocalMachine\Root to let this OS trust
this certificate

Export-Certificate -Type CERT -Force -Cert $certificate -FilePath
$Env:TEMP\tempCertificate.cer -NoClobber

Import-Certificate -FilePath $Env:TEMP\tempCertificate.cer
-CertStoreLocation "Cert:\LocalMachine\Root\"



## Update bind the 0.0.0.0:443 with this certificate

Invoke-Command -ScriptBlock { Param ($param1) netsh http update sslcert
ipport=0.0.0.0:443 certhash=$param1 } -ArgumentList
@($certificate.Thumbprint)
```

Configurar autenticação de cartão inteligente para Web Studio

Este artigo descreve as etapas necessárias para configurar e habilitar a autenticação de cartão inteligente para o Web Studio:

Etapa 1: Instalar o driver do cartão inteligente

Etapa 2: Emitir certificados para usuários de cartão inteligente

Etapa 3: Registrar certificados para usuários de cartão inteligente

Etapa 4: Configurar servidores IIS do Web Studio

Etapa 5 (Opcional): Configurar delegações de autenticação para o Web Studio

Etapa 6: Habilitar autenticação de cartão inteligente para o Web Studio

> **Observação:**

> A autenticação de cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory que os servidores do Web Studio.

Etapa 1: Instalar o driver do cartão inteligente

Instale o driver do cartão inteligente nas seguintes máquinas:

- Controladores de Domínio onde o Serviço de Certificado está instalado.
- Servidores do Web Studio
- Máquinas que os usuários finais usam para acessar o Web Studio
- Máquinas que você usa para registrar certificados para usuários de cartão inteligente

Os drivers de smart card variam de acordo com os fornecedores. Por exemplo, se estiver usando hardware de smart card fornecido pela ITS, baixe os drivers SaftNet em `<https://support.globalsign.com/ssl/ssl-certificates-installation/safenet-drivers>`.

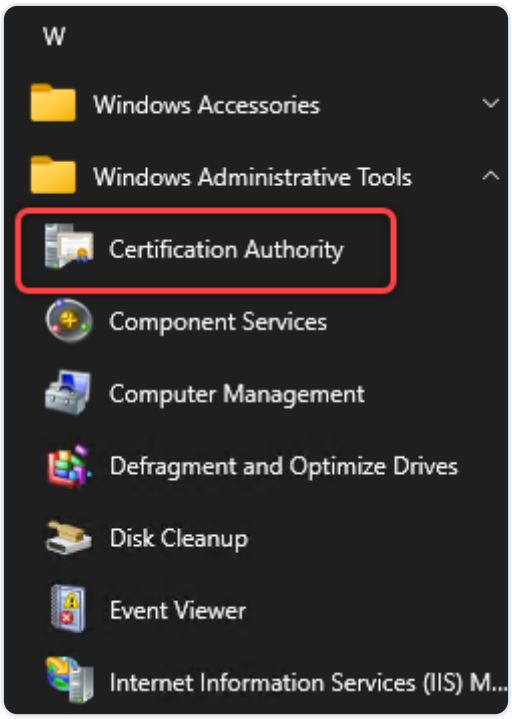
Etapa 2: Emitir certificados para usuários de smart card

> **Observação:**

> As etapas a seguir são fornecidas como um exemplo para guiá-lo através do processo.

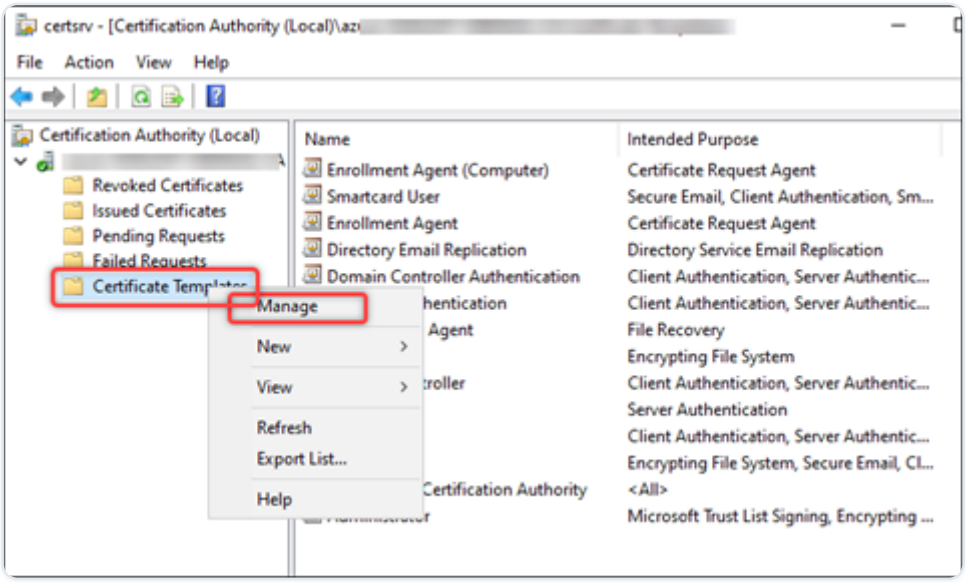
> No seu Controlador de Domínio, siga estas etapas para concluir a tarefa:

1. Acesse seu Controlador de Domínio e abra **Autoridade de Certificação**.



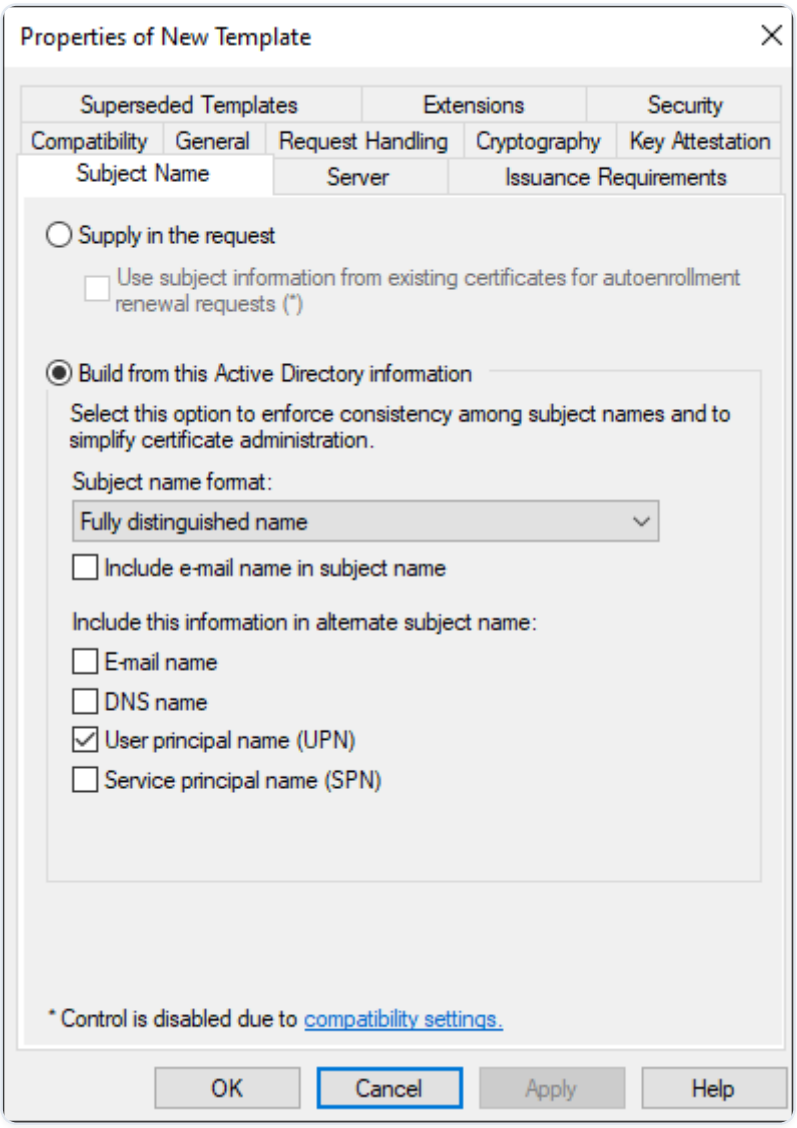
2. Duplique o modelo **Agente de Registro**. As etapas detalhadas são as seguintes:

   a. Clique com o botão direito em **Modelos de Certificado** e selecione **Gerenciar**.

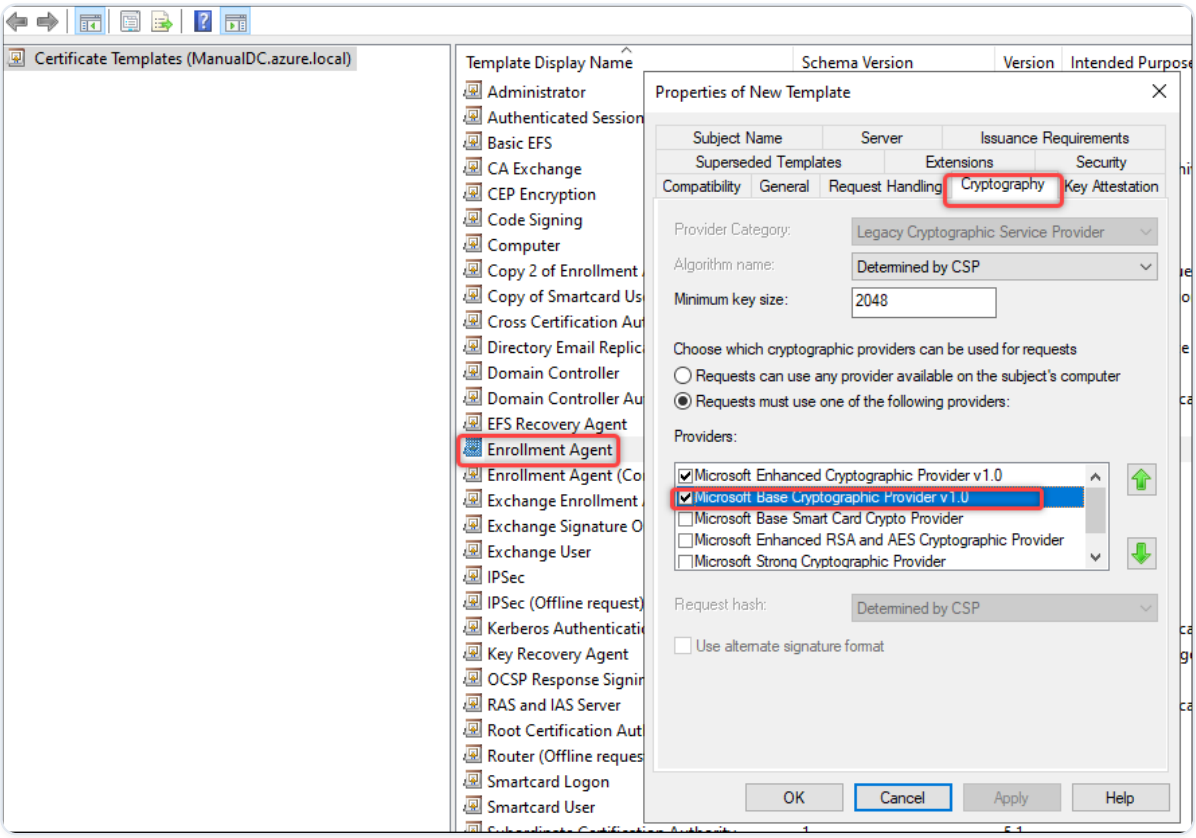


   b. Clique com o botão direito em **Agente de Registro** e selecione **Duplicar Modelo**.

   c. Na guia **Nome do Assunto**, certifique-se de que **Incluir e-mail no nome do assunto** esteja desmarcado.



d. Na guia **Criptografia**, selecione **Microsoft Base Smart Card Crypto Provider** e clique em **OK.** Um modelo chamado **Cópia de Agente de Registro** aparece na lista **Modelos de Certificado**.



3. Emita certificados para smart cards. As etapas detalhadas são as seguintes:

   a. Clique com o botão direito em **Modelos de Certificado** e selecione **Novo > Modelo a Ser Emitido**.

   b. Selecione **Cópia do Agente de Registro** e **Usuário de Cartão Inteligente**.

   c. Clique em **OK**.

Etapa 3: Registrar certificados para usuários de cartão inteligente

> **Observação:**

> As etapas a seguir são fornecidas como um exemplo para guiá-lo(a) através do processo.

> Em uma máquina Windows física ingressada no domínio, siga estas etapas para registrar certificados para cada cartão inteligente:

1. Prepare uma máquina Windows física ingressada no domínio para uso no registro:

   a. Certifique-se de que o driver do cartão inteligente esteja instalado.

   b. Insira um cartão inteligente na máquina.

c. Faça logon na máquina usando a conta de usuário que você deseja atribuir ao cartão inteligente.

2. Adicione o snap-in **Certificados** na máquina que você preparou na etapa 1. As etapas detalhadas são as seguintes:

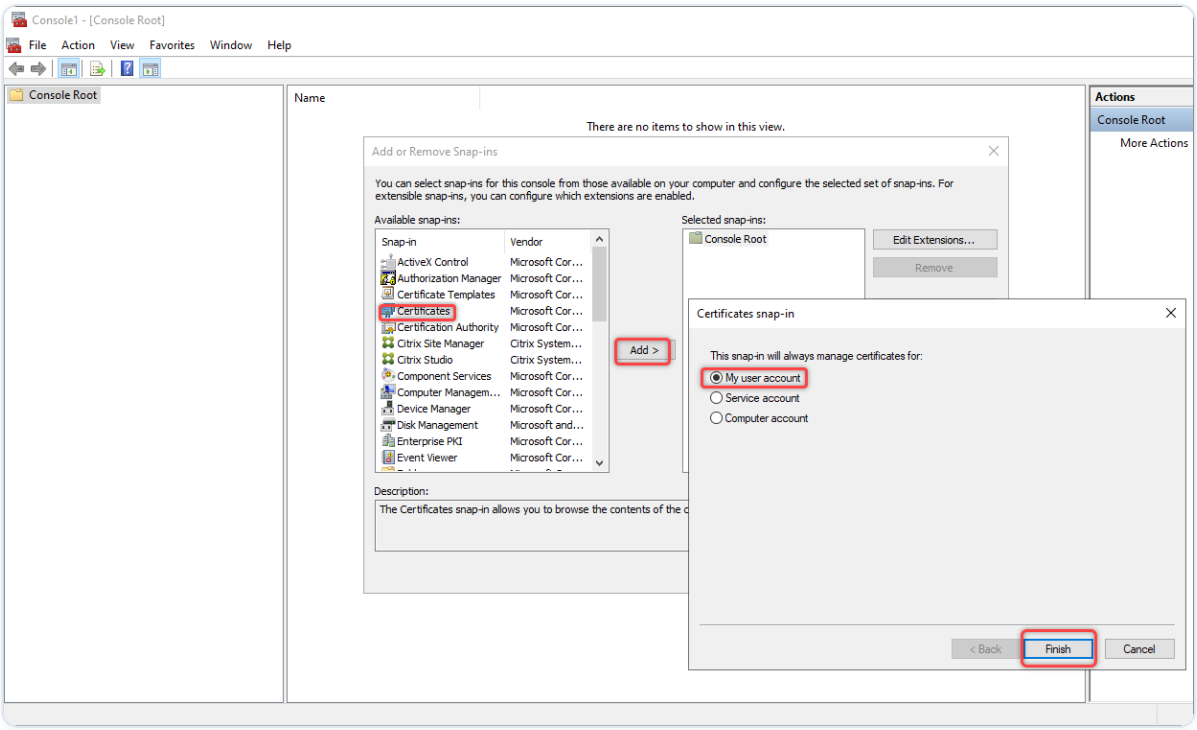
   a. Abra **mmc**.

   b. Clique em **Arquivo** e depois clique em **Adicionar/Remover Snap-in**.

   c. Na janela **Adicionar ou Remover Snap-ins** que aparece, selecione **Certificados** e depois clique em **Adicionar >**.

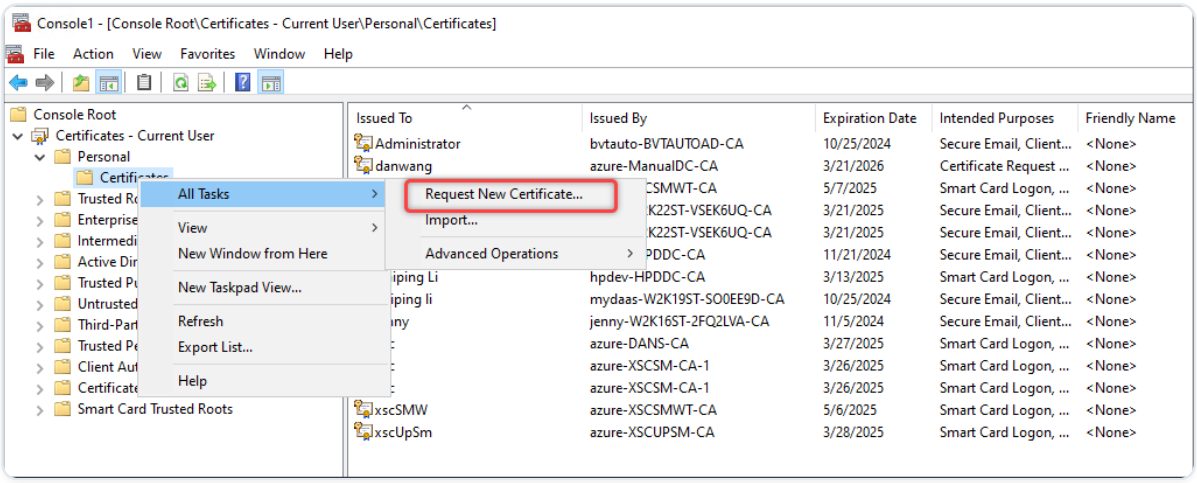
   d. Na caixa de diálogo que aparece, selecione **Minha conta de usuário** e clique em **Concluir**.

   e. Clique em **OK**.

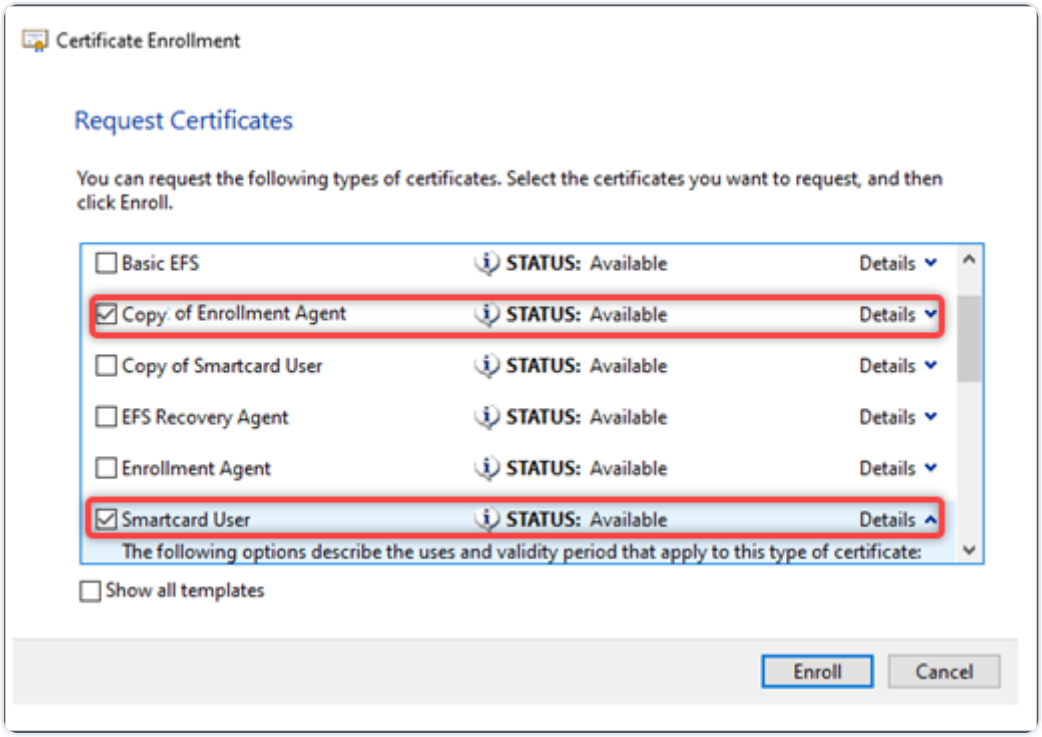


3. Solicite novos certificados para o snap-in **Certificados**. As etapas detalhadas são as seguintes:

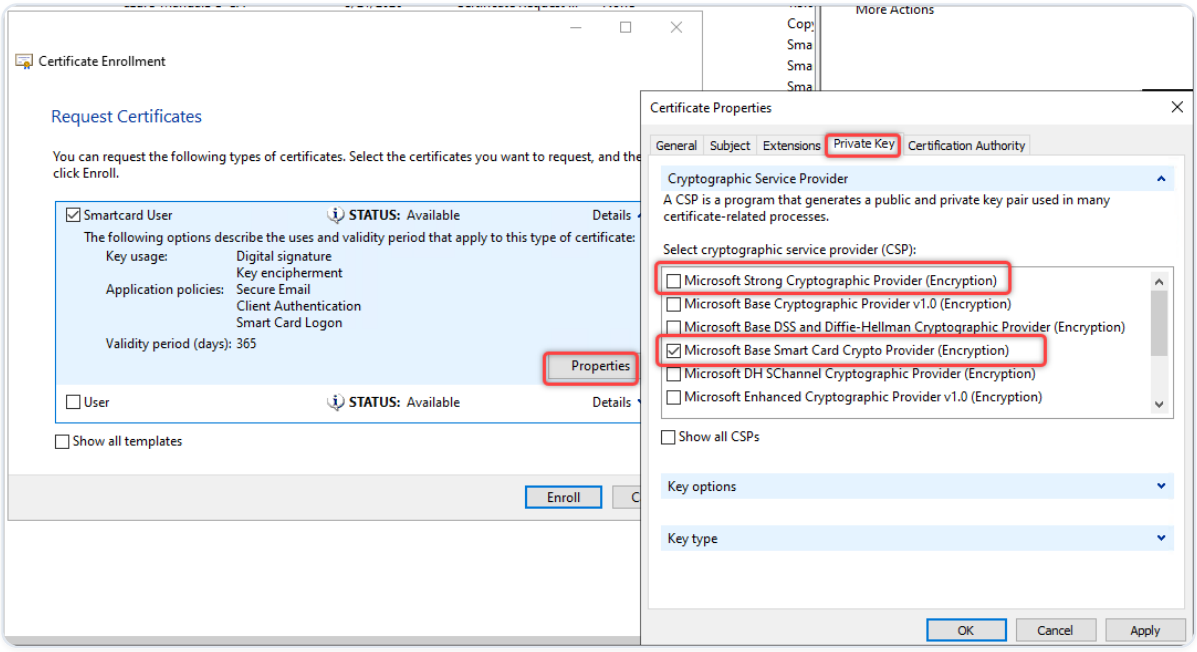
   a. Vá para **Certificados - Usuário Atual > Pessoal**, clique com o botão direito em **Certificados** e selecione **Todas as Tarefas > Solicitar Novo Certificado**.



b. Na caixa de diálogo **Solicitar Certificados** que aparece, selecione **Cópia do Agente de Registro** e **Usuário de Smartcard**.



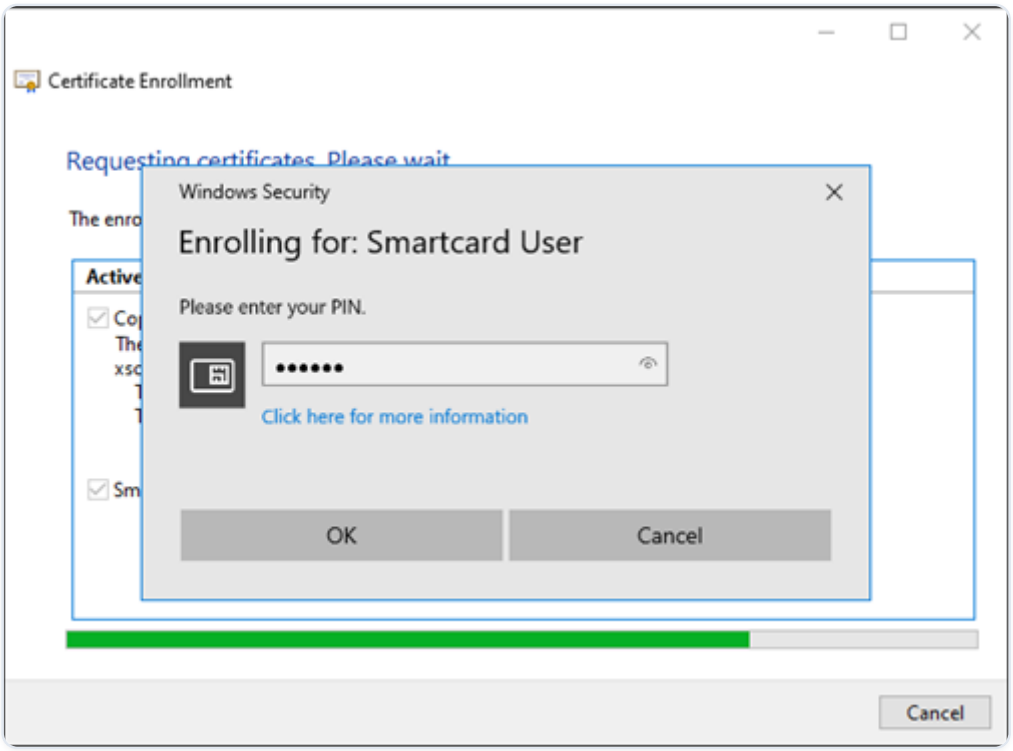
c. Na caixa de diálogo acima, clique em **Detalhes** para **Usuário de Smartcard** e, em seguida, clique em **Propriedades**. A caixa de diálogo **Propriedades do Certificado** é exibida.



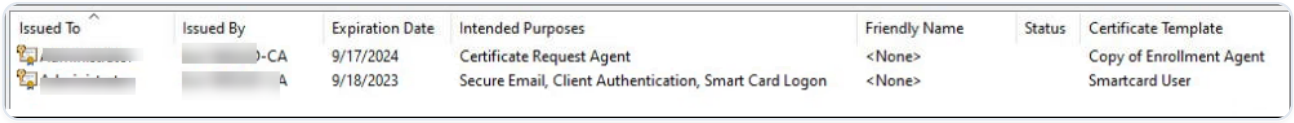
d. Na guia **Chave Privada**, expanda **Provedor de Serviços Criptográficos**, desmarque **Microsoft Strong Cryptographic Provider (Criptografia)**, selecione apenas **Microsoft Base Smart Card Crypto Provider (Criptografia)** e clique em **OK**.

e. Clique em **Registrar**.

f. Na caixa de diálogo **Segurança do Windows** que aparece, digite o código PIN do smart card e clique em **OK**. Quando o registro for concluído, clique em **Concluir**.



Após o registro bem-sucedido, dois certificados aparecem em **Certificados - Usuário Atual -> Pessoal -> Certificados**, conforme mostrado na seguinte captura de tela.



Etapa 4: Configurar os servidores IIS do Web Studio

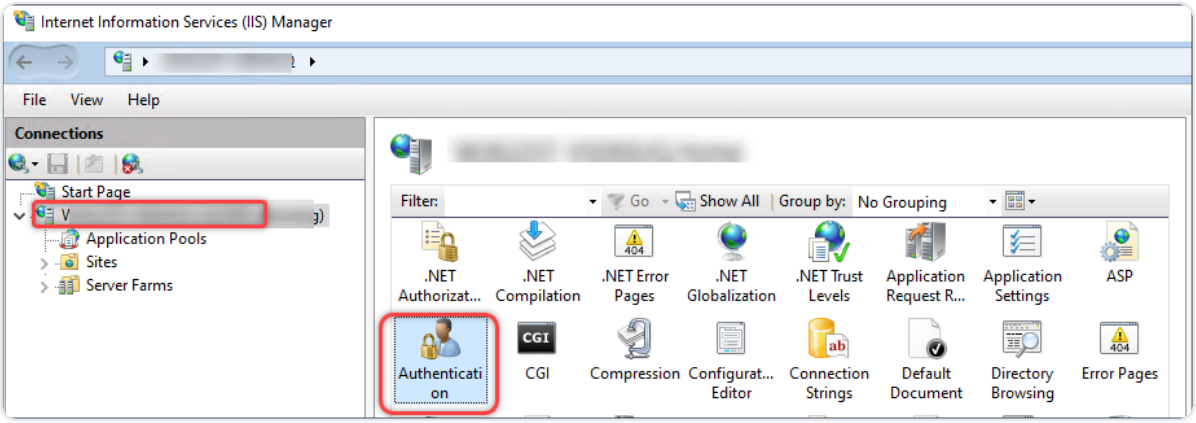
Em cada servidor Web Studio, siga estas etapas para configurar o IIS para autenticação de smart card:

1. Habilite a **Autenticação de Mapeamento de Certificado de Cliente** para a máquina do Web Studio**.

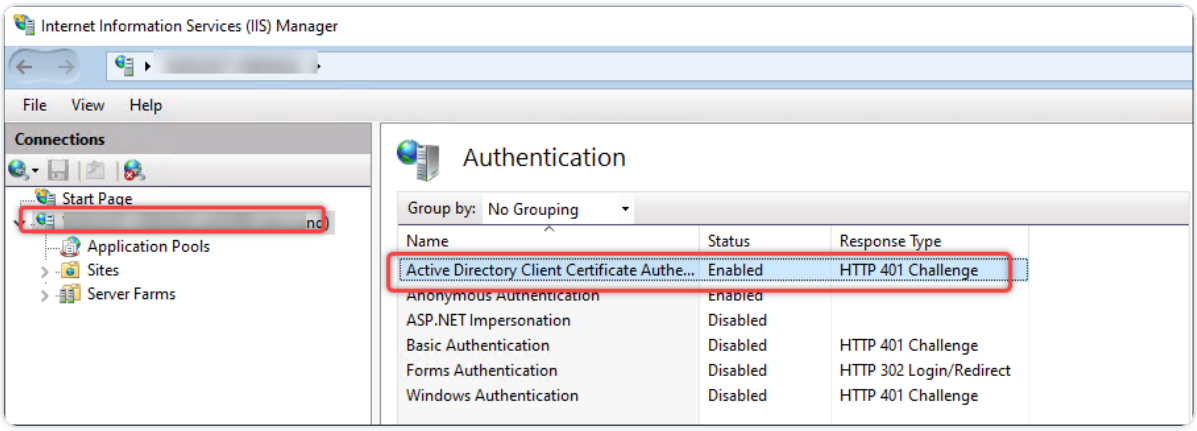
   O elemento `<clientCertificateMappingAuthentication>` não está disponível na instalação padrão do IIS 7 e posterior. Para obter mais informações sobre instalação e habilitação, consulte este artigo da Microsoft.

2. Inicie o **Gerenciador do IIS** na máquina do Web Studio.
3. Habilite a **Autenticação de Certificado de Cliente do Active Directory** para a máquina. As etapas detalhadas são as seguintes:

   a. Selecione a máquina no painel esquerdo e clique duas vezes em **Autenticação**.

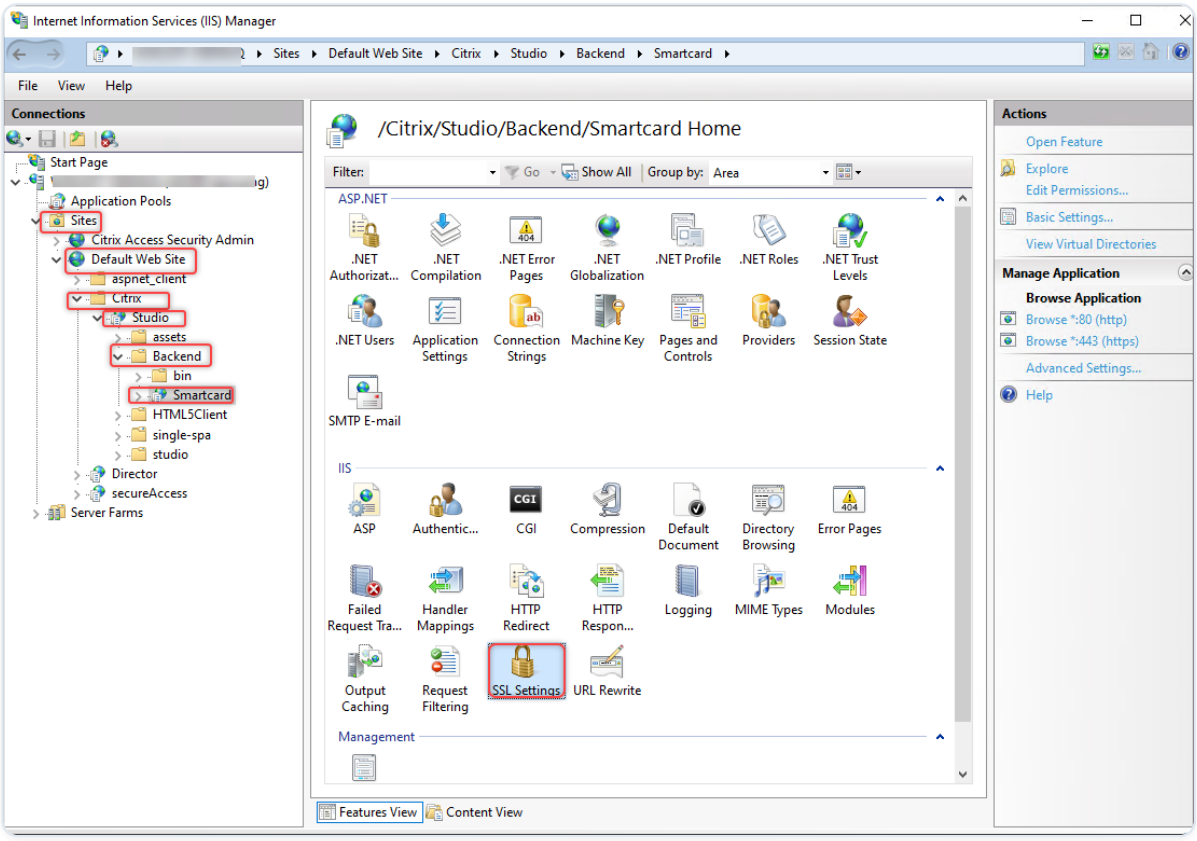


   b. Habilite a **Autenticação de Certificado de Cliente do Active Directory**.

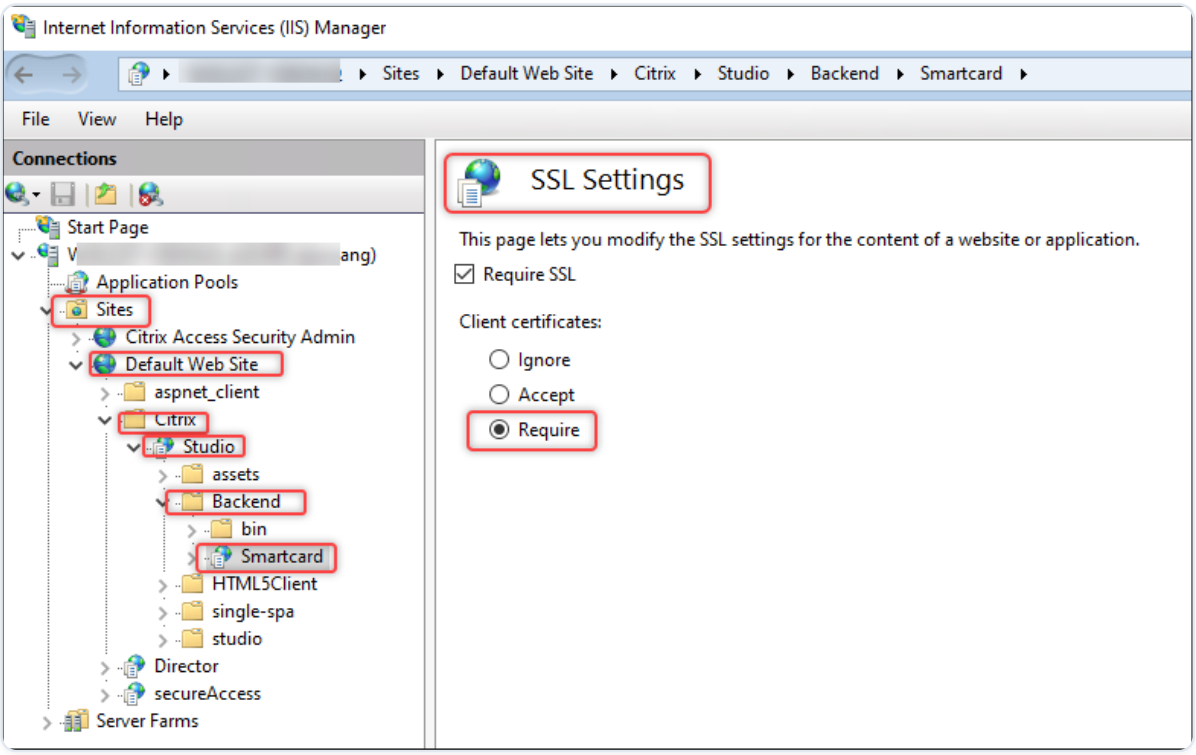


4. Configure o módulo de Backend do Web Studio para um protocolo HTTPS mais seguro com autenticação de certificado de cliente:

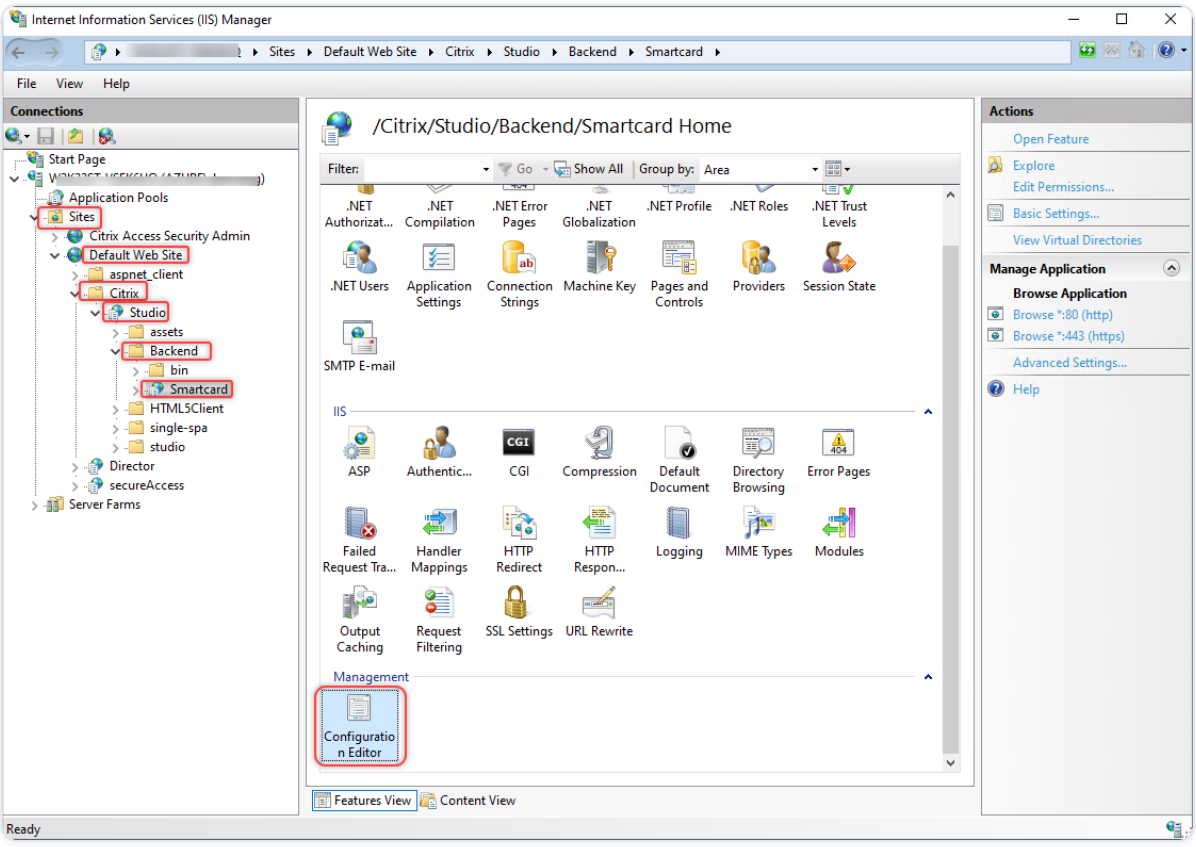
   a. Vá para **Sites > Default Web Site > Studio > Backend > Smartcard**, então clique duas vezes em **SSL Settings** na seção **IIS**.



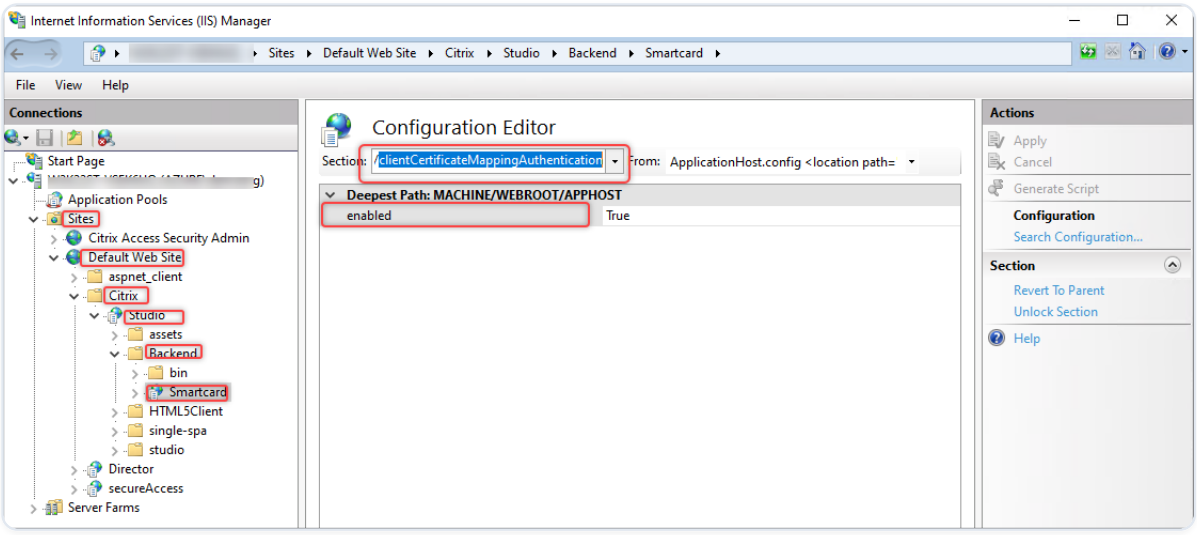
   b. Selecione **Exigir** para **Certificados de cliente**.



c. Retorne a **Sites > Default Web Site > Studio > Backend > Smartcard** e então clique duas vezes em **Configuration Editor** na seção **IIS**.



d. Certifique-se de que **/clientCertificateMappingAuthentication** esteja **habilitado**.

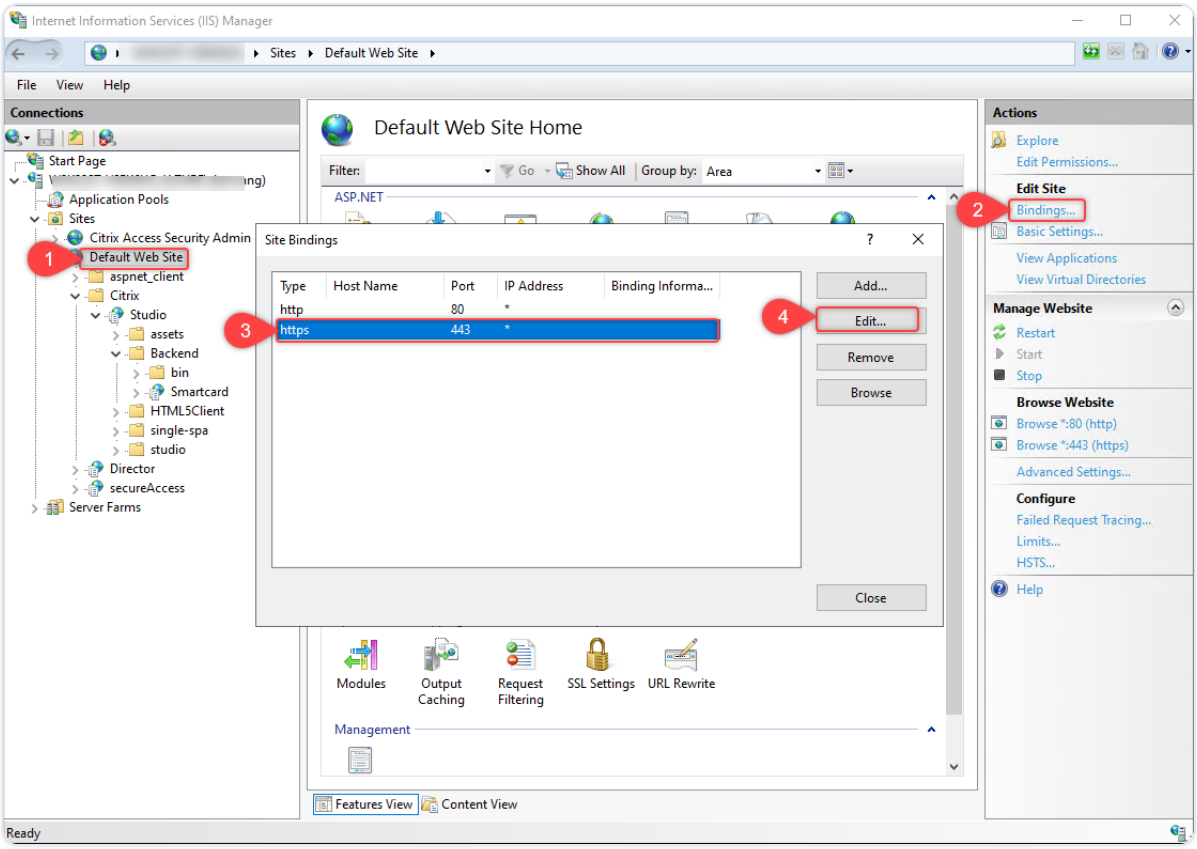


5. (Somente Windows 2022) Desative o TLS 3.1 sobre TCP. As etapas detalhadas são as seguintes:

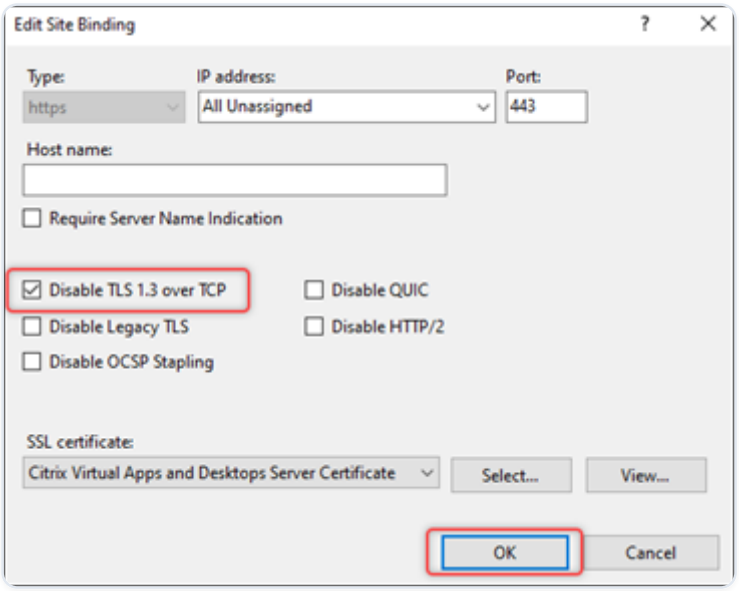
   a. Vá para **Sites > Default Web Site**.

   b. Clique em **Edit Site > Binding**.

   c. Na caixa de diálogo **Site Bindings** que aparece, selecione o registro **https** e clique em **Edit**.



   d. Na caixa de diálogo **Edit Site Binding** que aparece, selecione **Disable TLS 1.3 over TCP** e clique em **OK**.



É bom saber:

O backend do Web Studio é um módulo no Web Studio que fornece as seguintes funções:

- Autenticação de cartão inteligente.
- Recuperação de tokens de portador FMA do serviço de Orquestração usando autenticação integrada do Windows.

Etapa 5 (Opcional) Configure delegações de autenticação para o Web Studio

Quando o Web Studio e os Delivery Controllers são instalados em servidores diferentes, você deve configurar delegações para cada servidor Web Studio para os Delivery Controllers para os serviços HOST e HTTPS.

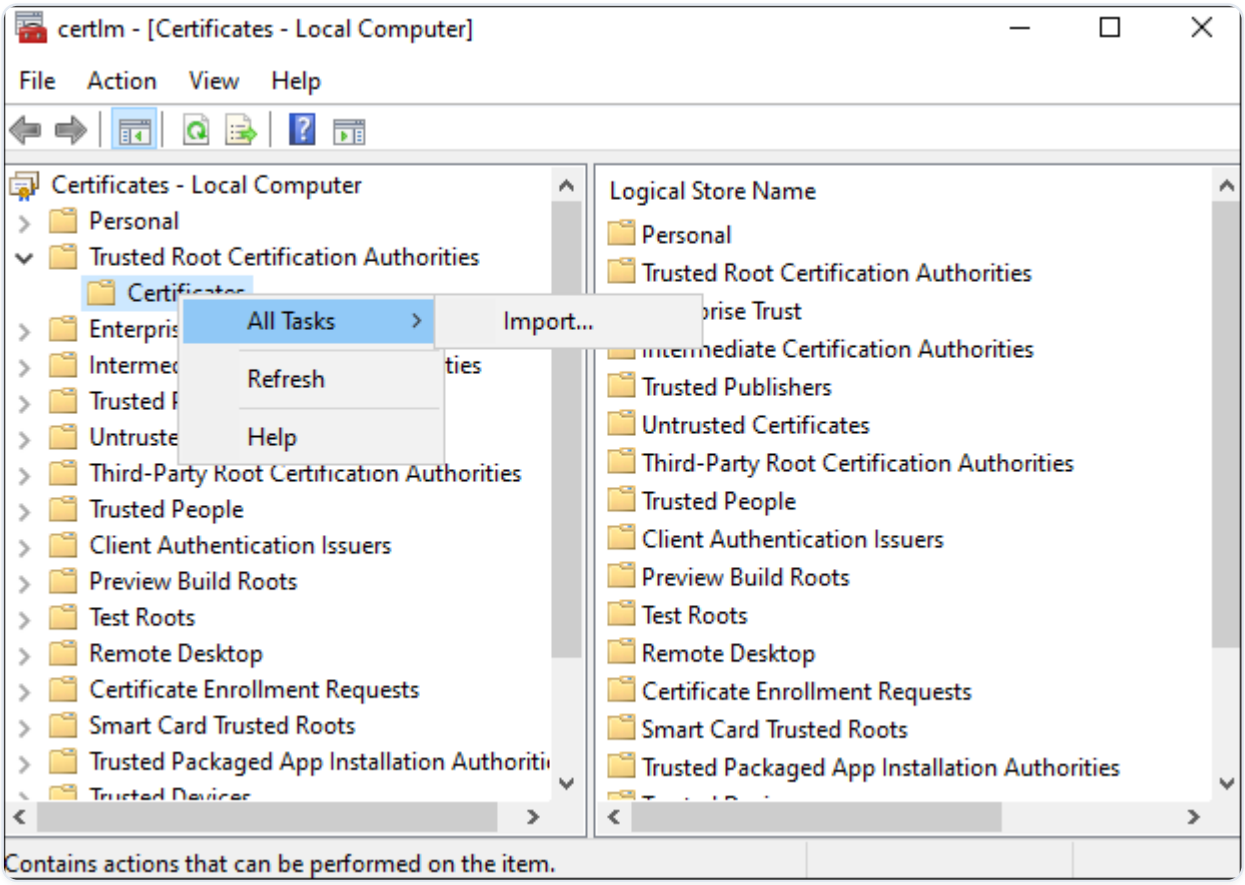
Siga estas etapas para concluir a tarefa para cada servidor Web Studio:

1. Importar o Certificado HTTPS de Orquestração do Delivery Controller™
2. Configurar delegação para o servidor Web Studio
3. （Opcional) Configurar delegação para a conta de serviço do servidor IIS do Web Studio

Importar o Certificado HTTPS de Orquestração do Delivery Controller

No servidor Web Studio, importe o certificado **Delivery Controller Orchestration HTTPS** para **Autoridades de Certificação Raiz Confiáveis**. As etapas detalhadas são as seguintes:

1. Inicie **Configurações > Gerenciar certificados do computador**.
2. Clique com o botão direito do mouse em **Autoridades de Certificação Raiz Confiáveis > Certificados** e selecione **Todas as Tarefas > Importar**.

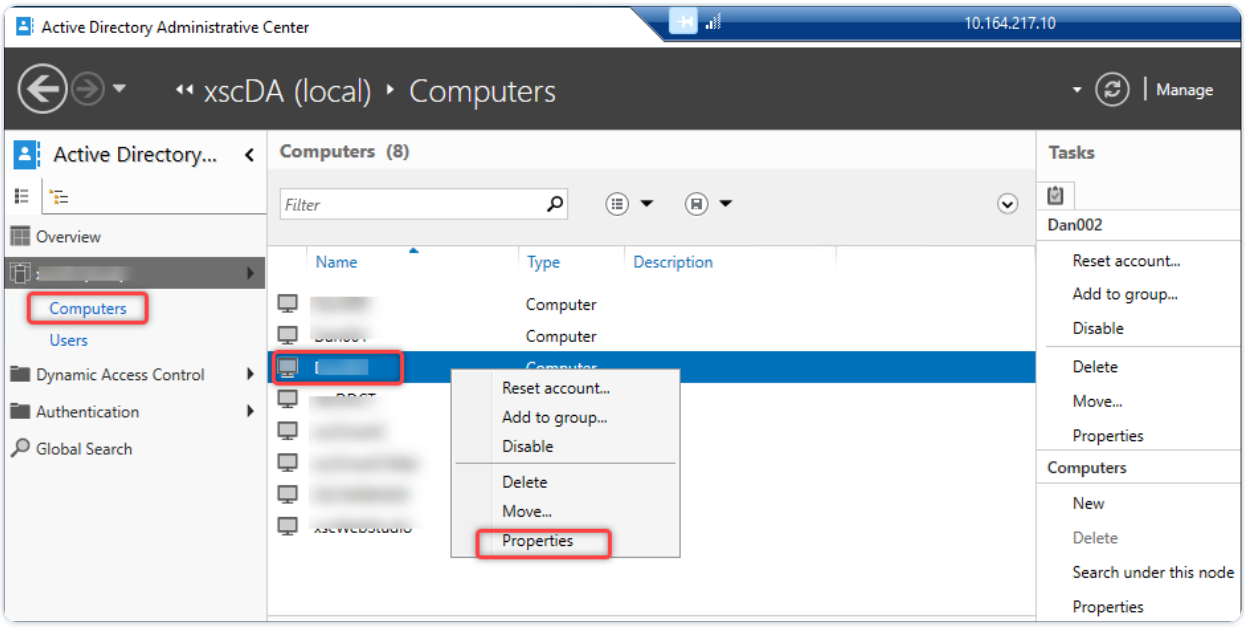


3. Siga as instruções na tela para importar o certificado **Delivery Controller Orchestration HTTPS**.

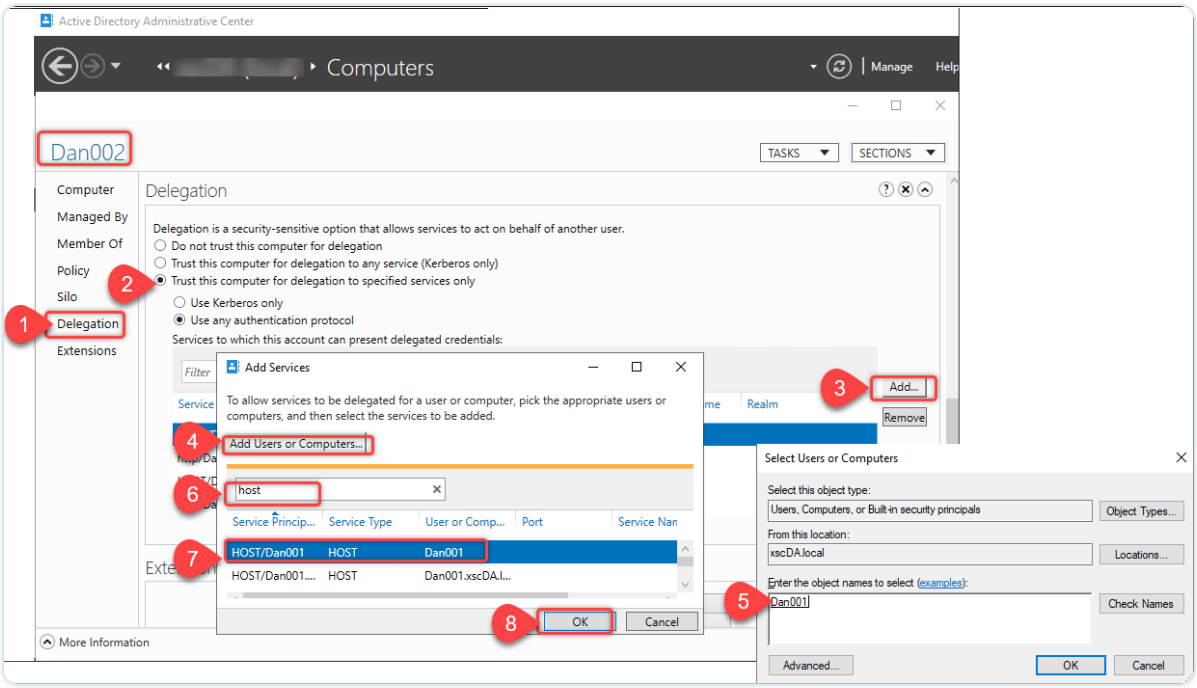
Configurar delegação para o servidor Web Studio

No controlador de domínio, configure a delegação para o servidor Web Studio para o Delivery Controller para serviços HOST e HTTP. Siga estas etapas para concluir a tarefa:

1. No controlador de domínio, inicie o **Centro Administrativo do Active Directory**.
2. Localize a conta de **computador** do servidor Web Studio para a qual você deseja configurar a delegação (*por exemplo, Dan002*).
3. Clique com o botão direito do mouse na conta, selecione **Propriedades** e, em seguida, conclua as seguintes etapas:



a. Vá para a guia **Delegação**.



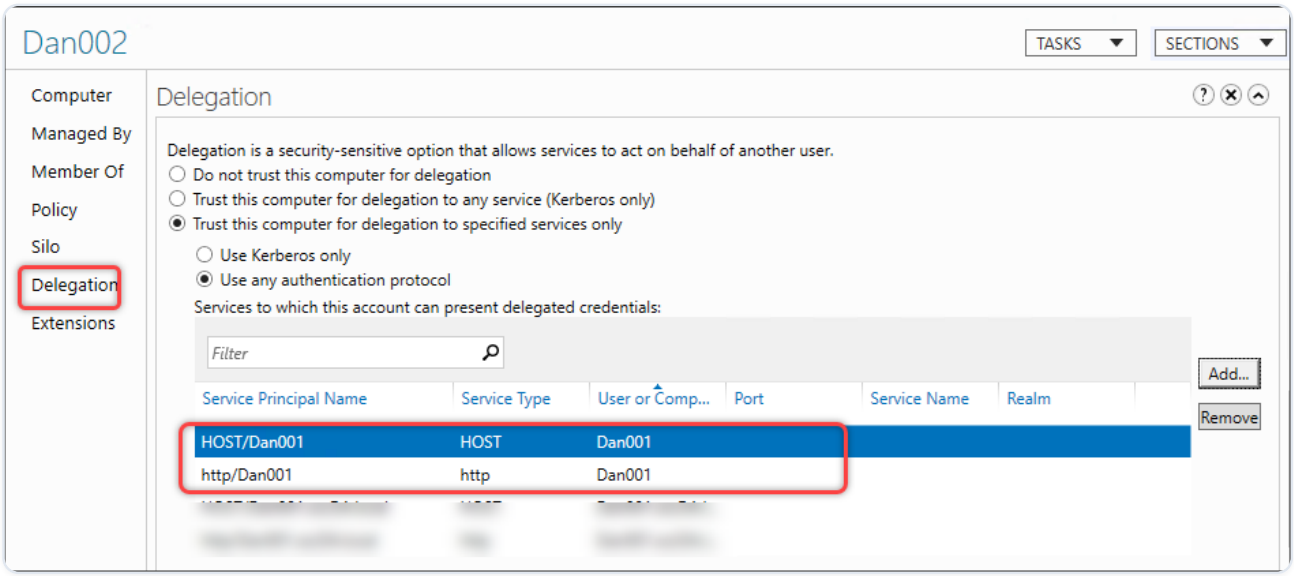
b. Selecione **Confiar neste usuário para delegação apenas para serviços especificados > Usar qualquer protocolo de autenticação**.

c. Clique em **Adicionar** para especificar a quais serviços esta conta de computador pode ser delegada.

d. Na caixa de diálogo **Adicionar Serviço** que aparece, clique em **Adicionar Usuários ou Computadores** para localizar o nome do computador do Delivery Controller (*por exemplo, Dan001*).

e. Selecione os serviços **HOST** e **HTTP** e, em seguida, clique em **OK**.

Os resultados da configuração são mostrados na captura de tela a seguir.

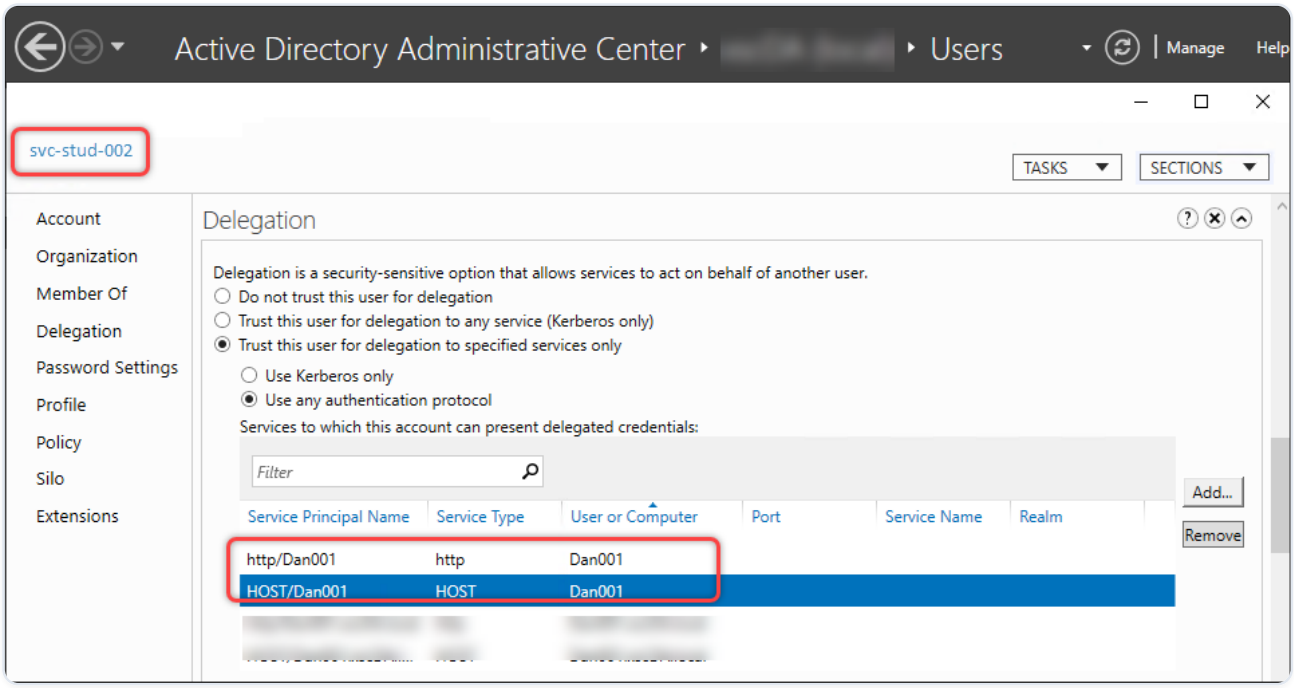


(Opcional) Configurar delegação para a conta de serviço do servidor IIS do Web Studio

Se você configurou uma conta de serviço para o servidor IIS do Web Studio, também precisará configurar a delegação para esta conta de serviço para o Delivery Controller para os serviços HOST e HTTP. Com esta delegação estabelecida, o servidor Web Studio pode usar sua conta de serviço para representar o usuário atual do cartão inteligente para acessar o Delivery Controller para os serviços HOST e HTTP. Siga estas etapas para concluir a configuração:

1. No controlador de domínio, inicie o **Centro Administrativo do Active Directory**.
2. Localize a conta de **usuário** do servidor IIS do Web Studio (conta de serviço) para a qual você deseja configurar a delegação (*por exemplo, svr-stud-002*).
3. Clique com o botão direito do mouse na conta e selecione **Propriedades**.
4. Siga o procedimento descrito na etapa 3 de Configurar delegação para o servidor Web Studio para delegar a conta de serviço do servidor IIS do Web Studio ao Delivery Controller para os serviços HOST e HTTP.

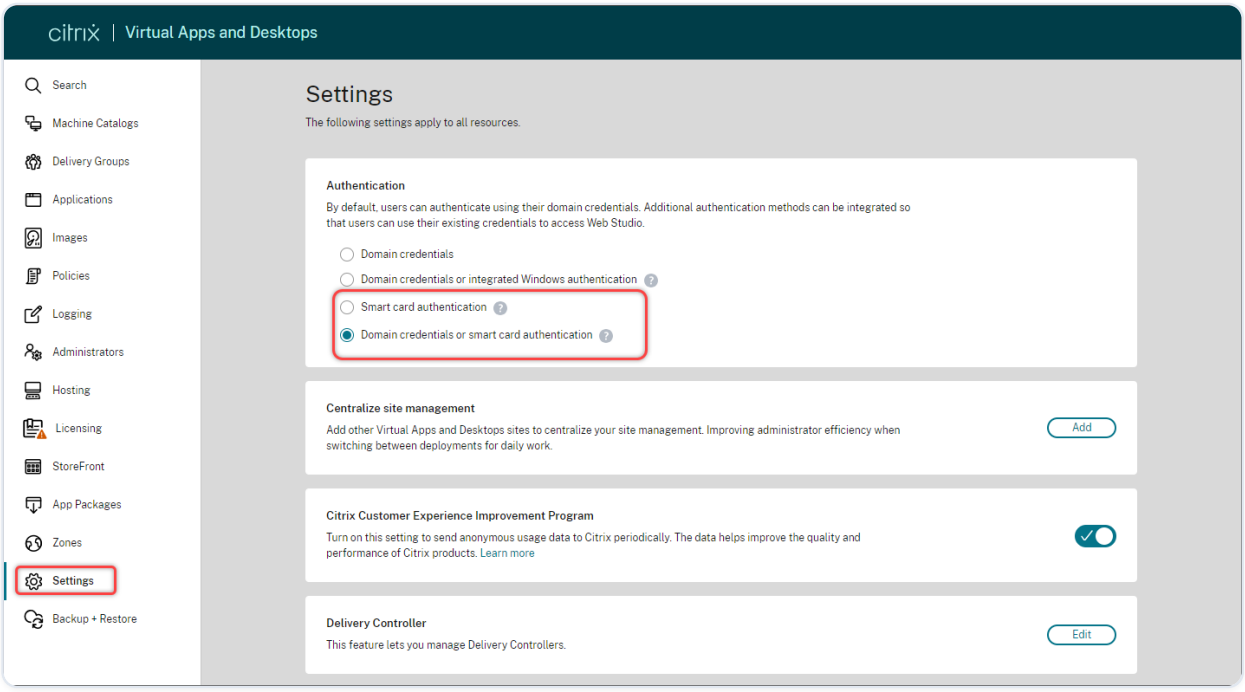
Os resultados da configuração são mostrados na captura de tela a seguir.



Etapa 6: Habilitar autenticação de cartão inteligente para Web Studio

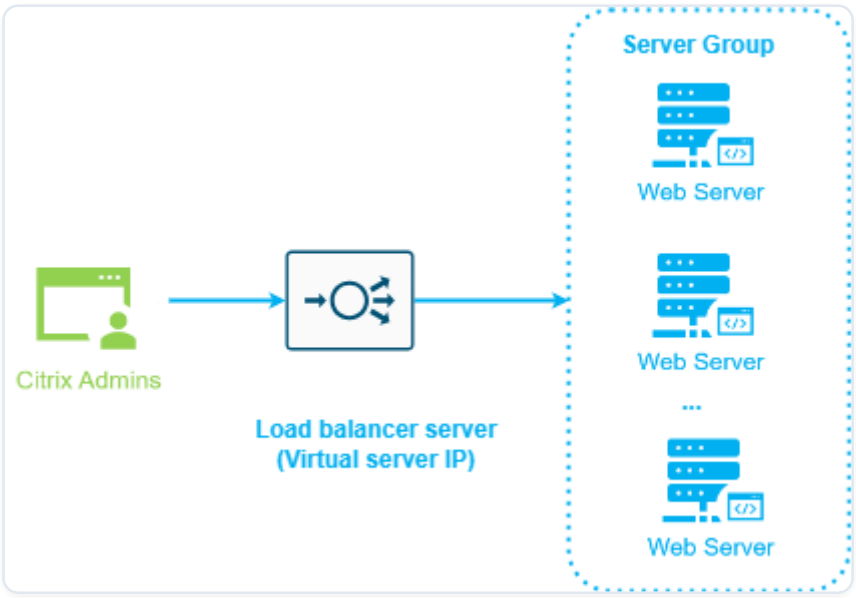
Siga estas etapas para habilitar a autenticação de cartão inteligente para Web Studio:

1. Faça login em **Web Studio** e selecione **Configurações** no painel esquerdo.
2. Selecione **Autenticação de cartão inteligente** ou **Credenciais de domínio ou autenticação de cartão inteligente** conforme necessário.
3. Clique em **Aplicar**.



Configurar uma implantação do Web Studio com balanceamento de carga

Para configurar implantações do Web Studio de alta disponibilidade, você pode escolher ferramentas como NetScaler® ADC ou Balanceamento de Carga de Rede do Windows. Este artigo fornece um guia passo a passo sobre como configurar uma implantação do Web Studio com balanceamento de carga usando um dispositivo NetScaler ADC.



Requisitos de certificado

Antes de comprar um certificado de uma autoridade de certificação comercial ou emitir um de sua autoridade de certificação corporativa, considere as seguintes opções com base em suas necessidades:

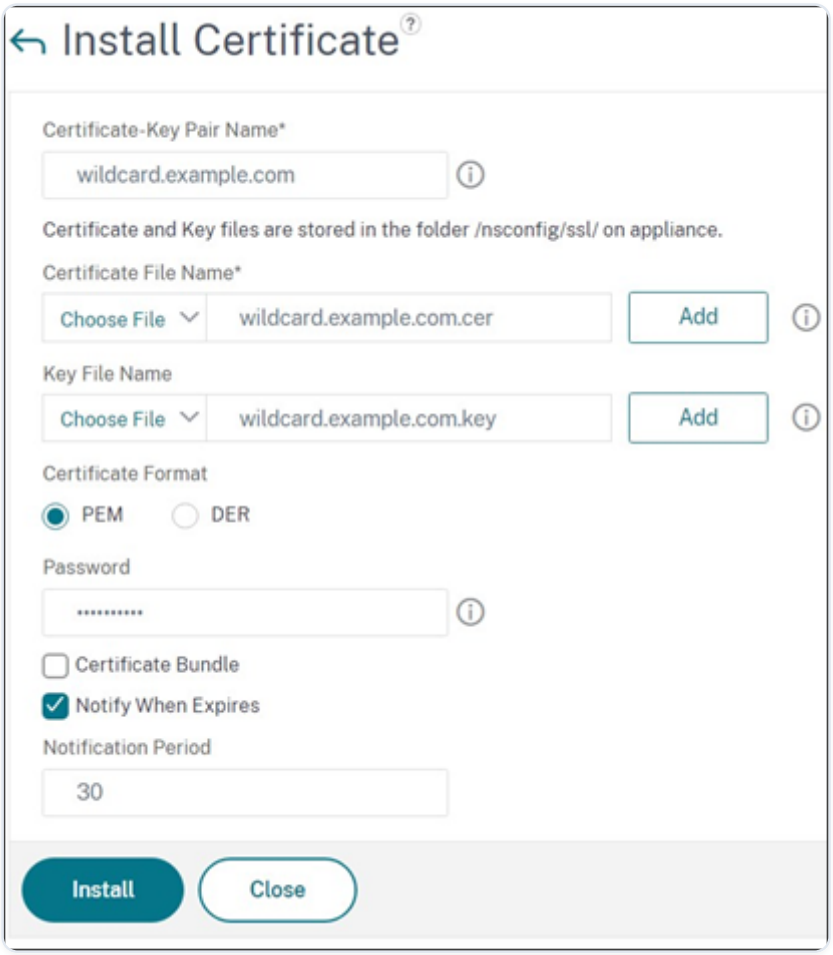
OPÇÃO	PRÓS	CONTRAS
Opção 1: Use um certificado curinga **.example.com* tanto no servidor de balanceamento de carga do dispositivo NetScaler ADC quanto nos servidores Web Studio.	• Simplifica a configuração • Mais fácil de gerenciar (certificado único) • Pode adicionar novos subdomínios	• Se o certificado curinga for comprometido, todos os subdomínios estarão em risco • Nem todos os aplicativos suportam

OPÇÃO	PRÓS	CONTRAS
	sem atualizar o certificado	certificados curinga • Pode ser mais caro do que certificados individuais
Opção 2: Use um certificado com Nomes Alternativos de Assunto (SANs) tanto no servidor de balanceamento de carga do dispositivo NetScaler ADC quanto nos servidores Web Studio.	• Flexível, pode incluir vários domínios e subdomínios específicos • Centraliza o gerenciamento para vários domínios • Suporta vários nomes distintos, proporcionando mais flexibilidade do que curingas	• O gerenciamento de entradas SAN pode se tornar complexo à medida que o número de domínios aumenta • Adicionar novos domínios requer a reemissão do certificado • Limitado pelo número de entradas SAN suportadas pela CA
Opção 3: Usar um certificado para cada servidor Web Studio e para o servidor balanceador de carga do dispositivo NetScaler ADC	• Cada servidor é protegido independentemente • O comprometimento de um	• Maior sobrecarga administrativa, pois cada certificado deve ser gerenciado separadamente

OPÇÃO	PRÓS	CONTRAS
	certificado não afeta os outros • Pode usar certificados específicos adaptados às necessidades de cada servidor	• Mais certificados para renovar e custos potencialmente mais altos • Deve garantir que todos os certificados estejam configurados de forma consistente

Configurar o certificado do servidor no balanceador de carga

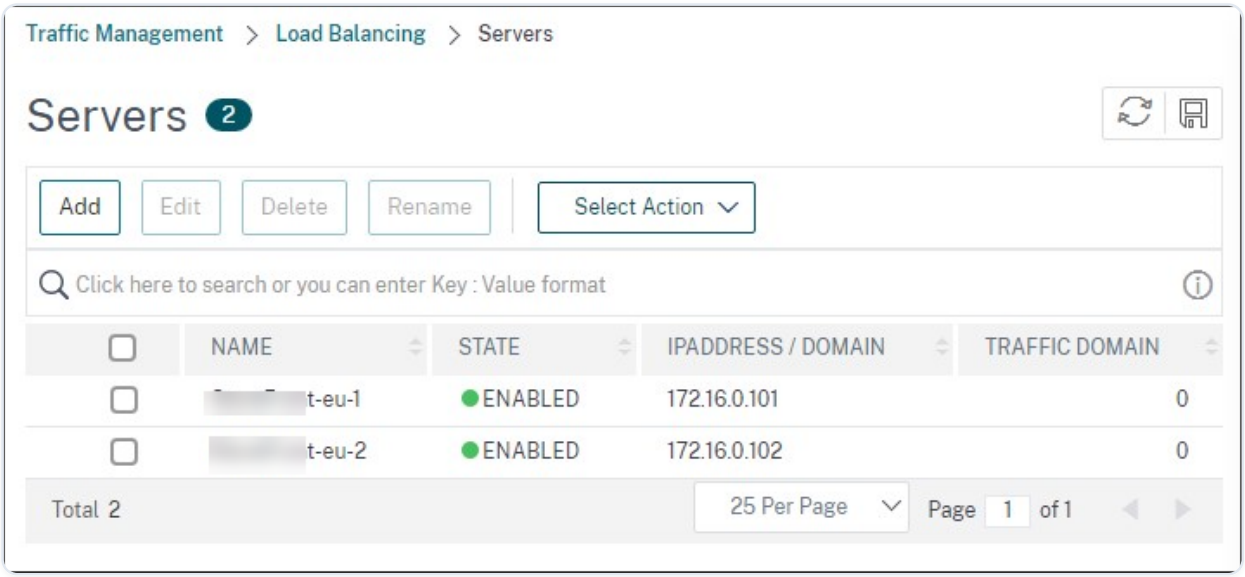
1. Faça logon na GUI de gerenciamento do dispositivo NetScaler ADC.
2. Selecione **Gerenciamento de Tráfego > SSL > Certificados > Certificados de Servidor**
3. Clique em **Instalar**.
4. Na página **Instalar Certificado de Servidor**, insira um Nome de Par de Chaves de Certificado, clique em **Escolher Arquivo** e, em seguida, procure o arquivo de certificado. Se o arquivo de certificado não incluir a chave privada, selecione um **Arquivo de Chave**.



Etapa 1: Adicionar nós de servidor do Web Studio

Adicione todos os nós de servidor do Web Studio (por exemplo, `Studio-eu-1` e `Studio-eu-2`) ao balanceador de carga.

1. Faça logon na GUI de gerenciamento do NetScaler ADC.
2. navegar para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**. Clique em **Adicionar**.
3. Insira o endereço IP do servidor de um nó de servidor do Web Studio.
4. Repita as etapas 2–3 para adicionar os outros servidores do Web Studio.



Etapa 2: Adicionar um monitor para nós de servidor do Web Studio

Configure um monitor no balanceador de carga para verificar o status de todos os nós de servidor do Web Studio.

1. Selecione **Gerenciamento de Tráfego > Balanceamento de Carga > Monitores > Adicionar**.
2. Na guia **Configuração**, preencha as seguintes configurações e deixe as outras configurações padrão:

   - Insira **Web Studio** para **Nome**.
   - Selecione **HTTP** ou **SSL** para **Tipo**.
   - Selecione a opção **Seguro**.
   - Insira **HEAD/citrix/studio/** para **Solicitação HTTP**.

   Captura de tela da tela Servidores com dois servidores(/en-us/citrix-virtual-apps-desktops/2407/media/netscaler-monitor-for-studio.png)

Etapa 3: Criar um grupo de serviços para nós de servidor do Web Studio

1. Selecione **Traffic Management > Load Balancing > Service Groups > Add**. Para se conectar aos servidores do Web Studio via HTTPS, selecione um protocolo SSL, deixe as outras configurações como padrão e clique em **OK**.
2. Dentro do seu Grupo de Serviços, em **Membros do Grupo de Serviços**, clique em **Nenhum Membro do Grupo de Serviços** e siga estas etapas para adicionar membros:

   a. Clique em **Baseado em Serviço**.

b. Selecione todos os servidores que você adicionou anteriormente.

c. Insira **443** para a porta.

Captura de tela da página Criar membro do grupo de serviços(/en-us/citrix-virtual-apps-desktops/2407/media/netscaler-create-service-group-member.png)

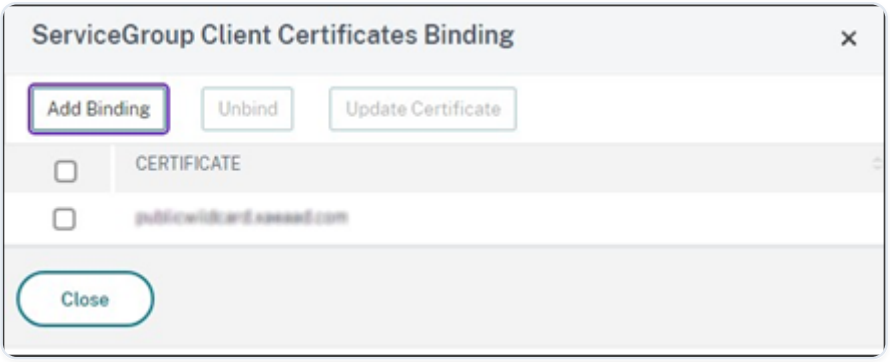
3. Adicione a seção **Monitores** e selecione o monitor do Web Studio que você criou anteriormente.

   Captura de tela da tela Monitor com um monitor listado(/en-us/citrix-virtual-apps-desktops/2407/media/monitors.png)

4. Adicione a seção **Certificados** e conclua as seguintes configurações:

   a. Vincular o certificado do cliente.

   b. Vincular o certificado CA usado para assinar o certificado do servidor que você importou anteriormente, e quaisquer outras CAs que possam fazer parte da cadeia de confiança PKI.



5. Adicione a seção **Configurações**, selecione **Inserir Cabeçalho IP do Cliente**, e então insira um nome de cabeçalho de **X-Forwarded-For**. Essa configuração permite que o Endereço IP do Cliente seja usado em Políticas.

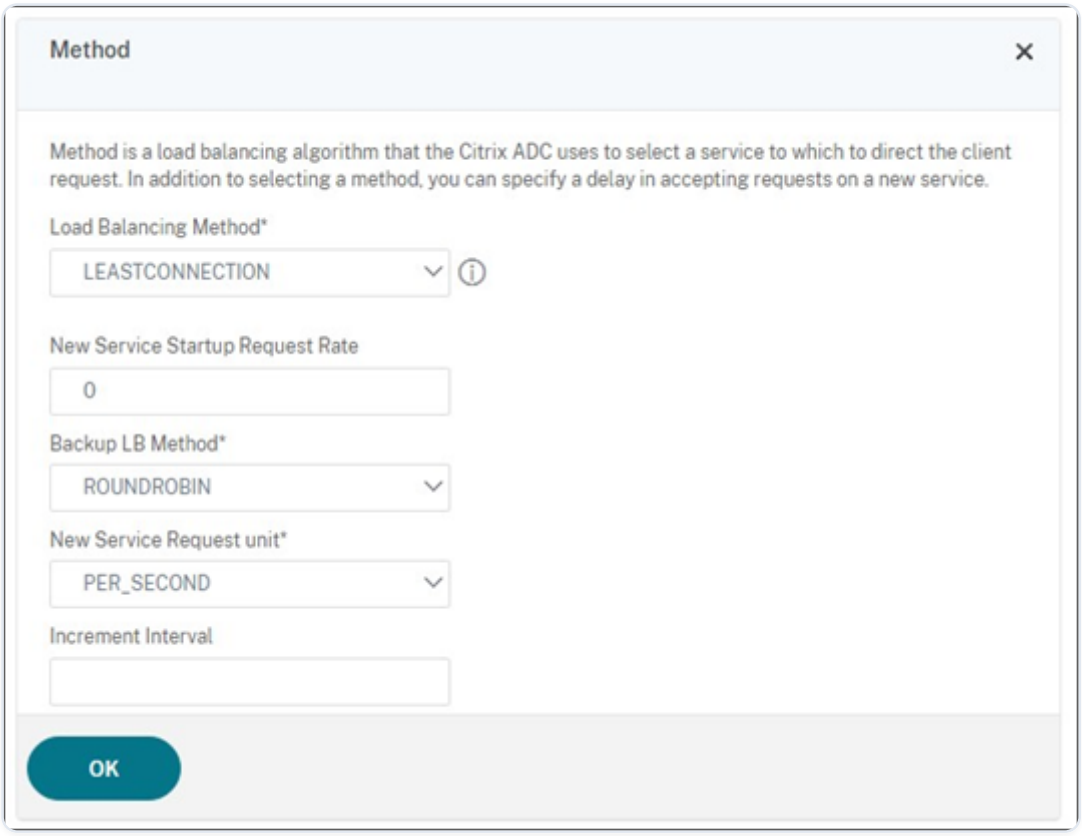
Etapa 4: Criar um servidor virtual

Crie um servidor virtual de balanceador de carga para que os usuários acessem o grupo de servidores do Web Studio.

1. navegar para **Traffic Management > Load Balancing > Virtual Servers**, e então clique em **Adicionar**.
2. Insira um nome, selecione **SSL** para o **Protocolo**, insira **443** para a **Porta**, e então clique em **OK**.



3. Vincule o **Grupo de Serviço** que você criou anteriormente ao servidor virtual de balanceamento de carga.
4. Vincule o certificado CA que você vinculou ao grupo de serviço em Etapa 3: Criar um grupo de serviço para nós de servidor do Web Studio.
5. Adicione a seção **Método** e selecione o método de balanceamento de carga. As escolhas comuns para o balanceamento de carga do Web Studio são **ROUNDROBIN** ou **LEASTCONNECTION**.



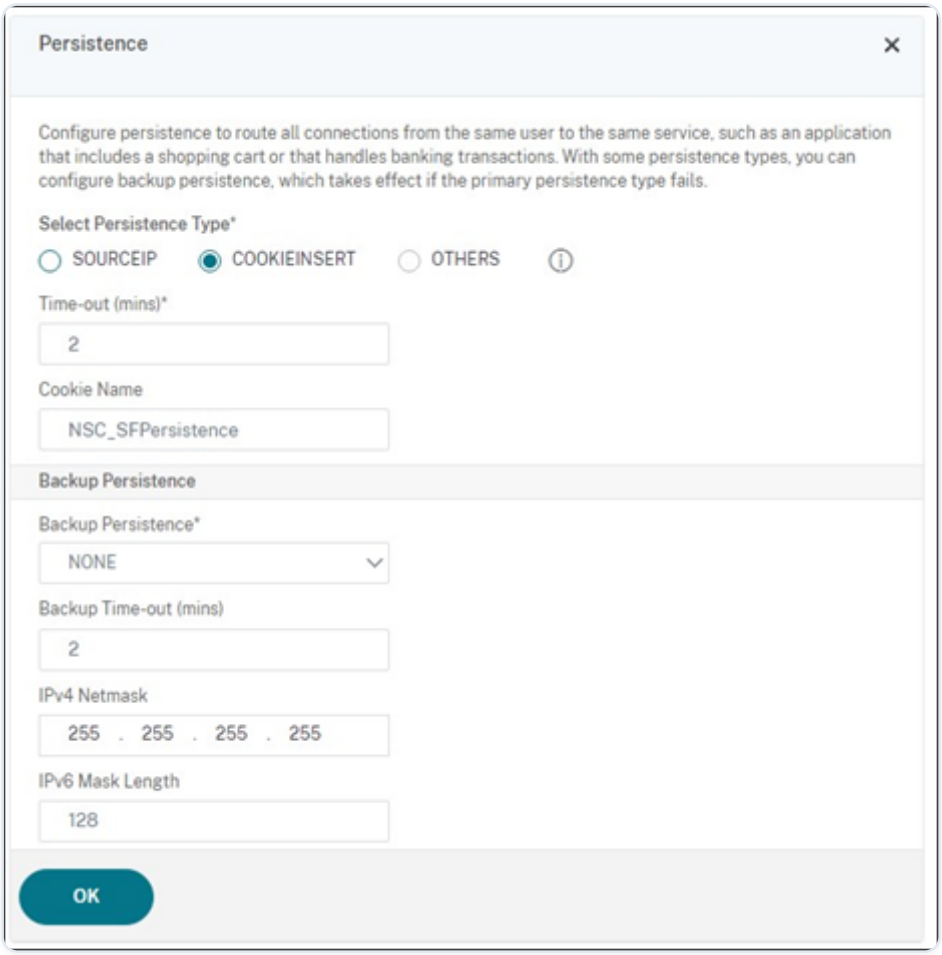
6. Adicione a seção **Persistência** e complete as seguintes configurações:

   a. Defina o método de persistência como **COOKIEINSERT**.

   b. Defina o tempo limite para ser o mesmo que o tempo limite da sessão no Web Studio (por padrão, 20 minutos).

   c. Nomeie o cookie para facilitar a depuração futura. Por exemplo, **NSC_SFPersistence**.

   d. Defina a persistência de backup como **NENHUM**.

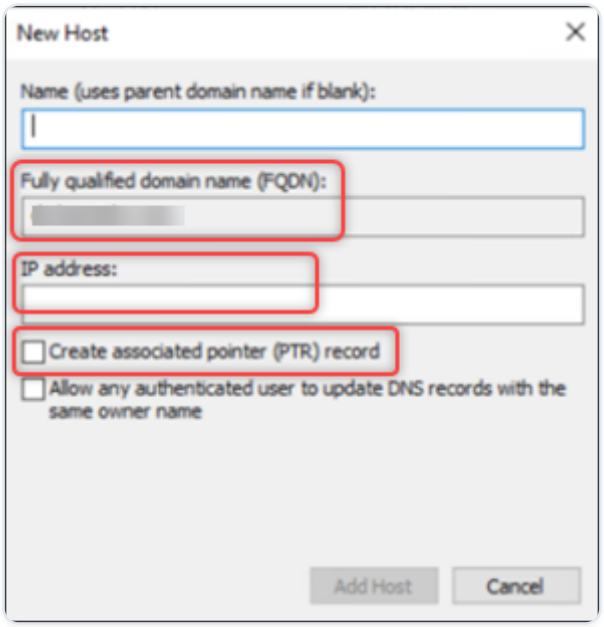


Observação:

Se o cliente não tiver permissão para armazenar o cookie HTTP, as solicitações subsequentes não terão o cookie HTTP, e a Persistência não será usada.

Etapa 5: Crie registros DNS para o servidor virtual

No Controlador de Domínio, crie um registro DNS e PTR para mapear o endereço IP do servidor virtual para um FQDN. Os usuários do Web Studio em sua rede usam este FQDN para acessar o grupo de servidores do Web Studio. Por exemplo, webstudio.example.com resolve para o endereço IP do servidor virtual do balanceador de carga (VIP).

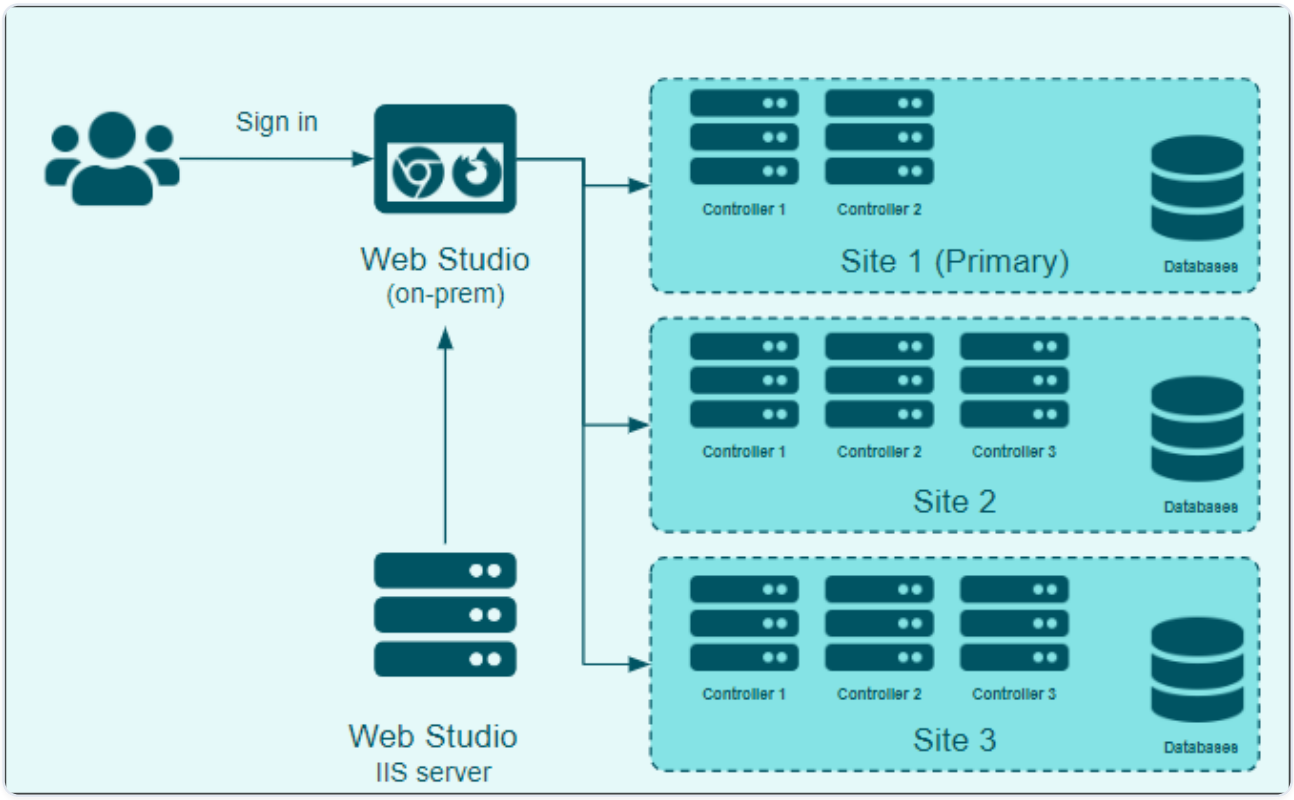


Forneça esta URL para os usuários acessarem os servidores do Web Studio: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`. Exemplo: `https://webstudio.example.com/citrix/studio`

Habilitar gerenciamento de múltiplos sites

Por padrão, um console do Web Studio é mapeado para um único site do Citrix Virtual Apps and Desktops™, e quando necessário, você pode configurar um console do Web Studio para gerenciar múltiplos sites. Dessa forma, você pode ter apenas um Web Studio instalado para configurar e gerenciar todos os seus sites.

O diagrama a seguir ilustra a arquitetura de múltiplos sites, onde uma única implantação do Web Studio gerencia múltiplos sites independentes do Citrix Virtual Apps and Desktops.



Benefícios

- Melhora a eficiência ao gerenciar múltiplos sites com uma experiência unificada de logon único.
- Facilita a solução de problemas com todas as configurações acessíveis a partir de um único console.

Considerações

Ao configurar e implantar os sites, tenha em mente os seguintes itens:

- Versão necessária:
  - Citrix Virtual Apps and Desktops 2311 e posterior.
  - A versão do Delivery Controller™ deve corresponder à versão do Web Studio ou ser anterior a ela, com um requisito mínimo de 2311 ou posterior.
  - Este recurso é exclusivo do Web Studio (baseado na web) e não está disponível no Citrix Studio (baseado em Windows).
- Para oferecer suporte ao logon único, implante todos os sites em domínios confiáveis.
- Você pode gerenciar um máximo de 10 sites do Citrix Virtual Apps and Desktops usando o console unificado do Web Studio.

Fluxo de trabalho

Antes de começar

- Determine o site primário e certifique-se de que o console do Web Studio esteja acessível para o gerenciamento do site primário.

  > **Observação:**
  >
  > - Ao projetar um site primário, esteja ciente de que a acessibilidade dos sites adicionados depende da disponibilidade do site primário. Problemas de desempenho com o site primário podem impactar o acesso aos sites adicionados.
  > - Se o Web Studio não estiver instalado, consulte Instalar o Web Studio.

- Certifique-se de que os sites que você pretende gerenciar com o Web Studio já estejam configurados.
  - Para criar um novo site, consulte Criar um site.
- (Recomendado) Para habilitar o logon único ao alternar entre os sites no console, habilite a Autenticação Integrada do Windows (IWA) em todos os sites. Para os sites onde o IWA não está habilitado, você também pode usar suas credenciais de logon para fazer login.

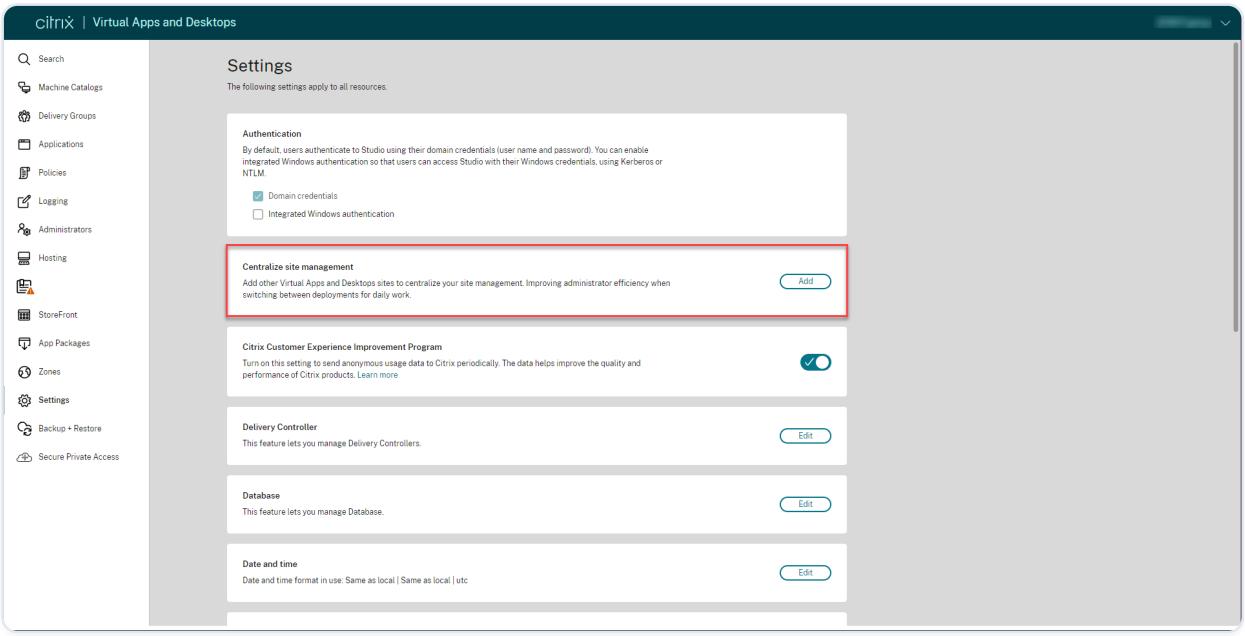
Etapa 1: Faça login no console do Web Studio

1. Abra um navegador da web. Digite `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Faça login no Web Studio para gerenciar o site primário.

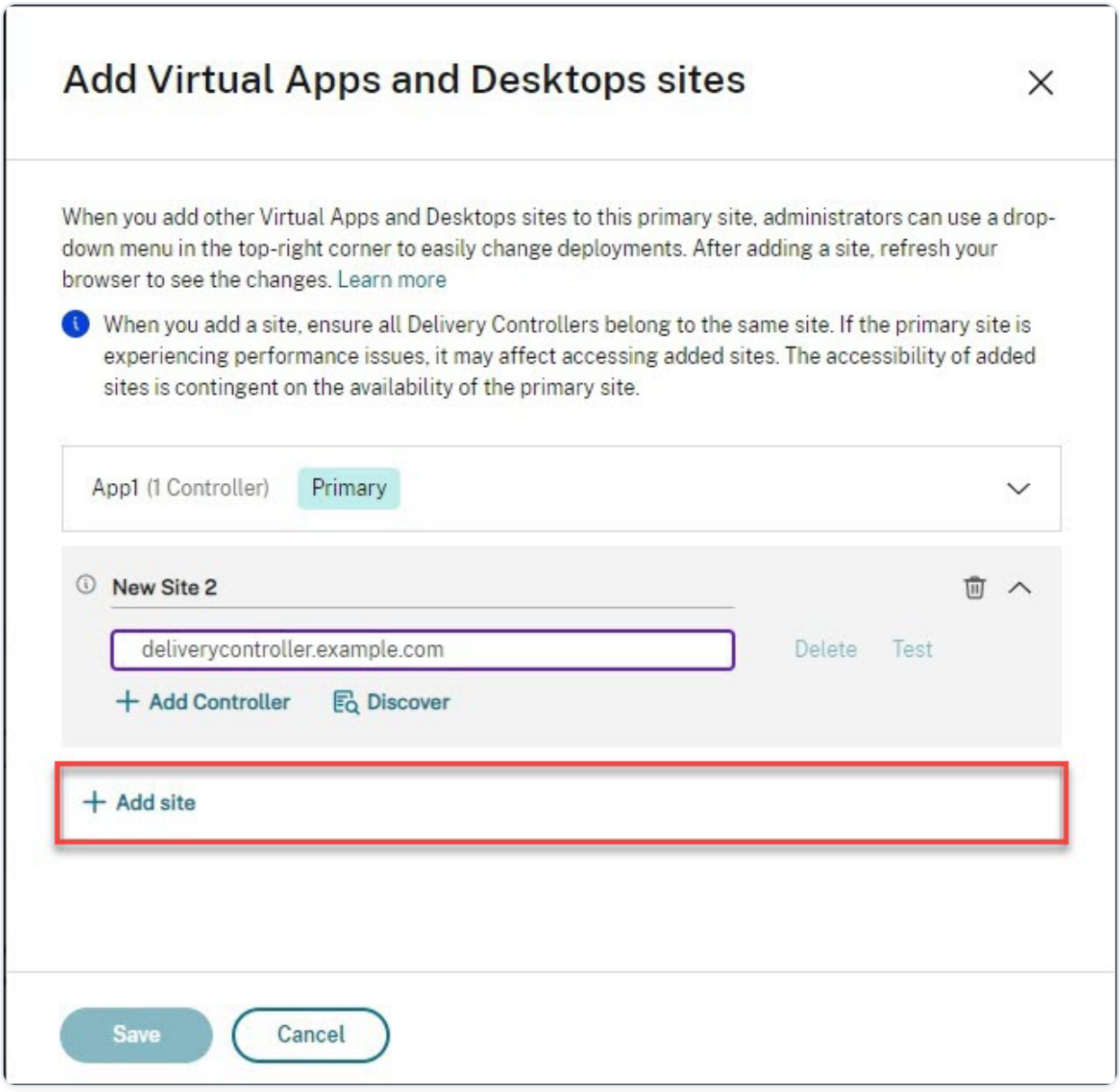
   > **Observação:**
   >
   > O endereço do Delivery Controller que você usa durante a instalação identifica o site. Se o Delivery Controller for do site primário, você fará login nesse site.

Etapa 2: Adicione sites usando o Web Studio

1. Vá para **Configurações** > **Gerenciamento centralizado de sites** e então clique em **Adicionar**.



2. Na página **Adicionar sites do Virtual Apps and Desktops**, clique em **Adicionar site**.



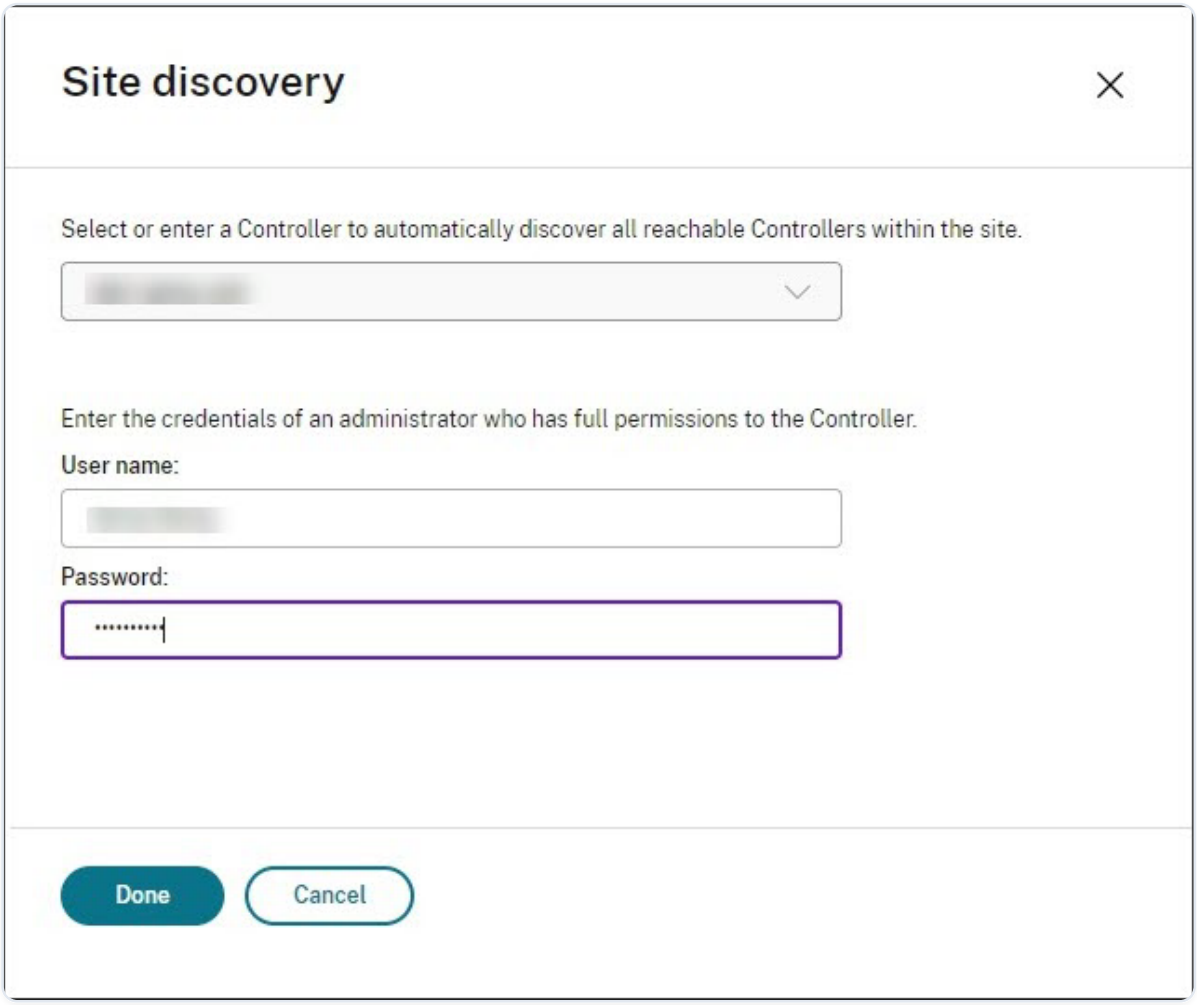
3. Execute uma das seguintes ações para adicionar os Delivery Controllers:

   - Clique em **Adicionar Controlador** e, em seguida, insira o FQDN. Clique em **Testar** para testar sua conectividade.
   - Clique em **Descobrir**.

     a. Na página **Descoberta de site**, selecione ou insira o endereço de um Controlador presente no site.

     b. Insira as credenciais de um administrador que tenha permissão total para o Controlador nos campos **Nome de usuário** e **Senha**.

     c. clique em **Concluído**.

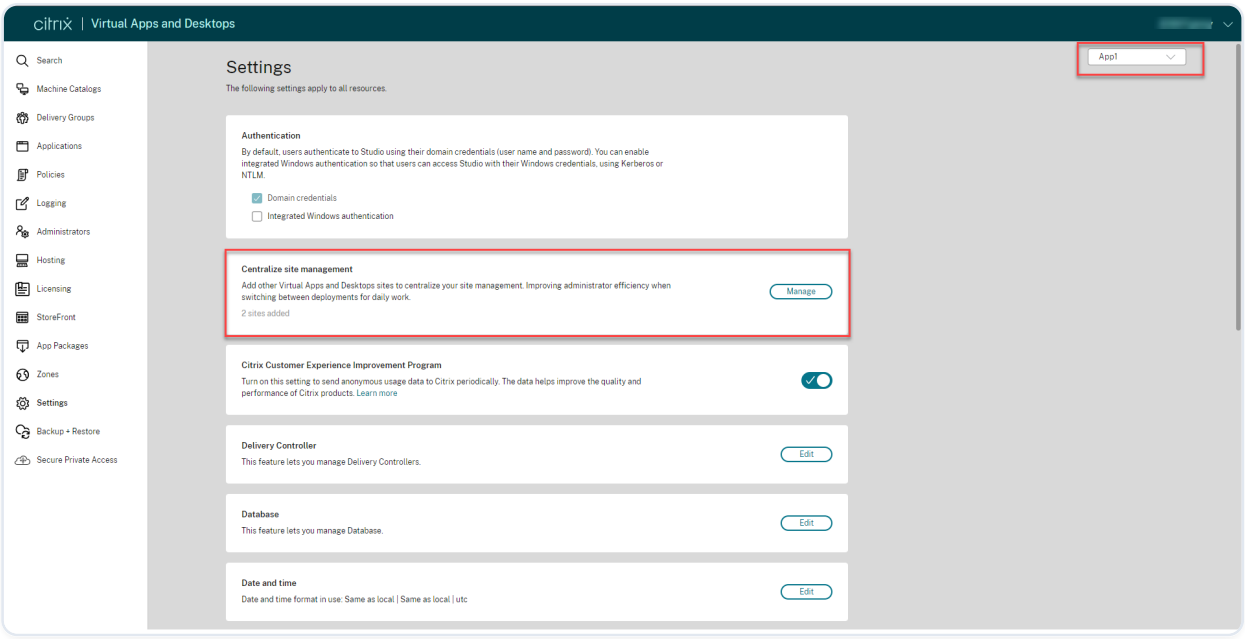


Observação:

O recurso Descobrir adiciona automaticamente os controladores de entrega acessíveis dentro do site com base no endereço do controlador de entrega que você insere.

4. Clique em **Salvar**.

   Para gerenciar ou editar as configurações do site, vá para **Configurações** > **Gerenciamento centralizado de sites** e clique em **Gerenciar**. A opção **Gerenciar** é habilitada apenas para o site principal.



Etapa 3: Gerenciar configurações do site

Atualize seu navegador para que as alterações de configuração do site apareçam. A caixa de seleção de site aparece no canto superior direito do console.

Na página **Configurações**, selecione o site no menu suspenso no canto direito, ao lado do ícone **Atualizar**. O console exibe a configuração do site selecionado.

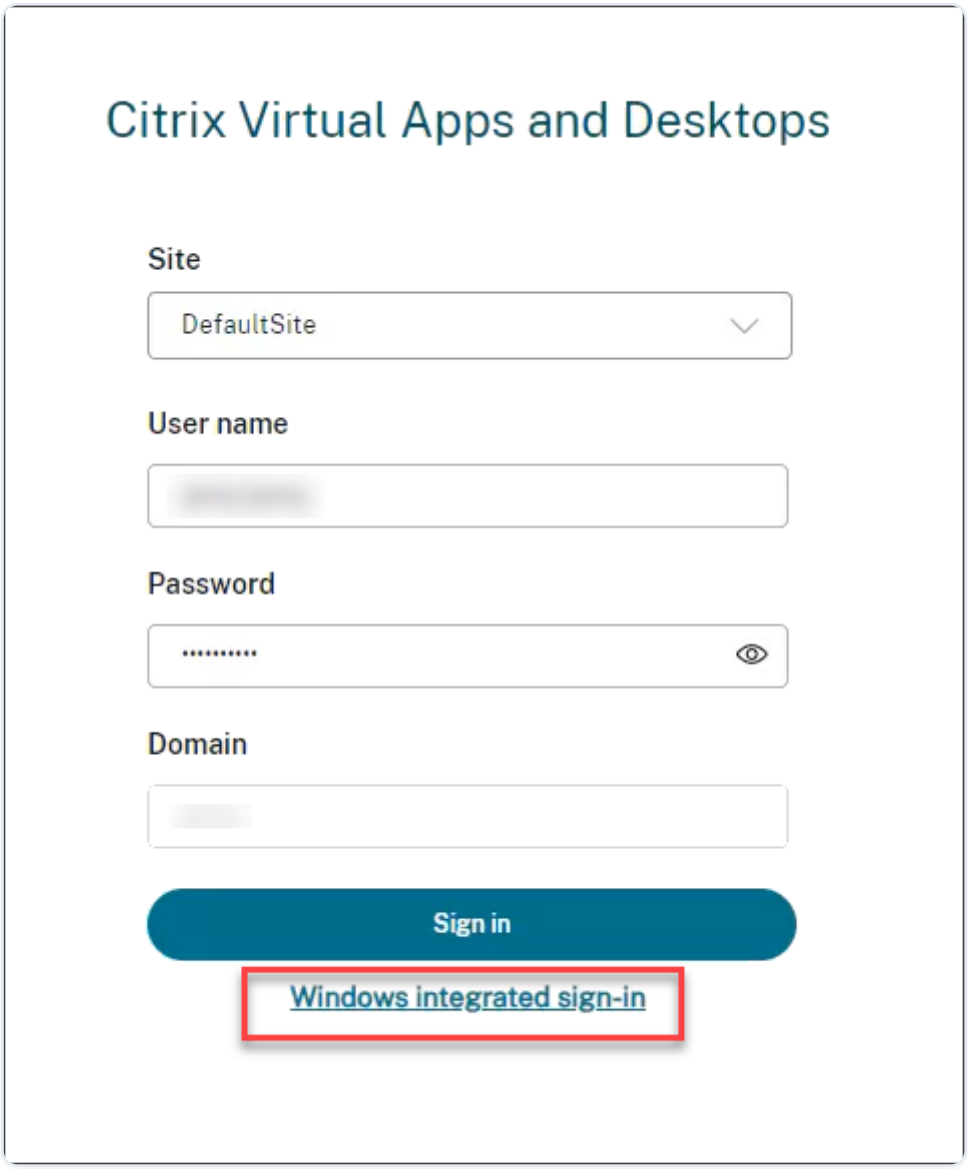
Observação:

- Quando o site principal não está acessível, você não pode acessar outros sites associados a ele.
- Ao alternar para outro site, certifique-se de ter as permissões ou credenciais de acesso necessárias para fazer login.

Experiência de login após a configuração do site

1. Abra um navegador da web. Insira `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Selecione um site no campo **Site**.
3. Selecione **Logon Integrado do Windows** ou insira o **Nome de usuário** e a **Senha** para fazer logon.

> **Observação:**
>
> O Logon Integrado do Windows está disponível apenas se estiver habilitado para o site selecionado. Para obter mais informações sobre a autenticação integrada do Windows, consulte Gerenciar autenticação.



Integrar Acesso Privado Seguro com Web Studio

Introdução

A partir de 2407, ao clicar no link Acesso Privado Seguro no Web Studio, o console do Acesso Privado Seguro é aberto dentro do console do Web Studio.

Anteriormente, o console do Acesso Privado Seguro era aberto em uma guia diferente quando acessado do Web Studio.

Para visualizar o console do Acesso Privado Seguro dentro do Web Studio, você deve executar as duas etapas a seguir:

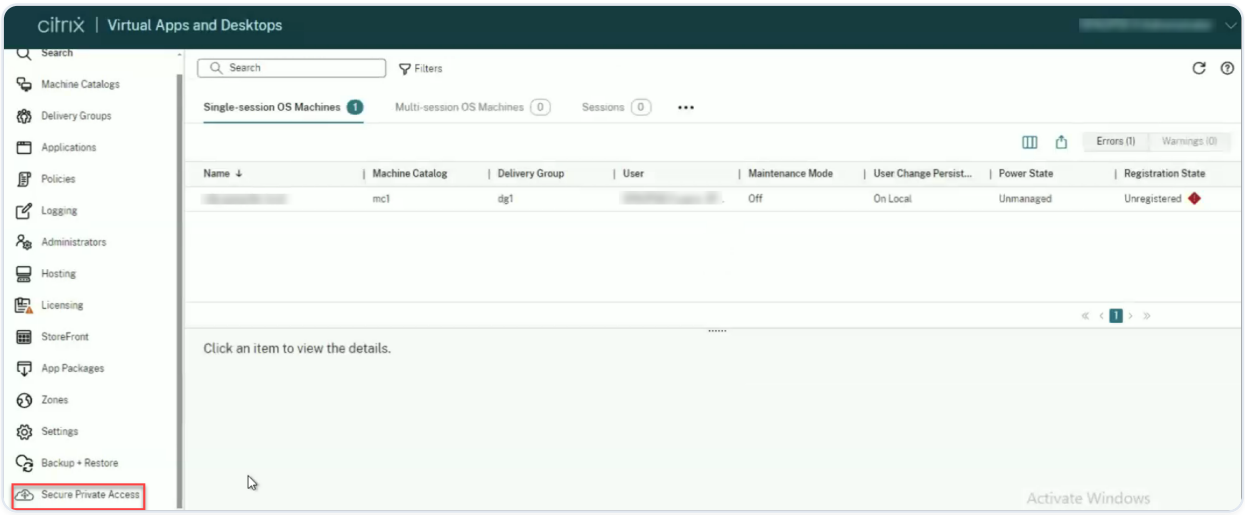
- Edite o arquivo spa-config para adicionar o servidor de Acesso Privado Seguro
- Habilite o logon único para o console do Acesso Privado Seguro

Editar o arquivo spa-config

1. navegar até `C:\Program Files\Citrix\Web Studio\Sites\studio\assets\json` e modifique o conteúdo do arquivo `spa-config.json`.
2. Em `<SpaServer>`, adicione o URL do seu servidor de Acesso Privado Seguro e adicione `<“styleIsolation”: false>` e salve o arquivo.



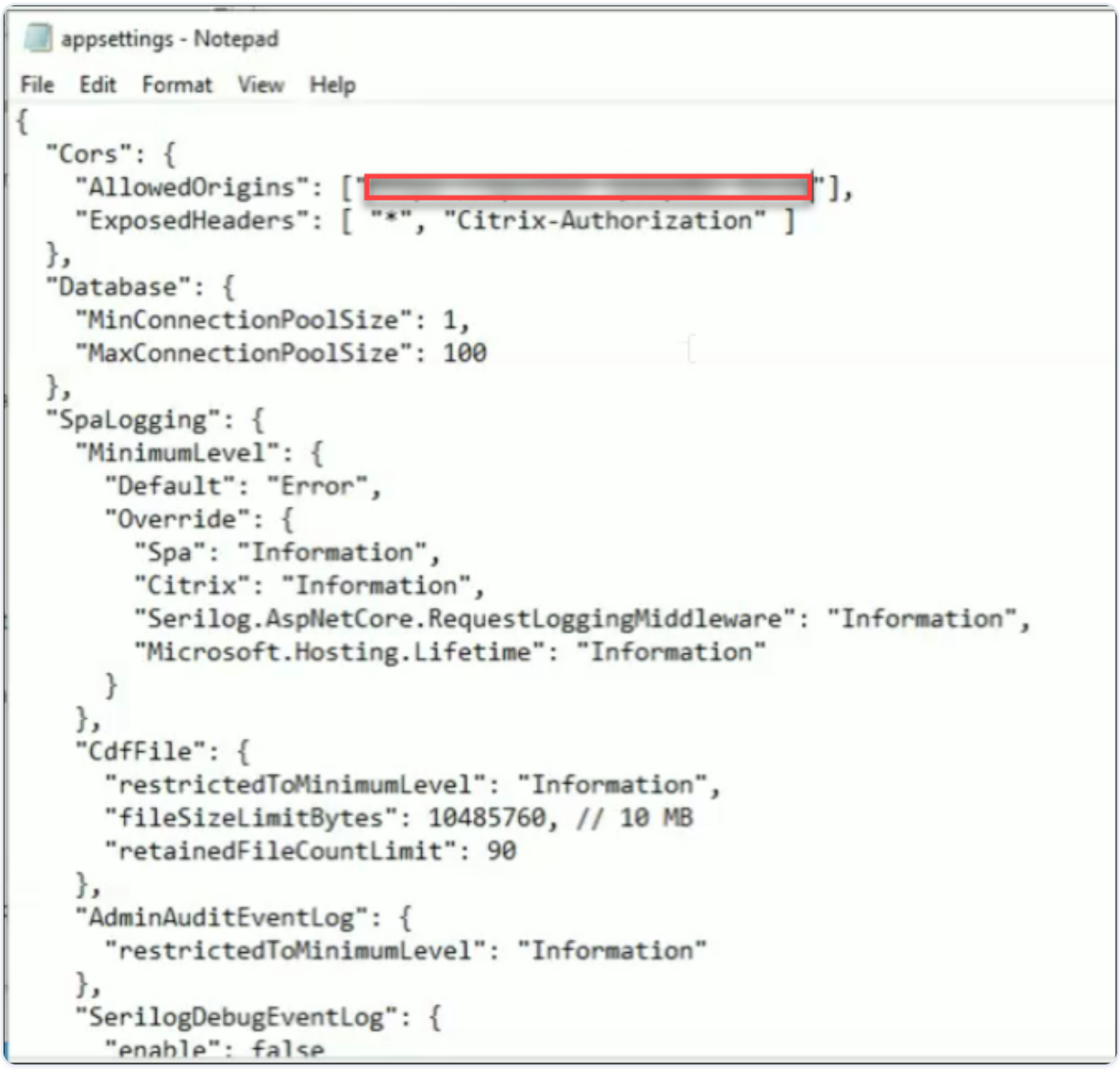
3. Atualize o console do Web Studio.
4. A guia **Acesso Privado Seguro** é exibida no Web Studio.



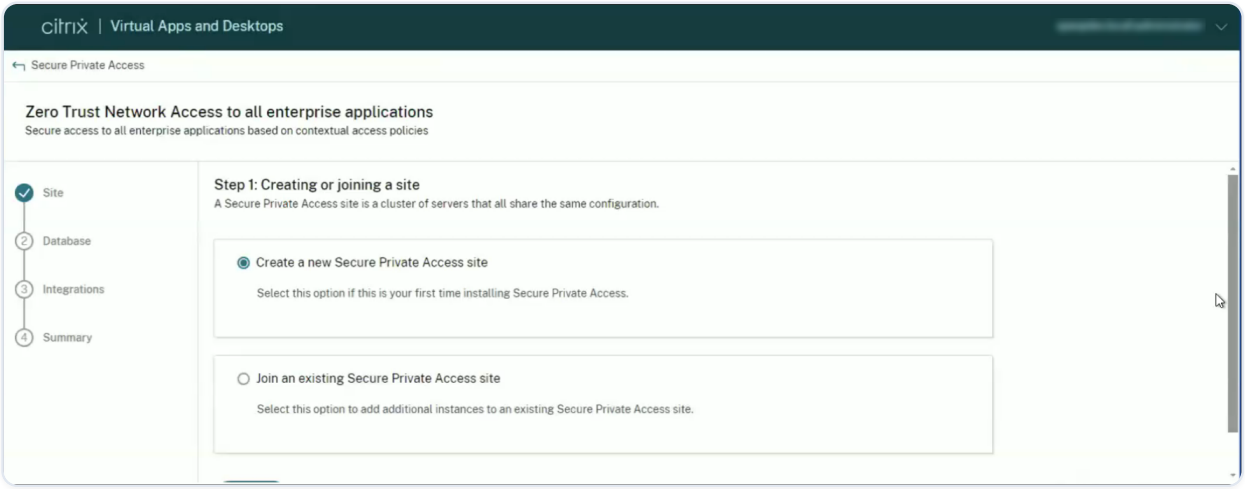
Habilitar logon único para o console do Acesso Privado Seguro

Ao clicar na guia Acesso Privado Seguro dentro da interface do usuário do Web Studio, o console do Acesso Privado Seguro deve ser aberto diretamente. Em vez disso, ele direciona o usuário para uma página de login. Para evitar isso e habilitar o logon único, execute as seguintes etapas:

1. Vá para `C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService` e modifique o conteúdo no arquivo appsettings.
2. No parâmetro `<AllowedOrigins>`, forneça a URL do Web Studio para permitir todo o tráfego do Web Studio dentro do Secure Private Access e salve o arquivo.



3. No Internet Information Services (IIS), reinicie o servidor Secure Private Access.
4. Clique em Secure Private Access no Web Studio. O Secure Private Access é aberto dentro do console do Web Studio.



Identidades de máquina

Cada máquina deve ter uma identidade de máquina exclusiva, também conhecida como conta de computador. As identidades de máquina podem ser criadas e gerenciadas nas máquinas localmente ou em um diretório, como o Active Directory (AD) local ou o Azure AD. O Citrix® oferece suporte à hospedagem de aplicativos e desktops virtuais em máquinas que são ingressadas no Active Directory, ingressadas no Azure Active Directory, ingressadas no Azure Active Directory Híbrido ou não ingressadas no domínio.

Tipos de identidade de máquina

Os seguintes tipos de identidade de máquina são suportados.

TIPO DE IDENTIDADE DE MÁQUINA	DESCRIÇÃO
Ingressado no AD	As identidades são criadas e gerenciadas no Active Directory local. As máquinas provisionadas são ingressadas no Active Directory local usando as identidades de máquina atribuídas.
Ingressado no Azure AD Híbrido	As identidades são criadas no Active Directory local e são sincronizadas com o Azure AD por meio do Azure AD Connect. As máquinas provisionadas são ingressadas no Active Directory local. 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 Virtual Apps and Desktops.
Não ingressado no domínio	As identidades são criadas e gerenciadas nas máquinas localmente. A importação de VMs para o Citrix Virtual Apps and Desktops não é suportada.

Configurações Suportadas

A seguir estão os detalhes das configurações suportadas para cada cenário.

Infraestrutura suportada

IDENTIDADE DA MÁQUINA	CITRIX APLICATIVOS VIRTUAIS E DESKTOPS™	CITRIX WORKSPACE™	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	CITRIX GATEWAY
Associado ao AD	Sim	Sim	Sim	Sim	Sim
Associado ao Azure AD	Não	Sim	Não	Sim	Não
Associado ao Azure AD Híbrido	Sim	Sim	Sim	Sim	Sim
Não associado ao domínio	Sim	Sim	Não	Sim	Não

Provedores de identidade de autenticação de workspace compatíveis

IDENTIDADE DA MÁQUINA	AZURE ACTIVE DIRECTORY	ACTIVE DIRECTORY	ACTIVE DIRECTORY E TOKEN	OKTA	SAML	CITRIX GATEWAY	AUTENTICAÇÃO ADAPTATIVA
Ingressado no AD	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Ingressado no Azure AD	Sim	Não	Não	Não	Não	Não	Não
Ingressado no Azure	Sim	Sim	Sim	Sim	Sim	Sim	Sim

IDENTIDADE DA MÁQUINA	AZURE ACTIVE DIRECTORY	ACTIVE DIRECTORY	ACTIVE DIRECTORY E TOKEN	OKTA	SAML	CITRIX GATEWAY	AUTENTICAÇÃO ADAPTATIVA
AD Híbrido							
Não ingressado no domínio	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Ingressado no Active Directory

O Active Directory é necessário para autenticação e autorização. A infraestrutura Kerberos no Active Directory é usada para garantir a autenticidade e a confidencialidade das comunicações com os Delivery Controllers. Para obter informações sobre o Kerberos, consulte a documentação da Microsoft.

O artigo (/pt-br/citrix-virtual-apps-desktops/2407/system-requirements.html) lista os níveis funcionais suportados para a floresta e o domínio. Para usar o Modelagem de Políticas, o controlador de domínio deve estar executando em todos os sistemas operacionais de servidor suportados. Isso não afeta o nível funcional do domínio.

Este produto suporta:

- **Implantações nas quais as contas de usuário e as contas de computador existem em domínios em uma única floresta do Active Directory.** As contas de usuário e computador podem existir em domínios arbitrários dentro de uma única floresta. Todos os níveis funcionais de domínio e níveis funcionais de floresta são suportados neste tipo de implantação.
- **Implantações nas quais as contas de usuário existem em uma floresta do Active Directory que é diferente da floresta do Active Directory que contém as contas de computador dos Controllers e dos desktops virtuais.** Neste tipo de implantação, os domínios que contêm as contas de computador do Controller e do desktop virtual devem confiar nos domínios que contêm as contas de usuário. Podem ser usadas confianças de floresta ou confianças externas. Todos os níveis funcionais de domínio e níveis funcionais de floresta são suportados neste tipo de implantação.
- **Implantações nas quais as contas de computador para Controllers existem em uma floresta do Active Directory que é diferente de uma ou mais florestas adicionais do**

Active Directory que contêm as contas de computador dos desktops virtuais. Neste tipo de implantação, deve existir uma confiança bidirecional entre os domínios que contêm as contas de computador do Controller e todos os domínios que contêm as contas de computador do desktop virtual. Neste tipo de implantação, todos os domínios que contêm contas de computador do Controller ou do desktop virtual devem estar no nível funcional "Windows 2000 nativo" ou superior. Todos os níveis funcionais de floresta são suportados.

- **Controladores de domínio graváveis.** Controladores de domínio somente leitura não são suportados.

Opcionalmente, os Virtual Delivery Agents (VDAs) podem usar informações publicadas no Active Directory para determinar com quais Controllers eles podem se registrar (descoberta). Este método é suportado principalmente para compatibilidade com versões anteriores e está disponível apenas se os VDAs estiverem na mesma floresta do Active Directory que os Controllers. Para obter informações sobre este método de descoberta, consulte descoberta baseada em OU do Active Directory e CTX118976.

> **Observação:**
>
> Não altere o nome do computador ou a associação de domínio de um Delivery Controller™ depois que o site for configurado.

Implantar em um ambiente de várias florestas do Active Directory

Em um ambiente do Active Directory com várias florestas, se houver confianças unidirecionais ou bidirecionais, você poderá usar encaminhadores DNS ou encaminhadores condicionais para pesquisa e registro de nomes. Para permitir que os usuários apropriados do Active Directory criem contas de computador, use o assistente de Delegação de Controle. Consulte a documentação da Microsoft para obter detalhes sobre este assistente.

Nenhuma zona DNS reversa é necessária na infraestrutura DNS se houver encaminhadores DNS apropriados entre as florestas.

A chave `SupportMultipleForest` é necessária se o VDA e o Controller estiverem em florestas separadas, independentemente de os nomes do Active Directory e do NetBIOS serem diferentes. Use as informações a seguir para adicionar a chave de registro ao VDA e aos Delivery Controllers:

> **Cuidado:**

> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Faça backup do registro antes de editá-lo.

> No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Em todos os Delivery Controllers, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nome: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Você pode precisar de configuração de DNS reverso se o seu namespace DNS for diferente do do Active Directory.

Uma entrada de registro foi adicionada para evitar a habilitação indesejada da autenticação NTLM em VDAs, que é menos segura que o Kerberos. Esta entrada pode ser usada em vez da entrada `SupportMultipleForest`, que ainda pode ser usada para compatibilidade com versões anteriores.

No VDA, configure: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`.

- Nome: `SupportMultipleForestDdcLookup`
- Tipo: `REG_DWORD`
- Dados: `0x00000001 (1)`

Esta chave de registro realiza uma pesquisa DDC em um ambiente de múltiplas florestas com confiança bidirecional que permite remover a autenticação baseada em NTLM durante o processo de registro inicial.

Se houver trusts externos durante a configuração, a chave de registro `ListOfSIDs` é necessária. A chave de registro `ListOfSIDs` também é necessária se o FQDN do Active Directory for diferente do FQDN do DNS, ou se o domínio que contém o Domain Controller tiver um nome NetBIOS diferente do FQDN do Active Directory. Para adicionar a chave de registro, use as seguintes informações:

Para o VDA, localize a chave de registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`.

- Nome: `ListOfSIDs`
- Tipo: `REG_SZ`
- Dados: Identificador de Segurança (SID) dos Controllers. (Os SIDs estão incluídos nos resultados do cmdlet `Get-BrokerController`.)

Quando houver trusts externos, faça a seguinte alteração no VDA:

1. Localize o arquivo `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.
2. Faça uma cópia de backup do arquivo.
3. Abra o arquivo em um programa de edição de texto, como o Bloco de Notas.
4. Localize o texto `allowNtlm="false"` e altere o texto para `allowNtlm="true"`.
5. Salve o arquivo.

Após adicionar a chave de registro `ListOfSIDs` e editar o arquivo `brokeragent.exe.config`, reinicie o Serviço de Área de Trabalho Citrix para aplicar as alterações.

A tabela a seguir lista os tipos de confiança suportados:

TIPO DE CONFIANÇA	TRANSITIVIDADE	DIREÇÃO	SUPORTADO NESTA VERSÃO
Pai e filho	Transitivo	Bidirecional	Sim
Raiz da árvore	Transitivo	Bidirecional	Sim
Externo	Não transitivo	Unidirecional ou bidirecional	Sim
Floresta	Transitivo	Unidirecional ou bidirecional	Sim

TIPO DE CONFIANÇA	TRANSITIVIDADE	DIREÇÃO	SUPORTADO NESTA VERSÃO
Atalho	Transitivo	Unidirecional ou bidirecional	Sim
Realm	Transitivo ou não transitivo	Unidirecional ou bidirecional	Não

Para obter mais informações sobre ambientes complexos do Active Directory, consulte CTX134971.

Ingressado no Azure Active Directory Híbrido

> **Observação:**
>
> Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência a Azure Active Directory, Azure AD ou AAD agora se refere a Microsoft Entra ID.

> Este artigo descreve os requisitos para criar catálogos ingressados no Azure Active Directory Híbrido (HAAD), além dos requisitos descritos na seção de requisitos do sistema.

Máquinas ingressadas no Azure AD Híbrido usam o AD local como provedor de autenticação. Você pode atribuí-las a usuários ou grupos de domínio no AD local. Para habilitar a experiência de SSO contínuo do Azure AD, você precisa ter os usuários de domínio sincronizados com o Azure AD.

> **Observação:**
>
> VMs ingressadas no Azure AD Híbrido são suportadas em infraestruturas de identidade federadas e gerenciadas.

Requisitos

- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2212 ou posterior

- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Qualquer hypervisor ou serviço de nuvem

Limitações

- Se o Citrix Federated Authentication Service (FAS) for usado, o logon único será direcionado para o AD local em vez do Azure AD. Neste caso, é recomendável configurar a autenticação baseada em certificado do Azure AD para que o token de atualização primário (PRT) seja gerado no logon do usuário, o que facilita o logon único para recursos do Azure AD dentro da sessão. Caso contrário, o PRT não estará presente e o SSO para recursos do Azure AD não funcionará. Para obter informações sobre como obter o logon único (SSO) do Azure AD para VDAs híbridos usando o Citrix Federated Authentication Service (FAS), consulte VDAs híbridos.
- Não pule a preparação da imagem ao criar ou atualizar catálogos de máquinas. Se você quiser pular a preparação da imagem, certifique-se de que as VMs mestras não estejam ingressadas no Azure AD ou no Azure AD Híbrido.

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 mestras da seguinte forma. A tarefa de desabilitar manualmente `autoWorkplaceJoin` é necessária apenas para a versão 2212 ou anterior do VDA.

  a. Execute `gpedit.msc`.

  b. navegar até **Configuração do Computador > Modelos Administrativos > Componentes do Windows > Registro de Dispositivo**.

  c. Defina **Registrar computadores ingressados no domínio como dispositivos** como **Desabilitado**.

- Selecione a Unidade Organizacional (UO) que está configurada para ser sincronizada com o Azure AD ao criar as identidades da máquina.
- Para VM mestre baseada no Windows 11 22H2, crie uma tarefa agendada na VM mestre que executa os seguintes comandos na inicialização do sistema usando a conta SYSTEM. Esta

tarefa de agendar uma tarefa na VM mestre é necessária apenas para a versão 2212 ou anterior do VDA.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force
```

```
        Start-Sleep 5
        dsregcmd /join
        break
    }
  }

  Start-Sleep 1
}
```

- Por padrão, o Azure AD Connect sincroniza a cada 30 minutos. As máquinas provisionadas podem levar até 30 minutos para serem ingressadas no Azure AD híbrido durante a primeira inicialização.

Próximos passos

Para obter mais informações sobre como criar catálogos ingressados no Azure Active Directory híbrido, consulte Criar catálogos ingressados no Azure Active Directory híbrido.

Não associado a domínio

Este artigo descreve os requisitos para criar catálogos não associados a domínio usando o Citrix Virtual Apps and Desktops, além dos requisitos descritos na seção Requisitos do Sistema.

Requisitos

- Plano de controle: Consulte Configurações Suportadas
- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2311 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), persistente e não persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Todas as plataformas compatíveis com MCS
- O Rendezvous V2 deve estar habilitado

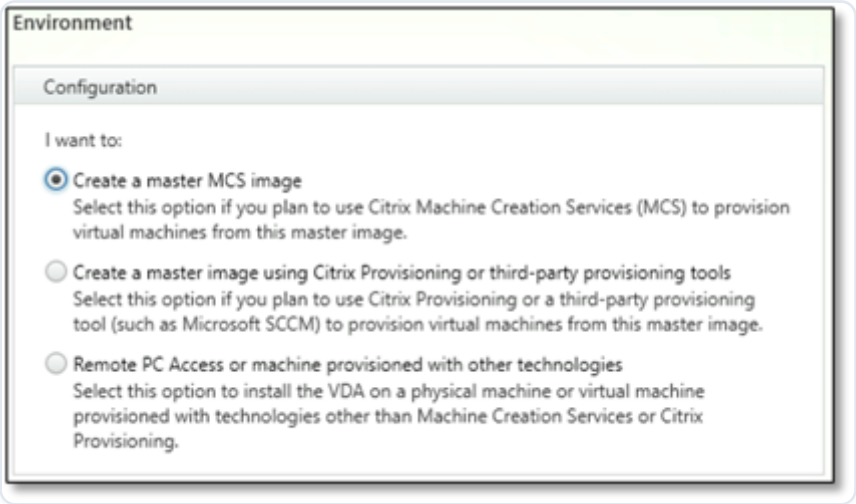
Limitações

- A continuidade do serviço não é suportada.
- Sempre que usamos um VDA de várias sessões não associado a domínio, os dados de perfil do usuário local não são retidos e são excluídos no logoff.

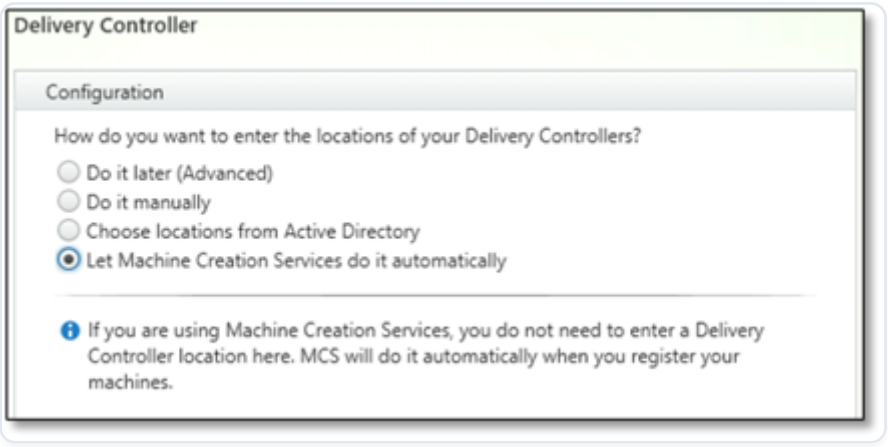
Instalação e configuração do VDA

Siga as etapas para instalar o VDA:

1. Certifique-se de selecionar as seguintes opções no assistente de instalação:
    - Na página Ambiente, selecione **Criar uma imagem mestre MCS**.



    - Na página Delivery Controller™, selecione **Deixar o Machine Creation Services fazer isso automaticamente**.



Próximos passos

Depois que o local do recurso e a conexão de hospedagem estiverem disponíveis, prossiga para criar o catálogo de máquinas. Para obter mais informações sobre como criar catálogos de máquinas não associados a domínio, consulte Criar catálogos não associados a domínio.

Preparar para instalar

A implantação do Citrix Virtual Apps and Desktops™ começa com a instalação dos seguintes componentes. Este processo prepara a entrega de aplicativos e desktops para usuários dentro do seu firewall.

- Um ou mais Delivery Controllers
- Citrix Director
- Citrix StoreFront™
- Citrix License Server
- Um ou mais Citrix Virtual Delivery Agents (VDAs)
- Componentes e tecnologias opcionais, como Universal Print Server, Federated Authentication Service e Self-Service Password Reset

Para usuários fora do seu firewall, instale e configure um componente extra, como o Citrix Gateway. Para uma introdução, consulte Integrar Citrix Virtual Apps and Desktops com Citrix Gateway.

> **Observação:**

> Certifique-se de que os seguintes pré-requisitos da Microsoft sejam atendidos no SO do servidor e no SO da estação de trabalho:

> - Os serviços Microsoft **Volume Shadow Copy** e **Microsoft Software Shadow Copy Provider** estão em execução. Para obter mais informações, consulte Serviço de Cópia de Sombra de Volume.
> - A versão do **MS-Defender** deve ser superior a 4.18.2105.5. Para obter mais informações, consulte Inteligência de segurança e atualizações de produto do Microsoft Defender Antivirus.

> Se sua implantação incluir cargas de trabalho do Windows Server, configure um Microsoft RDS License Server.

Você pode usar o instalador completo do produto no ISO do produto para implantar muitos componentes e tecnologias. Você pode usar um instalador VDA autônomo para instalar VDAs. Os

instaladores VDA autônomos estão disponíveis no site de download da Citrix. Todos os instaladores oferecem interfaces gráficas e de linha de comando. Consulte Instaladores.

O ISO do produto contém scripts de exemplo que instalam, atualizam ou removem VDAs para máquinas em um Active Directory. Você também pode usar os scripts para gerenciar imagens usadas pelo Machine Creation Services (MCS) e Citrix Provisioning (anteriormente Provisioning Services). Para obter detalhes, consulte Instalar VDAs usando scripts.

Informações a serem revisadas antes da instalação

- Visão geral técnica: Para se familiarizar com o produto e seus componentes.
- Segurança: Ao planejar seu ambiente de implantação.
- Problemas conhecidos: Problemas que você pode encontrar nesta versão.
- Bancos de dados: Saiba mais sobre os bancos de dados do sistema e como configurá-los. Durante a instalação do Controller, você pode instalar o SQL Server Express para usar como banco de dados do site. Você configura a maioria das informações do banco de dados ao criar um site, após instalar os componentes principais.
- Acesso Remoto para PC: Se você estiver implantando um ambiente que permite que seus usuários acessem suas máquinas físicas no escritório remotamente.
- Conexões e recursos: Se você estiver usando um hipervisor ou outro serviço para hospedar ou provisionar VMs para aplicativos e desktops. Você pode configurar a primeira conexão ao criar um site (após instalar os componentes principais). Configure seu ambiente de virtualização antes disso.
- Microsoft System Center Configuration Manager: Se você estiver usando o ConfigMgr para gerenciar o acesso a aplicativos e desktops, ou se estiver usando o recurso Wake on LAN com o Acesso Remoto para PC.
- **Conexões de host de Nuvem Pública:** Se você tiver uma Licença de Direitos Híbridos, poderá criar conexões de host para a nuvem pública. Para obter informações relacionadas à Licença de Direitos Híbridos, consulte Renovações de Direitos Híbridos. Para obter informações relacionadas ao direito à nuvem pública e os motivos para essa alteração, consulte CTX270373.

Onde instalar os componentes

Revise os Requisitos do sistema para plataformas, sistemas operacionais e versões suportados. Os pré-requisitos dos componentes são instalados automaticamente, exceto quando indicado.

Consulte a documentação do Citrix StoreFront e do Citrix License Server para suas plataformas e pré-requisitos suportados.

Você pode instalar os componentes principais no mesmo servidor ou em servidores diferentes.

- A instalação de todos os componentes principais em um único servidor pode funcionar para implantações de avaliação, teste ou pequenas produções.
- Para acomodar futuras expansões, considere instalar os componentes em servidores diferentes. Por exemplo, instalar o Studio em uma máquina diferente do servidor onde você instalou o Controller permite gerenciar o site remotamente.
- Para a maioria das implantações de produção, recomenda-se instalar os componentes principais em servidores separados.

  Instale o Citrix License Server e as licenças antes de instalar outros componentes em outros servidores.
- Para instalar um componente compatível em um Server CoreOS (como um Delivery Controller), você deve usar a linha de comando. Esse tipo de SO não oferece uma interface gráfica, então instale o Studio e outras ferramentas em outro lugar e, em seguida, aponte-os para o servidor Controller.

Você pode instalar um Delivery Controller™ e um VDA para SO multi-sessão no mesmo servidor. Inicie o instalador e selecione o Delivery Controller (além de quaisquer outros componentes principais que você deseja nessa máquina). Em seguida, inicie o instalador novamente e selecione o **Virtual Delivery Agent** para SO multi-sessão.

Certifique-se de que cada sistema operacional tenha as atualizações mais recentes.

Certifique-se de que todas as máquinas tenham os relógios do sistema sincronizados. A infraestrutura Kerberos que protege a comunicação entre as máquinas requer sincronização.

Com XenServers, o estado de energia da máquina virtual pode aparecer como desconhecido, mesmo que pareça registrado. Para resolver esse problema, edite o valor da chave de registro `HostTime` para desabilitar a sincronização de tempo com o host:

`HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"`

`HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"`

> **Dica:**

> O valor padrão é `HostTime="UTC"`. Altere este valor para algo diferente de UTC, por exemplo, `Local`. Essa alteração desabilita efetivamente a sincronização de tempo com o host.

> Orientações de otimização para máquinas Windows 10 de sessão única estão disponíveis em CTX216252.

Onde NÃO instalar componentes:

- Não instale nenhum componente em um controlador de domínio do Active Directory.
- Não há suporte para a instalação de um Controller em um nó em uma instalação de cluster do SQL Server, instalação de espelhamento do SQL Server ou em um servidor executando o Hyper-V.

Se você tentar instalar ou atualizar um VDA em um SO Windows que esta versão do produto não suporta, uma mensagem o guiará para um artigo que descreve as opções.

Requisitos de permissão e Active Directory

Você deve ser um usuário de domínio e um administrador local nas máquinas onde você está instalando os componentes.

Para usar um instalador VDA autônomo, você deve ter privilégios administrativos elevados ou usar **Executar como administrador**.

Configure seu domínio do Active Directory antes de iniciar uma instalação.

- Requisitos do sistema lista os níveis funcionais do Active Directory suportados. Active Directory unido contém mais informações.
- Você deve ter pelo menos um controlador de domínio executando os Serviços de Domínio do Active Directory.
- Não instale nenhum componente do Citrix Virtual Apps and Desktops em um controlador de domínio.
- Não use uma barra (/) ao especificar nomes de Unidades Organizacionais no Studio.

A conta de usuário do Windows usada para instalar o Citrix License Server é configurada automaticamente como um administrador completo de administração delegada.

Para mais informações:

- Melhores práticas de segurança
- Administração delegada
- Documentação da Microsoft para configuração do Active Directory

Orientação de instalação, considerações e melhores práticas

Durante a instalação de qualquer componente

- Ao instalar ou atualizar um Delivery Controller, Studio, License Server ou Director a partir da mídia do produto completo, se o instalador Citrix detectar que uma reinicialização está pendente de uma instalação anterior do Windows na máquina, o instalador para com o código de saída/retorno 9. Você será solicitado a reiniciar a máquina.

  Esta não é uma reinicialização forçada do Citrix. É devido a outros componentes instalados anteriormente na máquina. Se isso ocorrer, reinicie a máquina e, em seguida, inicie o instalador Citrix novamente.

  Ao usar a interface de linha de comando, você pode evitar a verificação da reinicialização pendente incluindo a opção `/no_pending_reboot_check` no comando.
- Geralmente, se um componente tiver pré-requisitos, o instalador os implanta se não estiverem presentes. Alguns pré-requisitos podem exigir a reinicialização da máquina.
- Ao criar objetos antes, durante e após a instalação, especifique nomes exclusivos para cada objeto. Por exemplo, forneça nomes exclusivos para redes, grupos, catálogos e recursos.
- Se um componente não for instalado com êxito, a instalação será interrompida com uma mensagem de erro. Os componentes instalados com êxito são mantidos. Você não precisa reinstalá-los.
- O Citrix Analytics é coletado automaticamente quando você instala (ou atualiza) componentes. Por padrão, esses dados são carregados para a Citrix automaticamente quando a instalação é concluída. Além disso, ao instalar componentes, você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix, que carrega dados anônimos.

  Durante a instalação, você também pode optar por participar de outras tecnologias Citrix que coletam diagnósticos para manutenção e solução de problemas. Para obter informações sobre esses programas, consulte Citrix Insight Services.
- O Google Analytics é coletado (e posteriormente carregado) automaticamente quando você instala (ou atualiza) o Studio. Após a instalação do Studio, você pode alterar essa configuração com a chave do Registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Um valor de **1** habilita a coleta e o upload, **0** desabilita a coleta e o upload.

- Se uma instalação de VDA falhar, um analisador MSI analisa o log MSI com falha, exibindo o código de erro exato. O analisador sugere um artigo CTX, se for um problema conhecido. O analisador também coleta dados anonimizados sobre o código de erro da falha. Esses dados são incluídos com outros dados coletados pelo CEIP. Se você encerrar a inscrição no CEIP, os dados coletados pelo analisador MSI não serão mais enviados à Citrix.

Durante a instalação do VDA

- O Citrix Workspace™ app para Windows está disponível, mas não é instalado por padrão ao instalar um VDA. Você ou seus usuários podem baixar e instalar (e atualizar) o Citrix Workspace app para Windows e outros aplicativos Citrix Workspace no site da Citrix. Alternativamente, você pode disponibilizar esses aplicativos Citrix Workspace a partir do seu servidor StoreFront. Consulte a documentação do StoreFront.
- O Serviço de Spooler de Impressão da Microsoft deve estar habilitado. Você não pode instalar um VDA com êxito se esse serviço estiver desabilitado.
- A maioria das edições do Windows compatíveis vem com o Microsoft Media Foundation já instalado. Se a máquina não tiver o Media Foundation (como as edições N), vários recursos multimídia não serão instalados e não funcionarão.
  - Redirecionamento de Mídia do Windows
  - Redirecionamento de Vídeo HTML5
  - Redirecionamento de Webcam HDX™ RealTime

  Você pode reconhecer a limitação ou encerrar a instalação do VDA e reiniciá-la mais tarde, após instalar o Media Foundation. Na interface gráfica, essa escolha é apresentada em uma mensagem. Na linha de comando, você pode usar a opção `/no_mediafoundation_ack` para reconhecer a limitação.
- Ao instalar o VDA, um novo grupo de usuários local chamado **Direct Access Users** é criado automaticamente. Em um VDA para SO de sessão única, este grupo se aplica apenas a conexões RDP. Em um VDA para SO de múltiplas sessões, este grupo se aplica a conexões ICA® e RDP.
- O VDA deve ter endereços de Controller válidos para se comunicar. Caso contrário, as sessões não podem ser estabelecidas. Você pode especificar os endereços do Controller ao instalar o VDA ou posteriormente. Lembre-se de que isso deve ser feito. Para obter mais informações, consulte Registro do VDA.

Reinicializações após e durante a instalação do VDA

É necessário reiniciar ao final da instalação do VDA. Essa reinicialização ocorre automaticamente por padrão.

Ao atualizar um VDA para a versão 7.17 (ou uma versão posterior compatível), ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Para minimizar o número de reinicializações necessárias durante a instalação do VDA:

- Certifique-se de que uma versão compatível do .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas com SO Windows multi-sessão, instale e habilite os serviços de função RDS antes de instalar o VDA.

Se você não instalar esses pré-requisitos antes de instalar o VDA:

- Se você estiver usando a interface gráfica ou a interface de linha de comando sem a opção `/noreboot`, a máquina reinicia automaticamente após a instalação do pré-requisito.
- Se você estiver usando a interface de linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Ao atualizar uma versão do VDA, ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Restaurar em caso de falha na instalação ou atualização

> **Observação:**

> Este recurso está disponível para VDAs de sessão única e multi-sessão.

> Se uma instalação ou atualização de VDA de sessão única falhar, e o recurso "restaurar em caso de falha" estiver habilitado, a máquina é retornada a um ponto de restauração que foi definido antes do início da instalação ou atualização.

Se uma instalação ou atualização de VDA multi-sessão falhar, e o recurso "restaurar em caso de falha" estiver habilitado, a máquina é retornada a um backup que foi realizado antes do início da instalação ou atualização.

Quando uma instalação ou atualização de VDA de sessão única é iniciada com este recurso habilitado, o instalador cria um ponto de restauração do sistema antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado do ponto de restauração. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração.

Quando uma instalação ou atualização de VDA multi-sessão é iniciada com este recurso habilitado, o instalador cria um backup do servidor antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado de backup. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração. O tempo para criar o backup do servidor é baseado no tamanho do backup necessário e na quantidade de recursos disponíveis para o servidor. O backup é armazenado em *C:\WindowsImageBackup\servername*.

Por padrão, este recurso está desabilitado.

Se você planeja habilitar este recurso, certifique-se de que a restauração do sistema não esteja desabilitada por meio de uma configuração de GPO (`Computer Configuration > Administrative Templates > System > System Restore`).

> **Observação:**
>
> Essa configuração de GPO não se aplica à restauração de um VDA multi-sessão.

Para habilitar este recurso ao instalar ou atualizar um VDA de sessão única ou multi-sessão:

- Ao usar a interface gráfica de um instalador VDA (como usando **Autostart** ou o comando `XenDesktopVDASetup.exe` sem quaisquer opções de restauração ou silenciosas), selecione a caixa de seleção **Habilitar restauração automática se a atualização falhar** na página **Resumo**.

  Se a instalação/atualização for concluída com sucesso, o ponto de restauração/backup não é usado, mas é retido.
- Execute um instalador VDA com a opção `/enablerestore` ou `/enablerestorecleanup` usando a linha de comando.
  - Se você usar a opção `/enablerestorecleanup`, e a instalação/atualização for concluída com sucesso, o ponto de restauração/backup do servidor será removido automaticamente.

- Se você usar a opção `/enablerestore`, e a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será retido.

Instaladores

Instalador completo do produto

Usando o instalador completo do produto fornecido na ISO, você pode:

- Instalar, atualizar ou remover componentes principais: Delivery Controller, Studio, Director e License Server.
- Instalar ou atualizar o StoreFront.
- Instalar ou atualizar VDAs do Windows para sistemas operacionais de sessão única ou multi-sessão.
- Instale o componente `UpsServer` do Universal Print Server em seus servidores de impressão.
- Instale o Federated Authentication Service.
- Instale o Session Recording.
- Instale o Workspace Environment Management.

> **Observação:**
>
> O instalador do Workspace Environment Management™ Agent não está localizado. Ele está disponível apenas em inglês.

Para entregar um desktop de um SO multi-sessão para um usuário (por exemplo, para desenvolvimento web), use a interface de linha de comando do instalador do produto completo. Para obter detalhes, consulte Server VDI.

Instaladores VDA autônomos

Os instaladores VDA autônomos estão disponíveis nas páginas de download da Citrix. (Eles não estão disponíveis na mídia de instalação do produto.) Os instaladores VDA autônomos são muito menores do que a ISO do produto completo. Eles acomodam mais facilmente implantações que:

- Usam pacotes de Distribuição Eletrônica de Software (ESD) que são preparados ou copiados localmente

- Possuem máquinas físicas
- Possuem escritórios remotos

Por padrão, os arquivos nos VDAs autônomos de autoextração são extraídos para a pasta **Temp**. É necessário mais espaço em disco na máquina ao extrair para a pasta **Temp** do que ao usar o instalador do produto completo. No entanto, os arquivos extraídos para a pasta **Temp** são automaticamente excluídos após a conclusão da instalação. Alternativamente, você pode usar o comando `/extract` com um caminho absoluto.

Três instaladores VDA autônomos estão disponíveis para download.

VDAServerSetup.exe:

Instala um VDA para SO multi-sessão. Ele oferece suporte a todas as opções de VDA para SO multi-sessão que estão disponíveis com o instalador do produto completo.

VDAWorkstationSetup.exe:

Instala um VDA para SO de sessão única. Ele oferece suporte a todas as opções de VDA para SO de sessão única que estão disponíveis com o instalador do produto completo.

VDAWorkstationCoreSetup.exe:

Instala um VDA para SO de sessão única otimizado para implantações de Acesso Remoto a PC ou instalações VDI principais. O Acesso Remoto a PC usa máquinas físicas. As instalações VDI principais são VMs que não estão sendo usadas como uma imagem. Ele instala apenas os serviços principais necessários para conexões VDA nessas implantações. Portanto, ele oferece suporte apenas a um subconjunto das opções válidas com o instalador do produto completo ou `VDAWorkstationSetup.exe`.

Este instalador não instala nem contém os componentes usados para:

- App-V.
- Gerenciamento de Perfis. Excluir o Citrix Profile Management da instalação afeta as exibições do Citrix Director. Para obter detalhes, consulte Instalar VDAs.
- Serviço de Identidade da Máquina.
- Ferramentas de Suporte Citrix.
- Citrix Files para Windows.
- Citrix Files para Outlook.

O instalador `VDAWorkstationCoreSetup.exe` não instala nem contém um aplicativo Citrix Workspace para Windows.

Usar `VDAWorkstationCoreSetup.exe` é equivalente a usar o instalador do produto completo ou `VDAWorkstationSetup` para instalar um VDA de SO de sessão única e uma das seguintes opções:

- Na interface gráfica: Selecionar a opção Acesso Remoto a PC na página **Ambiente**.
- Na interface de linha de comando: Especificando a opção `/remotepc`.
- Na interface de linha de comando: Especificando `/components vda` mais a opção `/exclude` que lista todos os nomes de componentes adicionais válidos.

Você pode instalar os componentes/recursos omitidos posteriormente executando o instalador completo do produto. Essa ação permite que você instale todos os componentes ausentes.

O instalador `VDAWorkstationCoreSetup.exe` instala automaticamente o MSI de Redirecionamento de Conteúdo do Navegador. Esta instalação automática se aplica à versão 2003 do VDA e versões posteriores suportadas.

Códigos de retorno da instalação do Citrix

O log de instalação contém o resultado das instalações de componentes como um código de retorno do Citrix, não um valor da Microsoft.

- 0 = Sucesso
- 1 = Falha
- 2 = SucessoParcial
- 3 = SucessoParcialEReincializaçãoNecessária
- 4 = FalhaEReincializaçãoNecessária
- 5 = UsuárioCancelou
- 6 = ArgumentoDeLinhaDeComandoInválido
- 7 = VersãoMaisRecenteEncontrada
- 8 = SucessoEReincializaçãoNecessária
- 9 = FileLockReboot
- 10 = Abortado
- 11 = FailedMedia

- 12 = FailedLicense
- 13 = FailedPrecheck
- 14 = AbortedPendingRebootCheck

Por exemplo, ao usar ferramentas como o Microsoft System Center Configuration Manager, uma instalação de VDA por script pode parecer falhar quando o log de instalação contém o código de retorno 3. Isso pode ocorrer quando o instalador do VDA está aguardando uma reinicialização que você deve iniciar (por exemplo, após a instalação de um pré-requisito de função RDS em um servidor). Uma instalação de VDA é considerada bem-sucedida somente depois que todos os pré-requisitos e componentes selecionados são instalados e a máquina é reiniciada após a instalação.

Alternativamente, você pode encapsular sua instalação em scripts CMD (que retornam códigos de saída da Microsoft) ou alterar os códigos de sucesso em seu pacote do Configuration Manager.

Configurar um Servidor de Licenças RDS da Microsoft para cargas de trabalho do Windows Server

Este produto acessa os recursos de sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2016. Isso geralmente requer uma licença de acesso de cliente dos Serviços de Área de Trabalho Remota (RDS CAL). O VDA deve ser capaz de contatar um servidor de licenças RDS para solicitar CALs RDS. Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento da Microsoft Activate the Remote Desktop Services License Server. Para ambientes de prova de conceito, você pode usar o período de carência fornecido pela Microsoft.

Com este método, você pode fazer com que este serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações de Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft License your RDS deployment with client access licenses (CALs).

Para configurar o servidor de licenças RDS usando as configurações de Política de Grupo:

1. Instale um Servidor de Licenças dos Serviços de Área de Trabalho Remota em uma máquina disponível. A máquina deve estar sempre disponível. As cargas de trabalho do produto Citrix devem ser capazes de alcançar este servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

As cargas de trabalho do Windows 10 exigem a ativação apropriada da licença do Windows 10. Recomendamos que você siga a documentação da Microsoft para ativar as cargas de trabalho do Windows 10.

Mais informações

Para configurar o local do recurso para tipos de host específicos:

- Ambientes de nuvem AWS(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/aws.html)
- Ambientes de virtualização XenServer
- Ambientes do Google Cloud(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/gcp.html)
- Ambientes de nuvem do Microsoft Azure Resource Manager(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/azure.html)
- Ambientes do Microsoft System Center Configuration Manager(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/configmgr.html)
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix
- Ambientes de virtualização VMware
- Soluções de nuvem e parceiros VMware

Ambientes de nuvem AWS

Este artigo orienta você na configuração de sua conta AWS como um local de recurso que você pode usar com o Citrix Virtual Apps and Desktops. O local de recurso inclui um conjunto básico de componentes, ideal para uma prova de conceito ou outra implantação que não exija recursos espalhados por várias zonas de disponibilidade. Depois de concluir essas tarefas, você pode instalar VDAs, provisionar máquinas, criar catálogos de máquinas e criar Grupos de Entrega.

Ao concluir as tarefas neste artigo, seu local de recurso inclui os seguintes componentes:

- Uma nuvem privada virtual (VPC) com sub-redes públicas e privadas dentro de uma única zona de disponibilidade.
- Uma instância que funciona como um Controlador de Domínio do Active Directory e servidor DNS, localizada na sub-rede privada da VPC.

- Uma instância que atua como um host bastion na sub-rede pública da sua VPC. Esta instância é usada para iniciar conexões RDP com as instâncias na sub-rede privada para fins de administração. Depois de concluir a configuração do seu local de recurso, você pode desligar esta instância para que ela não esteja mais prontamente acessível. Quando você precisar gerenciar outras instâncias na sub-rede privada, como instâncias VDA, você pode reiniciar a instância do host bastion.

Visão geral da tarefa

Configure uma nuvem privada virtual (VPC) com sub-redes públicas e privadas. Ao concluir esta tarefa, a AWS implanta um gateway NAT com um endereço IP Elástico na sub-rede pública. Esta ação permite que as instâncias na sub-rede privada acessem a Internet. As instâncias na sub-rede pública são acessíveis ao tráfego público de entrada, enquanto as instâncias na sub-rede privada não são.

Configurar grupos de segurança. Os grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também associa esses grupos de segurança a cada instância em sua VPC.

Crie um conjunto de opções DHCP. Com uma VPC da Amazon, os serviços DHCP e DNS são fornecidos por padrão, o que afeta como você configura o DNS em seu Controlador de Domínio do Active Directory. O DHCP da Amazon não pode ser desativado e o DNS da Amazon pode ser usado apenas para resolução de DNS público, não para resolução de nomes do Active Directory. Para especificar o domínio e os servidores de nomes entregues às instâncias via DHCP, crie um conjunto de opções DHCP. O conjunto atribui o sufixo de domínio do Active Directory e especifica o servidor DNS para todas as instâncias em sua VPC. Para garantir que os registros de Host (A) e Reverse Lookup (PTR) sejam registrados automaticamente quando as instâncias ingressarem no domínio, você configura as propriedades do adaptador de rede para cada instância que você adicionar à sub-rede privada.

Adicione um host bastion e um Controlador de Domínio à VPC. Através do host bastion, você pode fazer logon em instâncias na sub-rede privada para configurar o domínio e ingressar instâncias no domínio.

Tarefa 1: Configurar a VPC

1. No console de gerenciamento da AWS, selecione **VPC**.
2. No Painel da VPC, selecione **Criar VPC**.

3. Selecione **VPC e mais**.
4. Em NAT gateways ($), selecione **Em 1 AZ** ou **1 por AZ**.
5. Em opções de DNS, deixe **Habilitar nomes de host DNS** selecionado.
6. Selecione **Criar VPC**. A AWS cria as sub-redes públicas e privadas, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

Tarefa 2: Configurar grupos de segurança

Esta tarefa cria e configura os seguintes grupos de segurança para sua VPC:

- Um grupo de segurança público para associar às instâncias em sua sub-rede pública.
- Um grupo de segurança privado para associar às instâncias em sua sub-rede privada.

Para criar os grupos de segurança:

1. No Painel da VPC, selecione **Grupos de Segurança**.
2. Crie um grupo de segurança para o grupo de segurança público. Selecione **Criar Grupo de Segurança** e insira uma tag de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Sim, Criar**.

Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	ORIGEM
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	Selecione o grupo de segurança Público.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Confiabilidade da Sessão)	0.0.0.0/0

TIPO	ORIGEM
3389 (RDP)	0.0.0.0/0

3. Quando terminar, selecione **Salvar**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	DESTINO
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	0.0.0.0/0
ICMP	0.0.0.0/0

5. Quando terminar, selecione **Salvar**.

Configurar o grupo de segurança privado

1. Na lista de grupos de segurança, selecione o grupo de segurança Privado.
2. Se você não configurou o tráfego do grupo de segurança público, você deve definir as portas TCP; selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	ORIGEM
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	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.
TCP 389	Selecione o grupo de segurança Público.
UDP 389	Selecione o grupo de segurança Público.

TIPO	ORIGEM
443 (HTTPS)	Selecione o grupo de segurança Público.
TCP 1494 (ICA/HDX)	Selecione o grupo de segurança Público.
TCP 2598 (Confiabilidade da Sessão)	Selecione o grupo de segurança Público.
3389 (RDP)	Selecione o grupo de segurança Público.
TCP 49152–65535	Selecione o grupo de segurança Público.

3. Quando terminar, selecione **Salvar.**
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	DESTINO
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Quando terminar, selecione **Salvar**.

Tarefa 3: Iniciar instâncias

Siga as etapas abaixo para criar duas instâncias EC2 e descriptografar a senha padrão de Administrador que a Amazon gera:

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No Painel do EC2, selecione **Iniciar Instância**.
3. Selecione uma imagem de máquina do Windows Server e o tipo de instância.
4. Na página **Configure Instance Details**, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Sub-rede**, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione a sub-rede Pública

- Controlador de Domínio: Selecione a sub-rede Privada

6. Em **Atribuir automaticamente endereço IP público**, faça as seguintes seleções para cada instância:
   - Host bastion: Selecione **Enable.**
   - Controlador de Domínio: Selecione **Use default setting** ou **Disable**.
7. Em **Network Interfaces**, insira um endereço IP primário dentro do intervalo de IP da sua sub-rede privada para o Controlador de Domínio.
8. Se necessário, na página **Adicionar Armazenamento**, modifique o tamanho do disco.
9. Na página **Marcar Instância**, insira um nome amigável para cada instância.
10. Na página **Configurar Grupos de Segurança**, selecione **Selecionar um grupo de segurança existente** e, em seguida, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione o grupo de segurança Público.
    - Controlador de Domínio: Selecione o grupo de segurança Privado.
11. Revise suas seleções e, em seguida, selecione **Iniciar**.
12. Crie um novo par de chaves ou selecione um existente. Se você criar um novo par de chaves, baixe seu arquivo de chave privada (.pem) e guarde-o em um local seguro. Você deve fornecer sua chave privada ao adquirir a senha padrão do Administrador para a instância.
13. Selecione **Launch Instances**. selecione **View Instances** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-lançada tenha passado em todas as verificações de status antes de acessá-la.
14. Adquira a senha padrão do Administrador para cada instância:
    a. Na lista de instâncias, selecione a instância e, em seguida, selecione **Conectar**.
    b. Vá para a guia **Cliente RDP**, selecione **Obter Senha** e carregue seu arquivo de chave privada (`.pem`) quando solicitado.
    c. Selecione **Descriptografar Senha** para obter a senha legível. A AWS exibe a senha padrão.
15. Repita os passos a partir do passo 2 até ter criado duas instâncias:
    - Uma instância de host bastion em sua sub-rede pública
    - Uma instância na sua sub-rede privada que será usada como Controlador de Domínio.

Tarefa 4: Criar um conjunto de opções DHCP

1. No Painel da VPC, selecione **Conjuntos de Opções DHCP**.
2. Insira as seguintes informações:
    - Tag de nome: Insira um nome amigável para o conjunto.
    - Nome de domínio: Insira o nome de domínio totalmente qualificado que você usa ao configurar a instância do Controlador de Domínio.
    - Servidores de nome de domínio: Insira o endereço IP privado que você atribuiu à instância do Controlador de Domínio e a string **AmazonProvidedDNS**, separados por vírgulas.
    - Servidores NTP: Deixe este campo em branco.
    - Servidores de nome NetBIOS: Insira o endereço IP privado da instância do Controlador de Domínio.
    - Tipo de nó NetBIOS: Insira **2**.
3. Selecione **Sim, Criar.**
4. Associe o novo conjunto à sua VPC:
    a. No Painel da VPC, selecione **Suas VPCs** e, em seguida, selecione a VPC que você configurou anteriormente.
    b. Selecione **Ações > Editar Conjunto de Opções DHCP**.
    c. Quando solicitado, selecione o novo conjunto que você criou e, em seguida, selecione **Salvar**.

Tarefa 5: Configurar as instâncias

1. Usando um cliente RDP, conecte-se ao endereço IP público da instância do host bastion. Quando solicitado, insira as credenciais da conta de Administrador.
2. A partir da instância do host bastion, inicie a Conexão de Área de Trabalho Remota e conecte-se ao endereço IP privado da instância que você deseja configurar. Quando solicitado, insira as credenciais de Administrador para a instância.
3. Para todas as instâncias na sub-rede privada, configure as configurações de DNS:
    a. Selecione **Iniciar > Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento > Alterar configurações do adaptador**. Clique duas vezes na conexão de rede exibida.
    b. Selecione **Propriedades > Protocolo de Internet Versão 4 (TCP/IPv4) > Propriedades**.

c. Selecione **Avançado > DNS**. Certifique-se de que as seguintes configurações estejam ativadas e selecione **OK**:

- Registrar os endereços desta conexão no DNS
- Usar o sufixo DNS desta conexão no registro DNS

4. Para configurar o Controlador de Domínio:

a. Usando o Gerenciador de Servidores, adicione a função Serviços de Domínio Active Directory com todos os recursos padrão.

b. Promova a instância a um Controlador de Domínio. Durante a promoção, habilite o DNS e use o nome de domínio que você especificou ao criar o conjunto de opções DHCP. Reinicie a instância quando solicitado.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão na AWS, consulte Conexão com a AWS

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes do Google Cloud

O 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 apenas no Citrix Cloud.
- 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 novo.
- Habilite quatro APIs em seu projeto do Google Cloud. Para obter detalhes, consulte Habilitar APIs do Google Cloud.

- Conta de serviço do Google Cloud. A conta de serviço autentica-se no Google Cloud para permitir o acesso ao projeto. Para obter detalhes, consulte Configurar e atualizar contas de serviço.
- Habilite o acesso privado do Google. Para obter detalhes, consulte Habilitar acesso privado do Google.

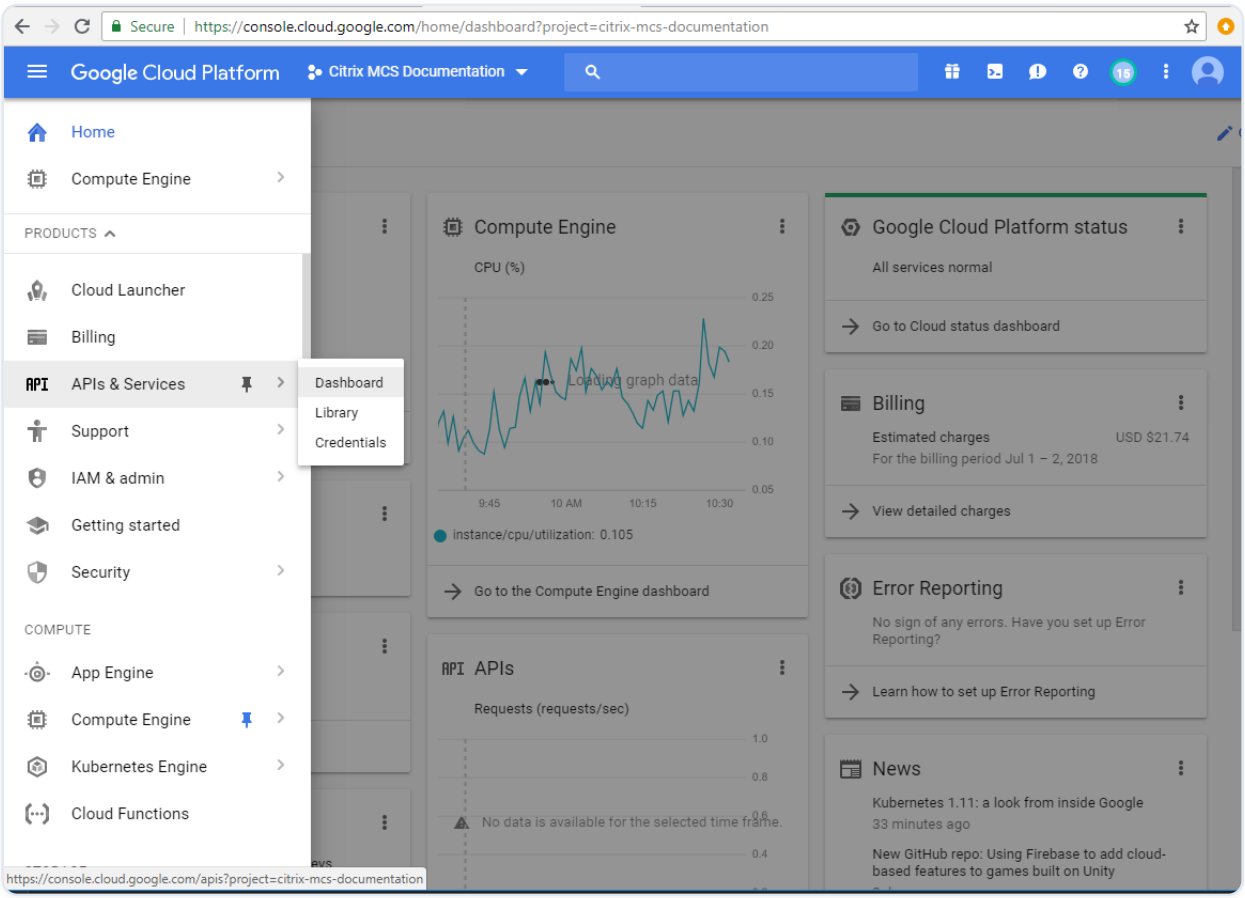
Habilitar APIs do Google Cloud

Para usar a funcionalidade do Google Cloud através do Web Studio, habilite estas APIs em seu projeto do Google Cloud:

- Compute Engine API
- Cloud Resource Manager API
- API de Gerenciamento de Identidade e Acesso (IAM)
- Cloud Build API
- Cloud Key Management Service (KMS)

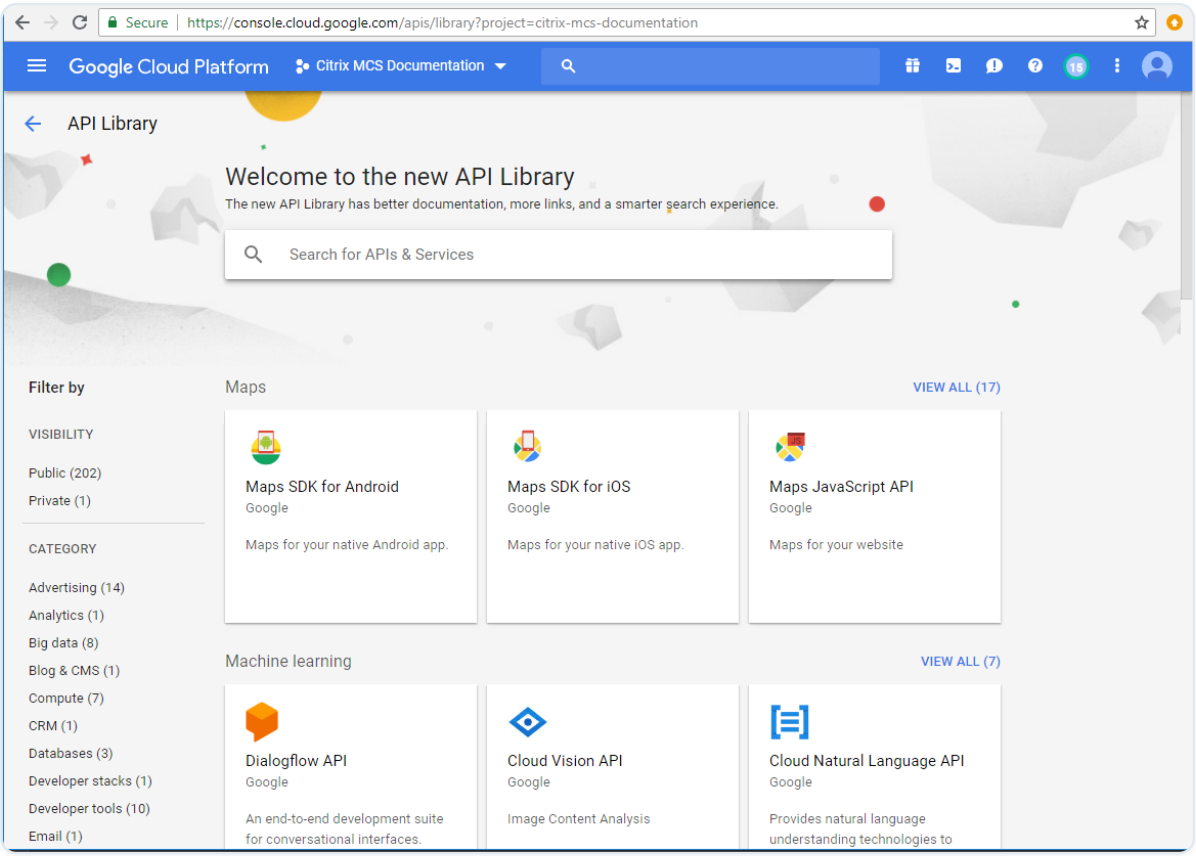
No console do Google Cloud, conclua estas etapas:

1. No menu superior esquerdo, selecione **APIs e Serviços > Painel**.



2. Na tela **Painel**, certifique-se de que a API do Compute Engine esteja habilitada. Se não estiver, siga estas etapas:

    a. navegar para **APIs and Services > Library**.



    b. Na caixa de pesquisa, digite *Compute Engine*.

    c. Nos resultados da pesquisa, selecione **Compute Engine API**.

    d. Na página **Compute Engine API**, selecione **Enable**.

3. Ative a API do Cloud Resource Manager.

    a. navegar para **APIs and Services > Library**.

    b. Na caixa de pesquisa, digite *Cloud Resource Manager*.

    c. Nos resultados da pesquisa, selecione **Cloud Resource Manager API**.

    d. Na página **Cloud Resource Manager API**, selecione **Enable**. O status da API é exibido.

4. Da mesma forma, habilite a **API Identity and Access Management (IAM)** e a **API Cloud Build**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para fazer isso:

1. Abra o Google Console e carregue o Cloud Shell.

2. Execute os quatro comandos a seguir no Cloud Shell:
    - gcloud services enable compute.googleapis.com.
    - gcloud serviços habilitar cloudresourcemanager.googleapis.com
    - gcloud serviços habilitar iam.googleapis.com
    - gcloud serviços habilitar cloudbuild.googleapis.com
3. Clique em **Autorizar** se o Cloud Shell solicitar.

Configurar e atualizar contas de serviço

> **Observação:**
>
> O GCP está introduzindo mudanças no comportamento padrão do Serviço Cloud Build e no uso de contas de serviço após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build habilitada antes de April 29, 2024 não são afetados por esta mudança. No entanto, se você quiser manter o comportamento existente do Serviço Cloud Build após April 29, você pode criar ou aplicar a política da organização para desabilitar a imposição da restrição antes de habilitar a API Cloud Build. Como resultado, o conteúdo a seguir é dividido em dois: Antes de April 29, 2024 e Depois de April 29, 2024. Se você definir a nova política da organização, siga a seção Antes de April 29, 2024.

Antes de April 29, 2024

O Citrix Cloud usa três contas de serviço separadas dentro do projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente, conforme descrito aqui. Para obter mais informações, consulte Criar uma Conta de Serviço do Citrix Cloud.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Conta de Serviço do Cloud Build*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e**

Administrador > IAM no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**.

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **cloudbuild**. Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

Verifique se a conta de serviço recebeu as seguintes funções. Se você precisar adicionar funções, siga as etapas descritas em Adicionar funções à conta de serviço do Cloud Build.

- Conta de Serviço do Cloud Build
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é adicionada pelo Google Cloud às instâncias criadas no Google Cloud assim que a API Compute é ativada. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar uma função de **Administrador de Armazenamento** que requer as seguintes permissões:
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`.

CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore
- Cloud KMS Crypto Operator

O Cloud KMS Crypto Operator requer as seguintes permissões:

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de

configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.

- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da Conta de Serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado 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, o Web Studio não poderá analisá-la.

Para criar uma chave de conta de serviço, navegar para **IAM e Administrador > Contas de serviço** e clique no endereço de e-mail da conta de serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

> **Dica:**
>
> Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CLOUD BUILD

Para adicionar funções à conta de serviço do Cloud Build:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a conta de serviço do Cloud Build, identificável por um endereço de e-mail que começa com o **ID do projeto** e a palavra **cloudbuild**.

   Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções.

Após April 29, 2024

O Citrix Cloud usa duas contas de serviço separadas dentro do projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Admin > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar a função de **Administrador de Armazenamento** que requer as seguintes permissões:
  - resourcemanager.projects.get

- storage.objects.create
- storage.objects.get
- storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com.`.

Verifique se a conta de serviço recebeu as seguintes funções.

- Conta de Serviço do Cloud Build
- Administrador de Instância de Computação
- Usuário da Conta de Serviço

CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

   Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

   - Administrador de Computação
   - Administrador de Armazenamento
   - Editor do Cloud Build
   - Usuário da Conta de Serviço
   - Usuário do Cloud Datastore
   - Cloud KMS Crypto Operator

   O Cloud KMS Crypto Operator requer as seguintes permissões:

   - cloudkms.cryptoKeys.get

- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.
- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da Conta de Serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado 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, o Web Studio não poderá analisá-la.

Para criar uma chave de conta de serviço, navegar para **IAM e Administrador > Contas de serviço** e clique no endereço de e-mail da conta de serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

> **Dica:**
>
> Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CLOUD COMPUTE

Para adicionar funções à Conta de Serviço do Cloud Compute:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a Conta de Serviço do Cloud Compute, identificável por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**.

   Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

> **Observação:**
>
> Habilite todas as APIs para obter a lista completa de funções.

Permissões de armazenamento e gerenciamento de bucket

O Citrix Virtual Apps and Desktops melhora o processo de relatório de falhas de compilação na nuvem para o serviço Google Cloud. Este serviço executa compilações no Google Cloud. O Citrix Virtual Apps and Desktops cria um bucket de armazenamento chamado `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` onde os serviços do Google Cloud capturam informações de log de compilação. Uma opção é definida neste bucket que exclui o conteúdo após um período de 30 dias. Este processo exige que a conta de serviço usada para a conexão tenha as permissões do Google Cloud definidas como `storage.buckets.update`. Se a conta de serviço não tiver essa permissão, o Citrix Virtual Apps and Desktops ignora os erros e prossegue com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de compilação aumenta e exige limpeza manual.

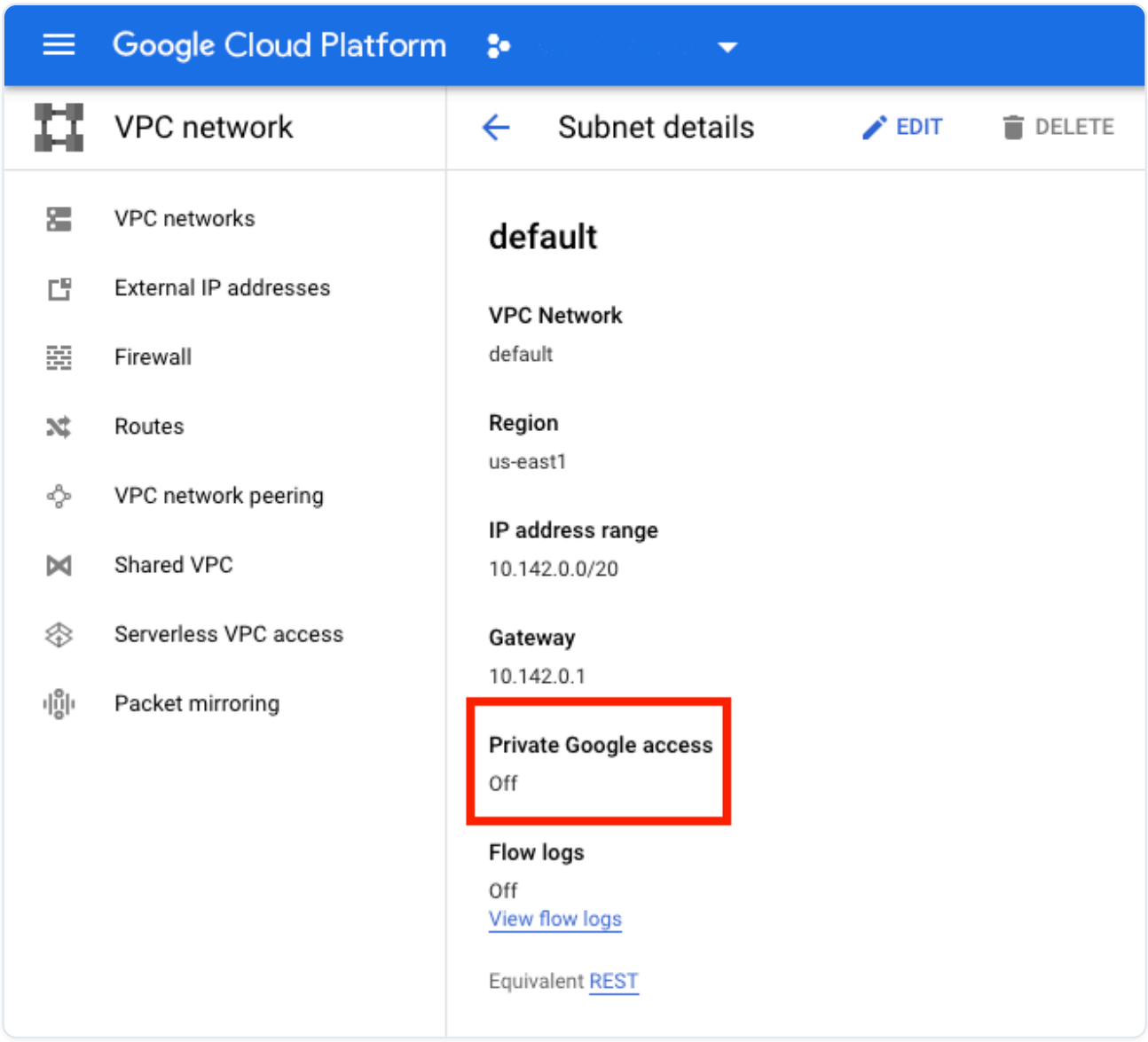
Habilitar acesso privado do Google

Quando uma VM não possui um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Ao habilitar o acesso privado, a VM se conecta ao conjunto de endereços IP externos usados pela API do Google e serviços associados.

> **Observação:**
>
> Independentemente de o acesso privado do Google estar habilitado, todas as VMs, com e sem endereços IP públicos, devem ser capazes de acessar as APIs Públicas do Google, especialmente se dispositivos de rede de terceiros tiverem sido instalados no ambiente.

> Para garantir que uma VM em sua sub-rede possa acessar as APIs do Google sem um endereço IP público para provisionamento MCS:

1. No Google Cloud, acesse a **configuração de rede VPC**.
2. Na tela de detalhes da Sub-rede, ative o **Acesso privado do Google**.



Para obter mais informações, consulte Configurando o Acesso Privado do Google.

> **Importante:**
>
> Se sua rede estiver configurada para impedir o acesso da VM à Internet, certifique-se de que sua organização assuma os riscos associados à habilitação do Acesso privado do Google para a sub-rede à qual a VM está conectada.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site

- Para criar e gerenciar uma conexão em ambientes Google Cloud, consulte Conexão com ambientes Google Cloud

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização HPE Moonshot

O Citrix Virtual Apps and Desktops™ gerencia suas cargas de trabalho HPE Moonshot por meio de um plug-in HPE Moonshot gerenciado pela Citrix. Com este plug-in, você pode criar conexões com seu chassi HPE Moonshot, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo.

Requisito

Instale o plug-in HPE Moonshot gerenciado pela Citrix no Delivery Controller.

> **Observação:**
>
> - Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, o Delivery Controller usará o plug-in HPE Moonshot gerenciado pela Citrix.
> - Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, e você quiser usar o plug-in Moonshot gerenciado pela HPE, desinstale o plug-in HPE Moonshot gerenciado pela Citrix e atualize o cache `RegisterPlugin`.

Instalar o plug-in HPE Moonshot gerenciado pela Citrix

Para instalar o plug-in HPE Moonshot gerenciado pela Citrix, faça o seguinte:

1. Instale `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi. `E:\` é a ISO.
2. Abra o PowerShell como Administrador e execute o seguinte comando.

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. Após o registro do plug-in ser bem-sucedido, reinicie os seguintes serviços no **Gerenciador de Tarefas**:
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. Execute `Get-HypHypervisorPlugins` para verificar se o plug-in está instalado no Delivery Controller. O campo **DisplayName** na saída deve ser exibido como **HPE Moonshot**.

Desinstalar o plug-in HPE Moonshot gerenciado pela Citrix e atualizar o cache RegisterPlugin

Se ambos os plug-ins HPE Moonshot gerenciados pela Citrix e gerenciados pela HPE estiverem instalados, e você quiser usar o plug-in Moonshot gerenciado pela HPE, você deve desinstalar o plug-in HPE Moonshot gerenciado pela Citrix e atualizar o cache `RegisterPlugin`. Para fazer isso:

1. Desinstale o plug-in HPE Moonshot gerenciado pelo Citrix.
2. Abra o PowerShell como Administrador e execute o seguinte comando:

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. Após o registro bem-sucedido do plug-in, reinicie os seguintes serviços a partir do **Gerenciador de Tarefas**:
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. Execute `Get-HypHypervisorPlugins` para verificar se o plug-in está instalado no Delivery Controller. O campo **DisplayName** na saída deve ser exibido como **HPE Moonshot Machine Manager**.

Etapas principais

1. Configure seus ambientes HPE.

2. Crie uma conexão com o chassi HPE Moonshot.
3. Criar um catálogo de máquinas.

> **Observação:**
>
> Antes de criar um catálogo, certifique-se de ter um ou mais nós de cartucho HPE Moonshot e instale VDAs nesses nós. Você pode considerar o chassi HPE Moonshot como o hipervisor e os nós de cartucho como VMs.

4. Crie um grupo de entrega.
5. Migre o restante dos nós HPE Moonshot não gerenciados para o catálogo gerenciado ou grupo de entrega.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão no HPE Moonshot, consulte Conexão com o HPE Moonshot

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de nuvem do Microsoft Azure Resource Manager

Ao usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™, familiarize-se com o seguinte:

- Azure Active Directory: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- Estrutura de consentimento: `<https://docs.microsoft.com/pt-br/azure/active-directory/manage-apps/plan-an-application-integration>`
- Entidade de serviço: `<https://docs.microsoft.com/pt-br/azure/active-directory/develop/app-objects-and-service-principals/>`

Para configurar seu Microsoft Azure Resource Manager, consulte Preparar para instalar.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes Azure, consulte Conexão com o Microsoft Azure

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas
- CTX219211: Configurar uma conta do Microsoft Azure Active Directory
- CTX219243: Conceder acesso do XenApp e XenDesktop à sua assinatura do Azure
- CTX219271: Implantar nuvem híbrida usando VPN site a site

Ambientes do Microsoft System Center Configuration Manager

Sites que usam o Microsoft System Center Configuration Manager (Configuration Manager) para gerenciar o acesso a aplicativos e desktops podem estender esse uso para o Citrix Virtual Apps and Desktops™ usando estas opções:

- Instalar VDAs usando SCCM.
- **Recurso Wake Proxy do Configuration Manager:** O recurso Wake on LAN do Acesso para PC Remoto é compatível com o Configuration Manager. Para obter detalhes, consulte Wake on LAN - SCCM integrado.
- **Propriedades do Citrix Virtual Apps and Desktops:** Propriedades permitem identificar o Citrix Virtual Desktops™ para gerenciamento através do Configuration Manager. (Em algumas versões, o Configuration Manager usa o nome anterior do Citrix Virtual Apps and Desktops: XenApp e XenDesktop.)

Propriedades

As propriedades estão disponíveis para o Microsoft System Center Configuration Manager para gerenciar desktops virtuais.

As propriedades booleanas exibidas no Configuration Manager aparecem como `1` ou `0`, não como verdadeiro ou falso.

As propriedades estão disponíveis para a classe `Citrix_virtualDesktopInfo` no namespace `Root\Citrix\DesktopInformation`. Os nomes das propriedades vêm do provedor Windows Management Instrumentation (WMI).

PROPRIEDADE	DESCRIÇÃO
`AssignmentType`	Define o valor de IsAssigned. Os valores válidos são: `ClientIP`, `ClientName`, `None` e `User` (define `IsAssigned` como `True`)
`BrokerSiteName`	Retorna o mesmo valor que `HostIdentifier`
`DesktopCatalogName`	Catálogo de máquinas associado ao desktop.
`DesktopGroupName`	Grupo de entrega associado ao desktop.
`HostIdentifier`	Retorna o mesmo valor que `BrokerSiteName`.
`IsAssigned`	`True` para atribuir a área de trabalho a um usuário, defina como `False` para uma área de trabalho aleatória
`IsMasterImage`	Permite decisões sobre o ambiente. Por exemplo, instalar aplicativos na imagem e não nas máquinas provisionadas. Os valores válidos são: `True` em uma VM que é usada como imagem. Este valor é definido durante a instalação com base em uma seleção, ou limpo em uma VM que é provisionada a partir dessa imagem.
`IsVirtualMachine`	`True` para uma máquina virtual, `false` para uma máquina física.
`OSChangesPersist`	`False` se a imagem do sistema operacional da área de trabalho for redefinida para um estado limpo toda vez que for reiniciada; caso contrário, `true`.

PROPRIEDADE	DESCRIÇÃO
`PersistentDataLocation`	O local onde o Configuration Manager armazena dados persistentes. Isso não é acessível aos usuários.
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	Determinados quando a área de trabalho se registra no Controller. Eles são nulos para uma área de trabalho que não foi totalmente registrada.

Para coletar as propriedades, execute um inventário de hardware no Configuration Manager. Para visualizar as propriedades, use o Gerenciador de Recursos do Configuration Manager. Nestes casos, os nomes incluem espaços ou variam ligeiramente dos nomes das propriedades. Por exemplo, `BrokerSiteName` aparece como `Broker Site Name`.

- Configure o Configuration Manager para coletar propriedades WMI do Citrix do Citrix VDA
- Crie coleções de dispositivos baseadas em consulta usando propriedades WMI do Citrix
- Crie condições globais com base em propriedades WMI do Citrix
- Use condições globais para definir requisitos de tipo de implantação de aplicativo

Você também pode usar propriedades da Microsoft na classe Microsoft `CCM_DesktopMachine` no namespace `Root\ccm_vdi`. Para obter mais informações, consulte a documentação da Microsoft.

Ambientes de virtualização Microsoft System Center Virtual Machine Manager

Siga esta orientação se você usar o Hyper-V com o Microsoft System Center Virtual Machine Manager (VMM) para fornecer máquinas virtuais.

Esta versão oferece suporte às versões do VMM listadas em Requisitos do sistema.

> **Observação:**
>
> Clusters Hyper-V mistos (contendo servidores executando diferentes versões do Hyper-V) não são suportados.

> Você pode usar o Citrix Provisioning (anteriormente Provisioning Services) e o Machine Creation Services™ para provisionar:

- VMs de SO de Desktop ou Servidor compatíveis com Geração 1.
- VMs de SO de Desktop ou Servidor compatíveis com Geração 2, incluindo suporte a Secure Boot.

Instalar e configurar um hipervisor

> **Importante:**
>
> Todos os Delivery Controllers devem estar na mesma floresta que os servidores VMM.

1. Instale o servidor Microsoft Hyper-V e o VMM em seus servidores.
2. Instale o console do System Center Virtual Machine Manager em todos os Controllers. A versão do console deve corresponder à versão do servidor de gerenciamento. Embora um console anterior possa se conectar ao servidor de gerenciamento, o provisionamento de VDAs falha se as versões forem diferentes.
3. Verifique as seguintes informações da conta:

   A conta que você usa para especificar hosts no Studio é um administrador VMM ou um administrador delegado VMM para as máquinas Hyper-V relevantes. Se esta conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados no Studio durante o processo de criação do host.

   A conta de usuário usada para a integração do Studio também deve ser membro do grupo de segurança local de administradores em cada servidor Hyper-V. Essa configuração oferece suporte ao gerenciamento do ciclo de vida da VM, como criação, atualização e exclusão de VMs.

   A instalação de um Controller em um servidor executando o Hyper-V não é suportada.

Em grandes implantações onde um único SCVMM gerencia vários clusters em diferentes data centers, você pode limitar o escopo dos grupos de host de administradores delegados.

Para limitar o escopo dos grupos de host, use a função de Administrador Delegado no console do Microsoft System Center Virtual Machine Manager (VMM):

1. No **Assistente para Criar Funções de Usuário**, selecione Administrador de Malha (Administrador Delegado) como uma função de usuário.
2. Em **Membros**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Escopo**, selecione os grupos de host aos quais você deseja que o administrador delegado tenha acesso.
4. Crie uma nova **Conta Executar como** usando as credenciais de usuário do administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão no SCVMM, consulte Conexão com o Microsoft System Center Virtual Machine Manager

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização Nutanix

Siga esta orientação ao usar o Nutanix Acropolis para fornecer máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops™. O processo de configuração inclui as seguintes tarefas:

- Instale e registre o plug-in do Nutanix em seu ambiente Citrix Virtual Apps and Desktops.
- Crie uma conexão com o hipervisor Nutanix Acropolis.
- Crie um catálogo de máquinas que usa um instantâneo de uma imagem mestre que você criou no hipervisor Nutanix.

Para obter mais informações, consulte o Guia de Instalação do plug-in MCS do Nutanix Acropolis, disponível no Portal de Suporte da Nutanix.

Instalar e registrar o plug-in Nutanix

Conclua o procedimento a seguir para instalar e registrar o plug-in do Nutanix em todos os seus Delivery Controllers. Use o Citrix Studio para criar uma conexão com o Nutanix. Em seguida, crie um catálogo de máquinas que usa um instantâneo de uma 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™ ao instalar ou atualizar o plug-in do Nutanix.
>
> Para obter informações sobre como instalar o plug-in do Nutanix, consulte o site de Documentação da Nutanix.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes Nutanix, consulte Conexão com Nutanix

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Soluções de nuvem e parceiros Nutanix

O Citrix Virtual Apps and Desktops™ oferece suporte à seguinte solução de nuvem e parceira da Nutanix:

- Clusters de Nuvem Nutanix no AWS

Clusters de Nuvem Nutanix no AWS

O Citrix Virtual Apps and Desktops oferece suporte aos Clusters de Nuvem Nutanix no AWS. Os clusters Nutanix simplificam a forma como os aplicativos são executados em nuvens privadas ou

em múltiplas nuvens públicas. Para obter mais informações sobre Clusters de Nuvem Nutanix no AWS, consulte Guia de Implantação e Usuário de Clusters de Nuvem Nutanix no AWS.

> **Dica:**
>
> Este suporte oferece a mesma funcionalidade de um cluster Nutanix local. Apenas um único cluster é suportado, o *Prism Element*. Para obter mais informações, consulte aqui.

Requisitos

Você precisa do seguinte para usar os Clusters Nutanix no AWS:

- Uma conta Nutanix.
- Uma conta 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 **Nutanix cluster** e clique em **Launch**. O **Nutanix Console** é aberto. Para obter mais informações, consulte Introdução ao Cluster Nutanix no AWS.
3. Escolha criar uma **new VPC**.

O processo de criação do cluster pode falhar com os seguintes erros:

- O cluster falhou ao ser criado dentro do tempo especificado. Excluindo cluster.
- Cluster Nutanix do Host - Nó `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- Cluster Nutanix do Host - Nó `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

Se o cluster falhou ao ser criado:

- Tente recriar um em uma região diferente.

- Certifique-se de excluir o Nutanix CloudFormation Stack (CFS) antes de tentar novamente.

Além de outros recursos, o Nutanix CFS cria:

- 1 VPC nomeada *Nutanix Cluster xxxxxxxxxxxx* 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

Assim 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.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão de soluções de nuvem e parceiros Nutanix, consulte Conexão com soluções de nuvem e parceiros Nutanix

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização VMware

Siga esta orientação se você usa VMware para fornecer máquinas virtuais.

Instale o vCenter Server e as ferramentas de gerenciamento apropriadas. (Nenhum suporte é fornecido para a operação do vSphere vCenter Linked Mode.)

Se você planeja usar o MCS, não desative o recurso Datastore Browser no vCenter Server (descrito em `<https://kb.vmware.com/s/article/2101567>`). Ao desativar esse recurso, o MCS não funciona corretamente.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão em ambientes VMware, consulte Conexão com VMware

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Soluções de nuvem e parceiros VMware

O Citrix Virtual Apps and Desktops™ oferece suporte às seguintes soluções de nuvem e parceiros VMware:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Integração do Azure VMware Solution (AVS)

O serviço Citrix Virtual Apps and Desktop oferece suporte a AVS. O AVS fornece infraestrutura de nuvem contendo clusters vSphere criados pela infraestrutura do Azure. Aproveite o serviço Citrix Virtual Apps and Desktop para usar o AVS para provisionar sua carga de trabalho VDA da mesma forma que você usaria o vSphere em ambientes locais.

Configurar o cluster AVS

Para permitir que o serviço Citrix Virtual Apps™ and Desktop use o AVS, execute as seguintes etapas no Azure:

- Solicitar uma cota de host
- Registrar o provedor de recursos Microsoft.AVS
- Lista de Verificação de Rede
- Criar uma nuvem privada do Azure VMware Solution
- Acessar uma nuvem privada do Azure VMware Solution
- Configurar a rede para sua nuvem privada VMware no Azure

- Configurar DHCP para Azure VMware Solution
- Adicionar um segmento de rede no Azure VMware Solution
- Verificar o ambiente do Azure VMware Solution

SOLICITAR COTA DE HOST PARA CLIENTES DO CONTRATO ENTERPRISE DO AZURE

Na página **Ajuda + Suporte** do portal do Azure, selecione **Nova solicitação de suporte** e inclua as seguintes informações:

- Tipo de problema: Técnico
- Assinatura: Selecione sua assinatura
- Serviço: Todos os serviços > Azure VMware Solution
- Recurso: Pergunta geral
- Resumo: Necessidade de capacidade
- Tipo de problema: Problemas de gerenciamento de capacidade
- Subtipo de problema: Solicitação do cliente para cota/capacidade de host adicional

Na **Descrição** do tíquete de suporte, inclua as seguintes informações na guia **Detalhes**:

- POC ou Produção
- Nome da Região
- Número de hosts
- Quaisquer outros detalhes

> **Nota:**

> O AVS requer um mínimo de três hosts e recomenda que você use redundância de hosts N+1.

> Após especificar os detalhes para o tíquete de suporte, selecione **Revisar + Criar** para enviar a solicitação ao Azure.

REGISTRAR O PROVEDOR DE RECURSOS MICROSOFT.AVS

Após solicitar a cota de host, registre o provedor de recursos:

1. Faça login no portal do Azure.
2. No menu do portal do Azure, selecione **Todos os serviços**.

3. No menu **Todos os serviços**, insira a assinatura e selecione **Assinaturas**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Provedores de recursos** e insira **Microsoft.AVS** na barra de pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

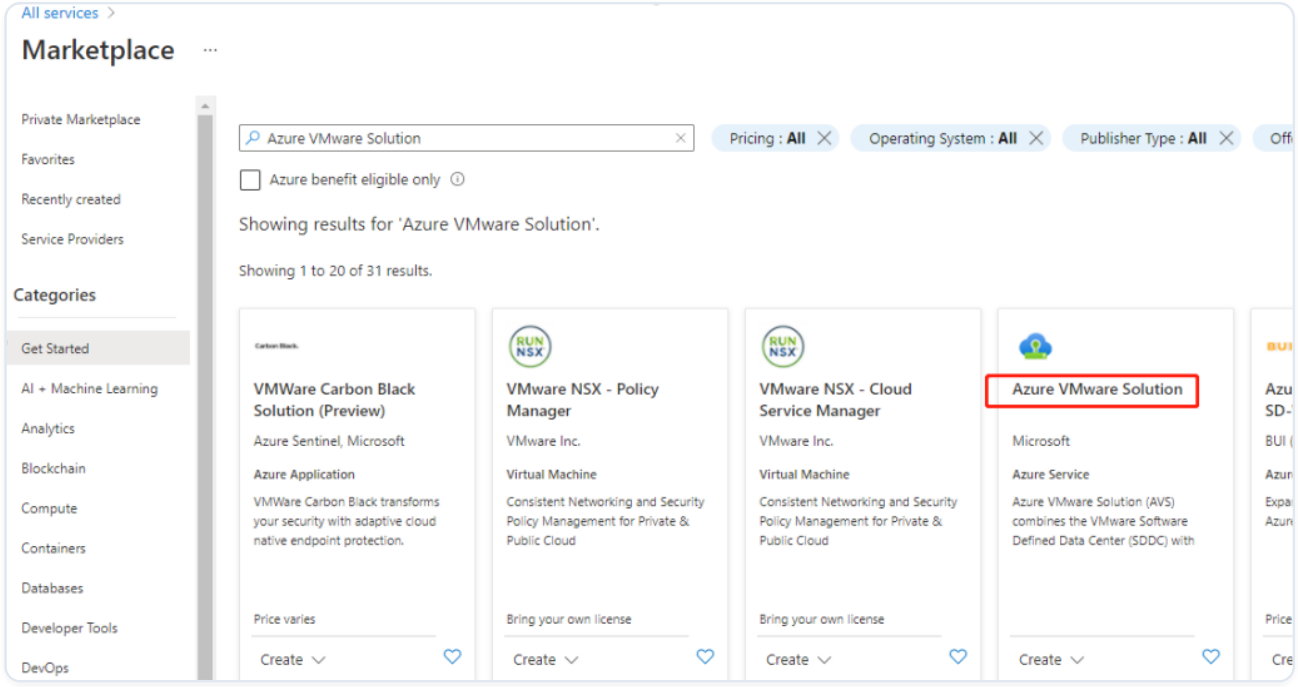
CONSIDERAÇÕES DE REDE

O AVS oferece serviços de rede que exigem intervalos de endereços de rede específicos e portas de firewall. Consulte Lista de verificação de planejamento de rede para a Solução VMware do Azure para obter mais informações.

CRIAR UMA NUVEM PRIVADA DO AZURE VMWARE SOLUTION

Após considerar os requisitos de rede para seu ambiente, crie uma nuvem privada ASV:

1. Faça login no portal do Azure.
2. Selecione **Criar um novo recurso**.
3. Na caixa de texto **Pesquisar no Marketplace**, digite *Azure VMware Solution* e selecione **Azure VMware Solution** na lista.



imagem

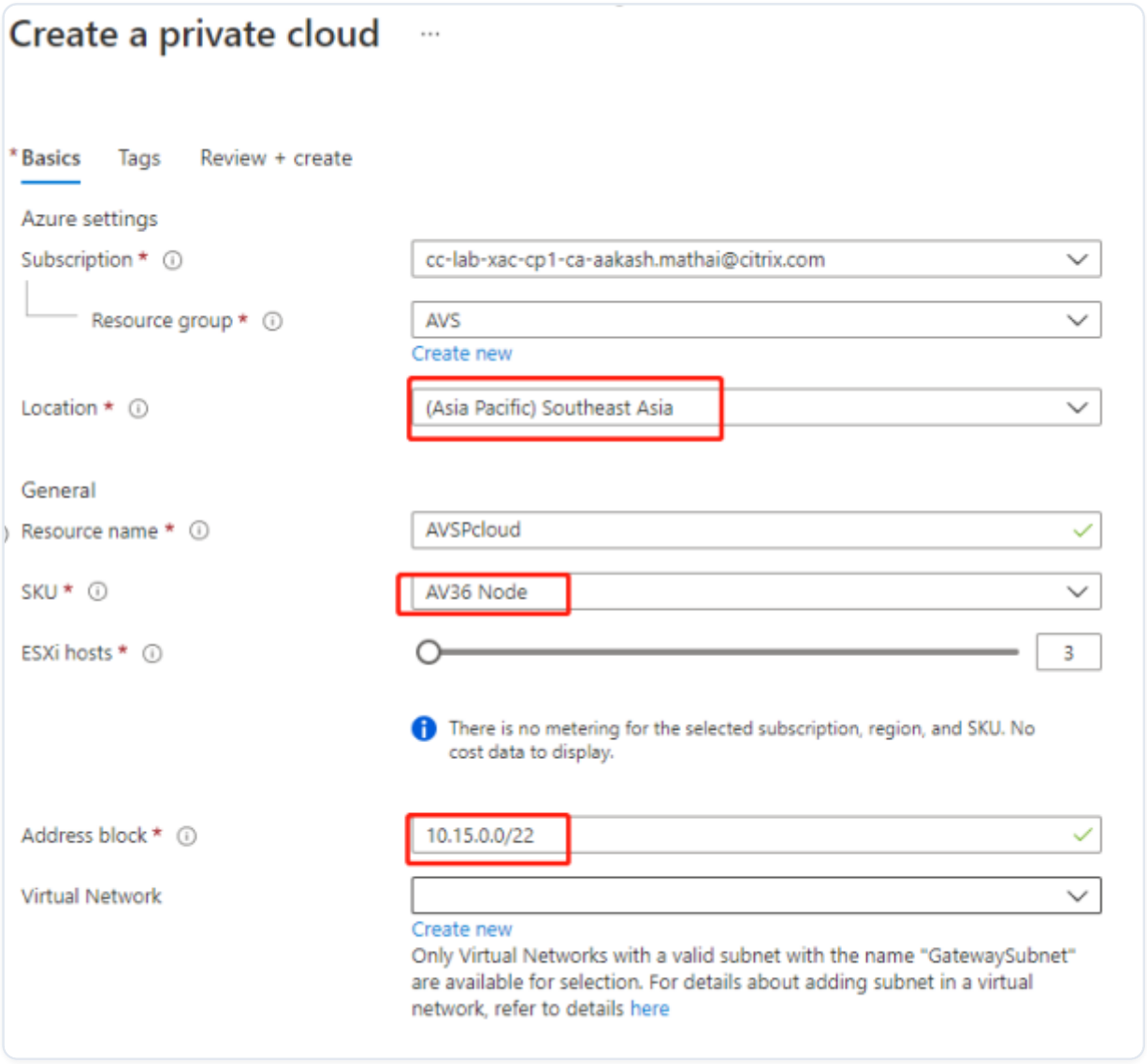
Na janela **Azure VMware Solution**:

1. Selecione **Criar**.
2. Clique na guia **Básico**.
3. Insira os valores para os campos, usando as informações na tabela abaixo:

CAMPO	VALOR
Assinatura	Selecione a assinatura que você planeja usar para a implantação. Todos os recursos em uma assinatura do Azure são cobrados juntos.
Grupo de recursos	Selecione o grupo de recursos para sua nuvem privada. Um grupo de recursos do Azure é um contêiner lógico no qual os recursos do Azure são implantados e gerenciados. Alternativamente, você pode criar um novo grupo de recursos para sua nuvem privada.
Localização	Selecione um local, como leste dos EUA. Esta é a região que você definiu durante a fase de planejamento.
Nome do recurso	Forneça o nome da sua nuvem privada do Azure VMware Solution.
SKU	Selecione AV36.
Hosts	Mostra o número de hosts alocados para o cluster da nuvem privada. O valor padrão é 3, que pode ser aumentado ou diminuído após a implantação.
Bloco de endereços	Forneça um bloco de endereços IP para a nuvem privada. O CIDR representa a rede de gerenciamento da nuvem privada e será usado para os serviços de gerenciamento de cluster, como vCenter Server e NSX-T Manager. Use o espaço de endereço /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure, bem como a redes locais.
Rede Virtual	Deixe este campo em branco porque o circuito ExpressRoute do Azure VMware Solution é estabelecido como uma etapa pós-implantação.

Na tela **Criar uma nuvem privada**:

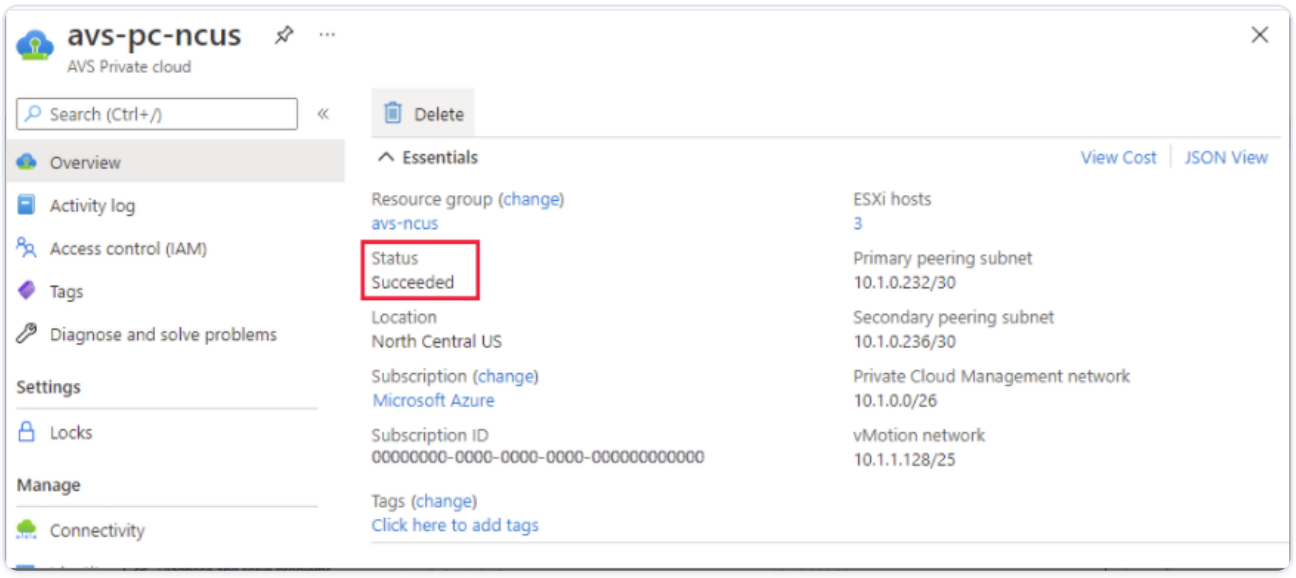
1. No campo **Localização**, selecione a região que possui o AVS; a região do grupo de recursos é a mesma da região do AVS.
2. No campo **SKU**, selecione **Nó AV36**.
3. Especifique um endereço IP no campo **Bloco de Endereços**. Por exemplo, 10.15.0.0/22.
4. Selecione **Revisar + Criar**.
5. Após revisar as informações, clique em **Criar**.



Dica:

A criação de uma nuvem privada pode levar de 3 a 4 horas. Adicionar um único host ao cluster pode levar de 30 a 45 minutos.

> Verifique se a implantação foi bem-sucedida. navegar para o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Bem-sucedido**, a implantação estará concluída.



ACESSAR UMA NUVEM PRIVADA DO AZURE VMWARE SOLUTION

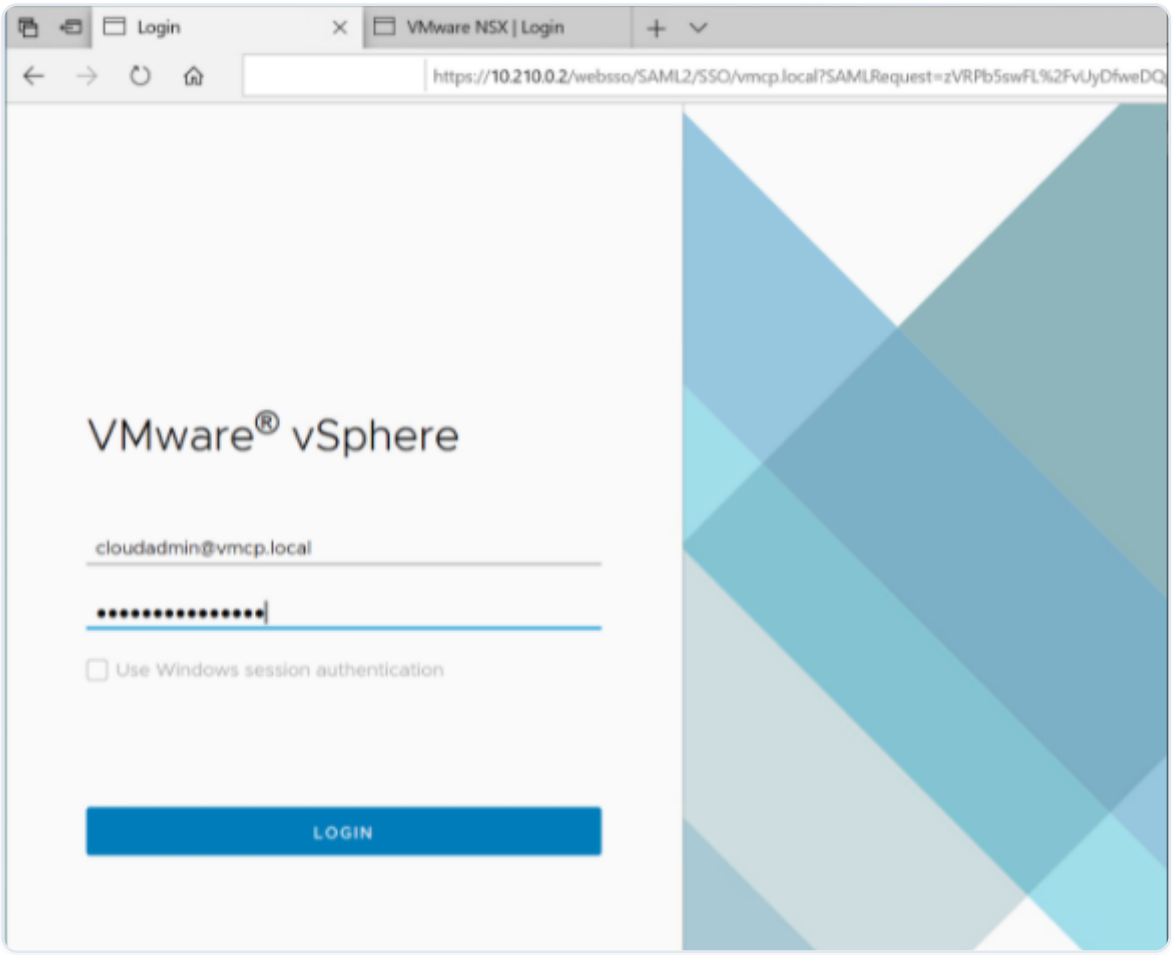
Depois de criar uma nuvem privada, crie uma VM Windows e conecte-se ao vCenter local da sua nuvem privada.

Criar uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar** e, em seguida, pesquise e selecione **Microsoft Windows 10/2016/2019**.
2. Clique em **Criar**.
3. Insira as informações necessárias e selecione **Revisar + Criar**.
4. Assim que a validação for aprovada, selecione **Criar** para iniciar o processo de criação da máquina virtual.

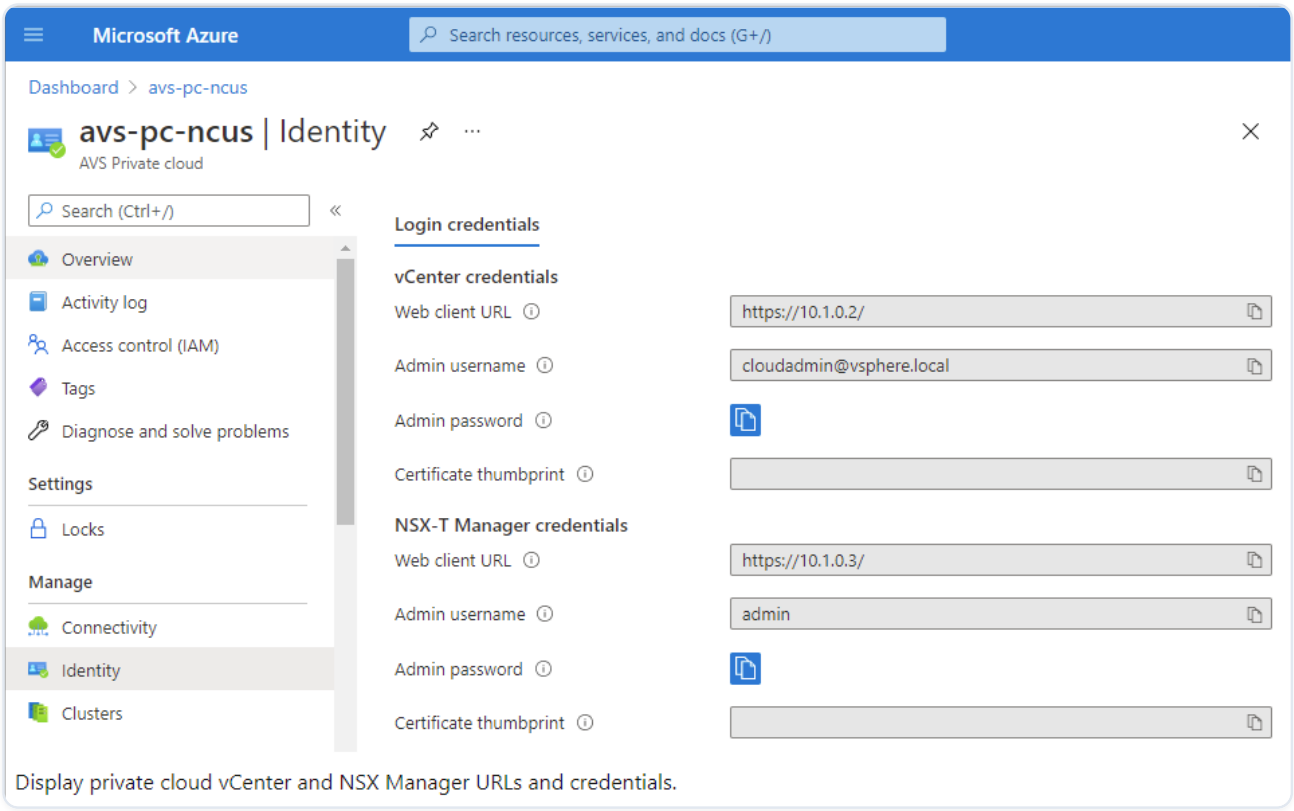
Conectar-se ao vCenter local da sua nuvem privada

1. Faça login no **vSphere Client com VMware vCenter SSO** como administrador de nuvem.



2. No portal do Azure, selecione sua nuvem privada e, em seguida, **Gerenciar > Identidade**.

As URLs e as credenciais de usuário para o vCenter da nuvem privada e o NSX-T Manager aparecem:



Após confirmar as URLs e as credenciais de usuário:

1. navegar para a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegar para as URLs do vCenter e do NSX-T Manager em duas guias do navegador. Na guia do vCenter, insira as credenciais de usuário *cloudadmin@vmcp.local* da etapa anterior.

CONFIGURAR A REDE PARA SUA NUVEM PRIVADA VMWARE NO AZURE

Após acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.
Criar uma rede virtual

1. Faça login no portal do Azure.
2. navegar para o grupo de recursos criado anteriormente.
3. Selecione **+ Adicionar** para definir um novo recurso.
4. Na caixa de texto **Pesquisar no Marketplace**, digite *rede virtual*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Rede Virtual**, selecione **Criar** para configurar a rede virtual para sua nuvem privada.
6. Na página **Criar Rede Virtual**, insira os detalhes da sua rede virtual.
7. Na guia **Básico**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Avançar: Endereços IP.**

8. Na guia **Endereços IP**, em espaço de endereço IPv4, insira o endereço criado anteriormente.

> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço que você usou ao criar sua nuvem privada.

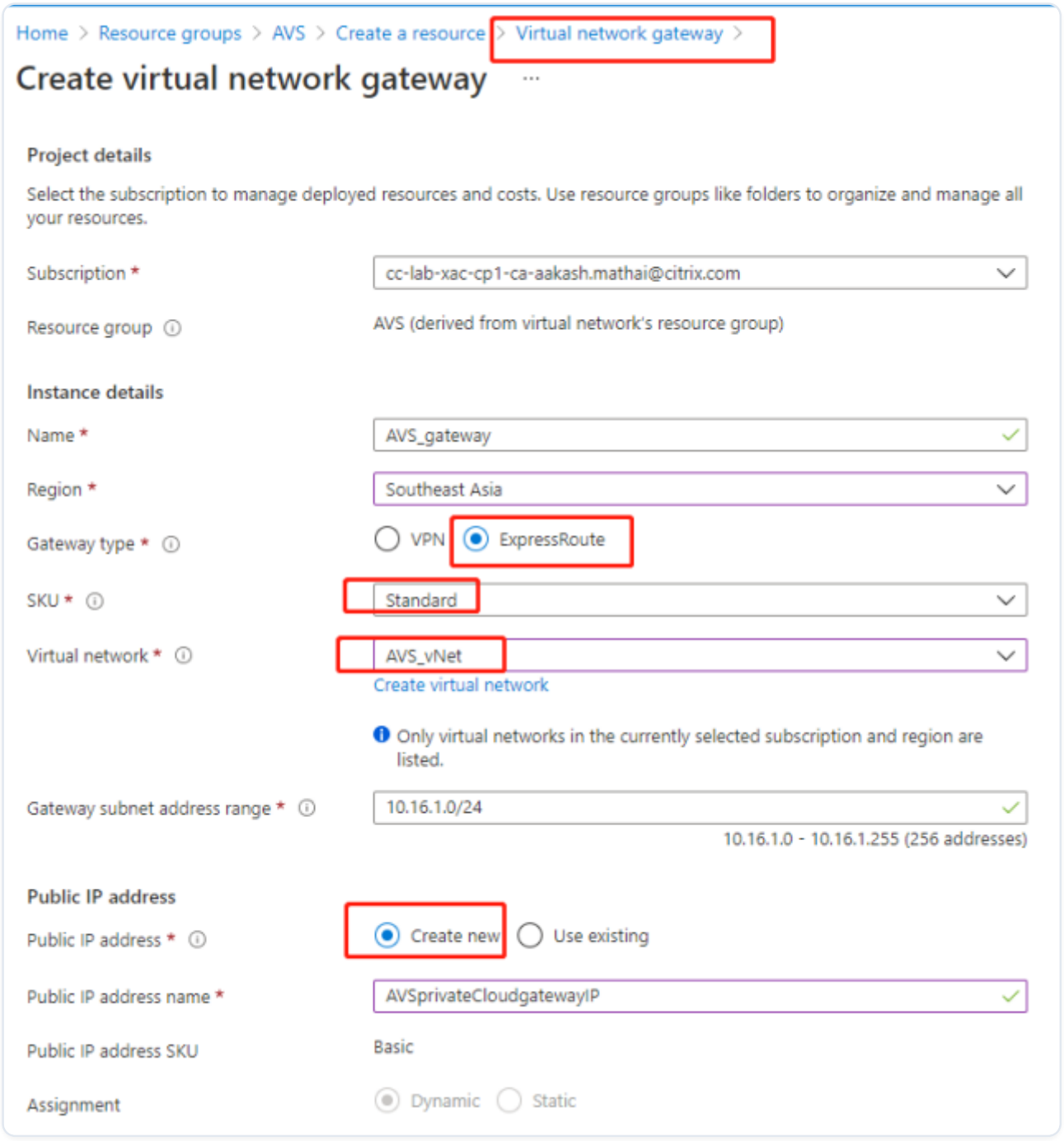
> Após inserir o espaço de endereço:

1. Selecione **+ Adicionar sub-rede**.
2. Na página **Adicionar sub-rede**, dê um nome à sub-rede e um intervalo de endereços apropriado.
3. Clique em **Adicionar.**
4. Selecione **Revisar + criar**.
5. Verifique as informações e clique em **Criar**. Assim que a implantação for concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual

Após criar uma rede virtual, crie um gateway de rede virtual.

1. No seu grupo de recursos, selecione **+ Adicionar** para adicionar um novo recurso.
2. Na caixa de texto **Pesquisar no Marketplace**, digite *gateway de rede virtual*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Gateway de Rede Virtual**, clique em **Criar**.
4. Na guia **Básico** da página **Criar gateway de rede virtual**, forneça valores para os campos.
5. Clique em **Revisar + criar**.



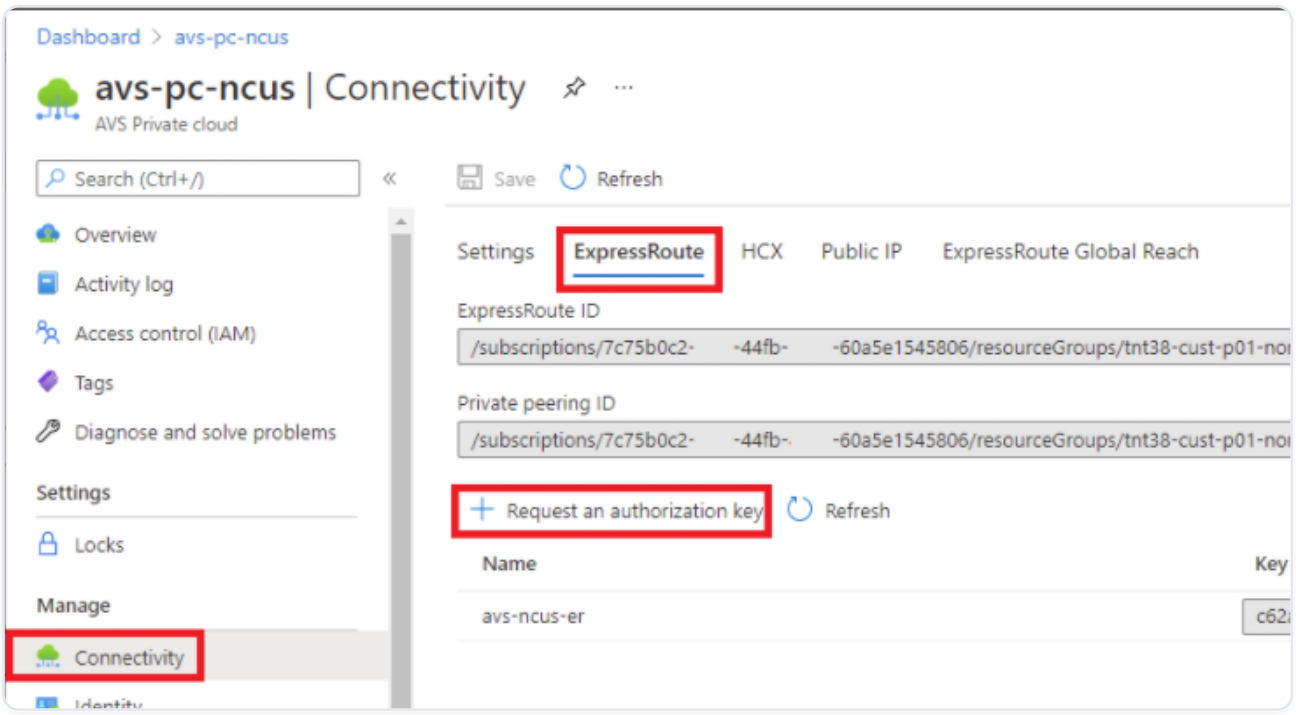
Após revisar a configuração do gateway de rede virtual, clique em **Criar** para implantar seu gateway de rede virtual. Assim que a implantação for concluída, conecte sua conexão **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada Azure AVS.

CONECTAR O EXPRESSROUTE AO GATEWAY DE REDE VIRTUAL

Após implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada Azure AVS:

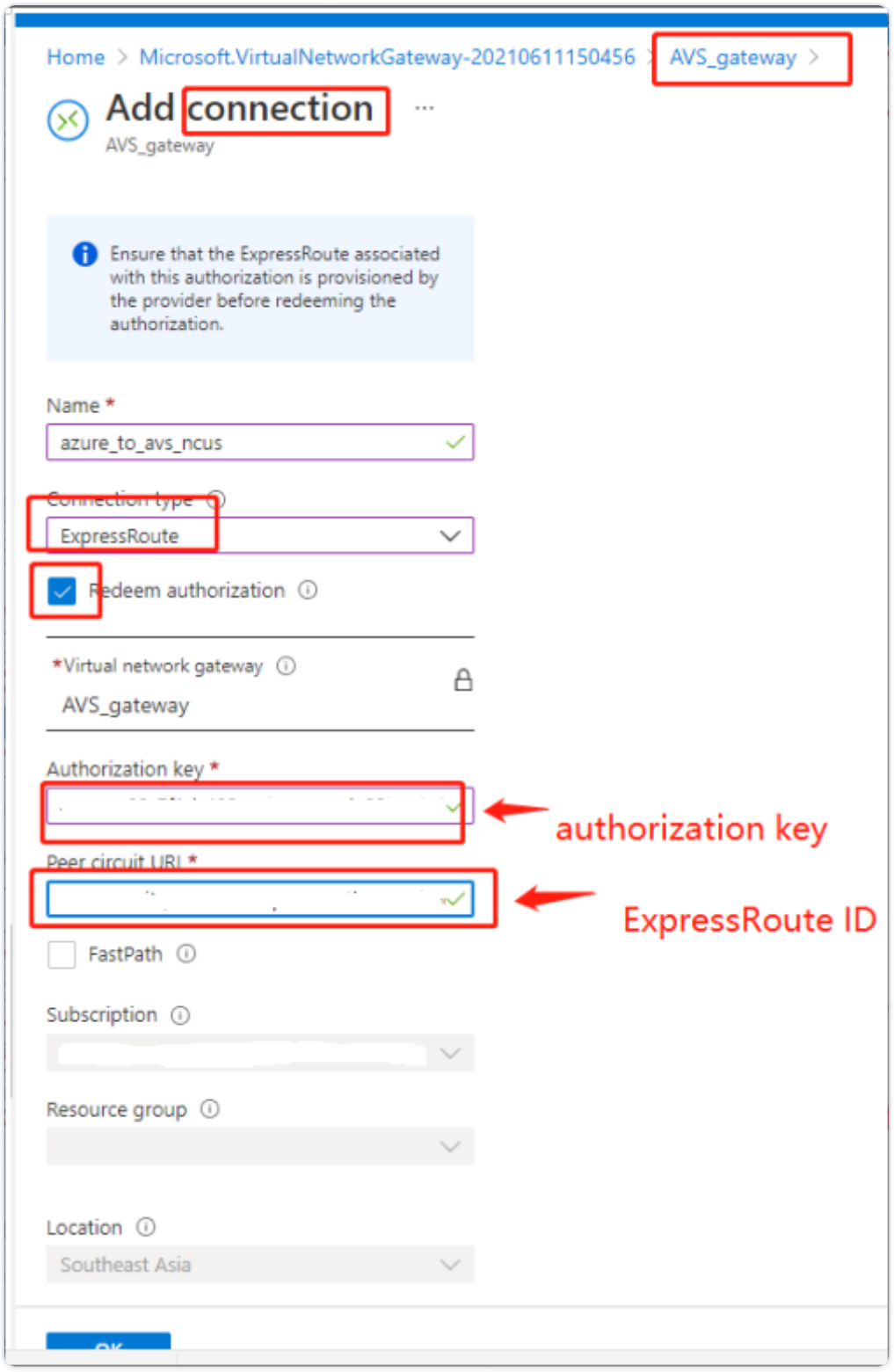
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegar até a **nuvem privada da Solução VMware do Azure**. Selecione **Gerenciar > Conectividade > ExpressRoute** e, em seguida, selecione **+ Solicitar uma chave de autorização.**

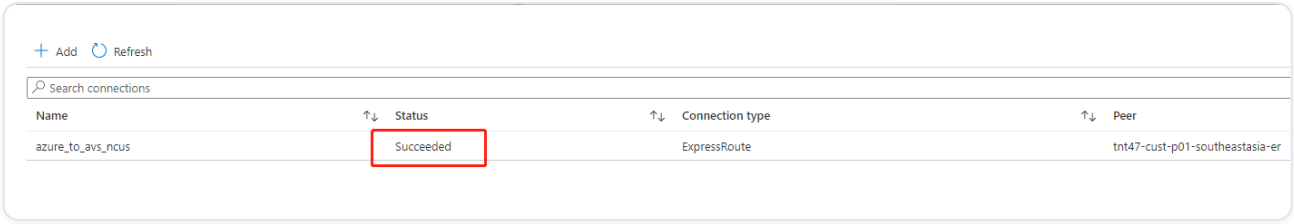


Após solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Criar**. Pode levar cerca de 30 segundos para criar a chave. Uma vez criada, a nova chave aparece na lista de chaves de autorização para a nuvem privada.
2. Copie a **chave de autorização** e o **ID do ExpressRoute**. Você precisará deles para concluir o processo de emparelhamento. A chave de autorização desaparece após algum tempo, então copie-a assim que ela aparecer.
3. navegar até o **gateway de rede virtual** que você planeja usar e selecione **Conexões > + Adicionar**.
4. Na página **Adicionar conexão**, forneça valores para os campos e selecione **OK.**



A conexão é estabelecida entre seu circuito ExpressRoute e sua rede virtual:



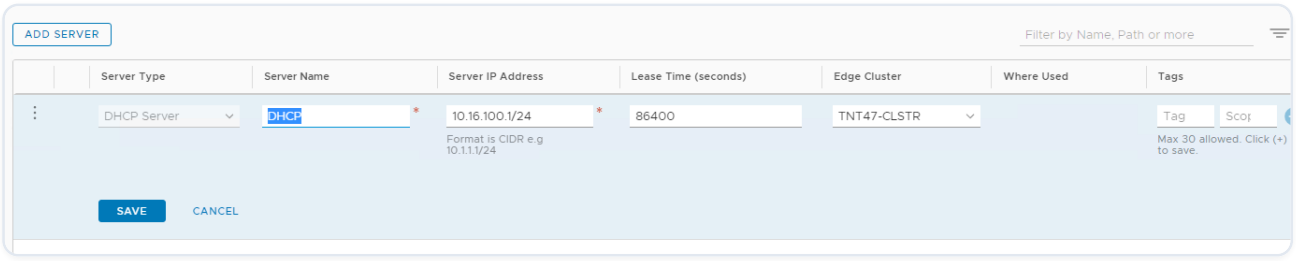
CONFIGURAR DHCP PARA AZURE VMWARE SOLUTION

Após conectar o ExpressRoute ao gateway virtual, configure o DHCP.

Use o NSX-T para hospedar seu servidor DHCP

No NSX-T Manager:

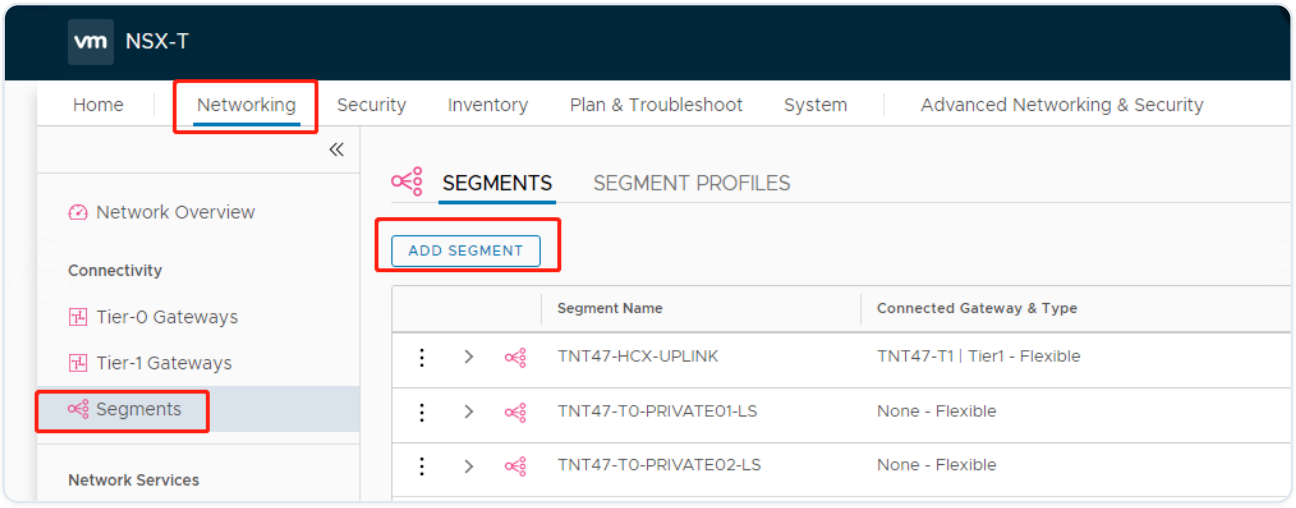
1. Selecione **Rede > DHCP** e então selecione **Adicionar Servidor**.
2. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Gateways de Camada 1**, selecione as reticências verticais no gateway de Camada 1 e então selecione **Editar**.
5. Selecione **Nenhum Conjunto de Alocação de IP** para adicionar uma sub-rede.
6. Selecione **Servidor DHCP Local** para o **Tipo**.
7. Para o **Servidor DHCP**, selecione **DHCP Padrão** e então clique em **Salvar**.
8. Clique em **Salvar** novamente e, em seguida, selecione **Fechar Edição**.



ADICIONAR UM SEGMENTO DE REDE NO AZURE VMWARE SOLUTION

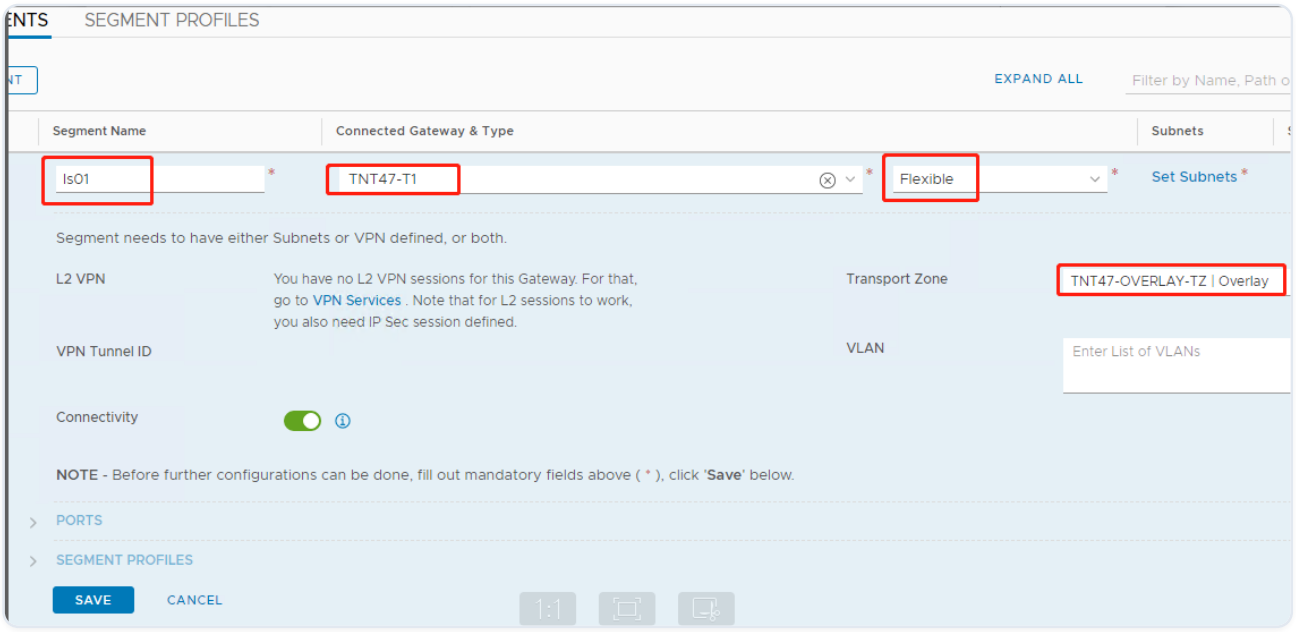
Após configurar o DHCP, adicione um segmento de rede.

Para adicionar um segmento de rede, no NSX-T Manager, selecione **Rede > Segmentos** e, em seguida, clique em **Adicionar Segmento**.



Na tela **Perfil de segmentos**:

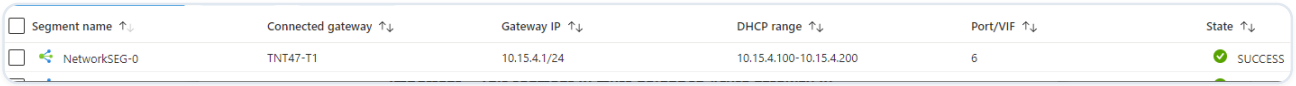
1. Insira um **nome** para o segmento.
2. Selecione o **Gateway Tier-1 (TNTxx-T1)** como o **Gateway Conectado** e deixe o **Tipo** como **Flexível**.
3. Selecione a **Zona de Transporte (TNTxx-OVERLAY-TZ)** de sobreposição pré-configurada.
4. Clique em **Definir Sub-redes**.



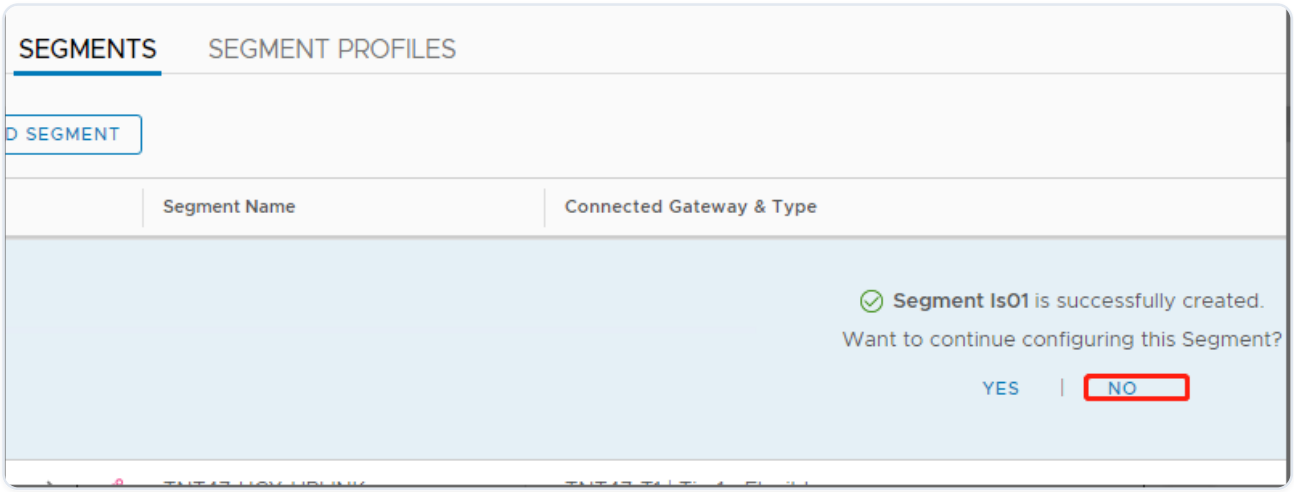
Na seção **Sub-redes**:

1. Insira o endereço IP do gateway.
2. Selecione **Adicionar**.

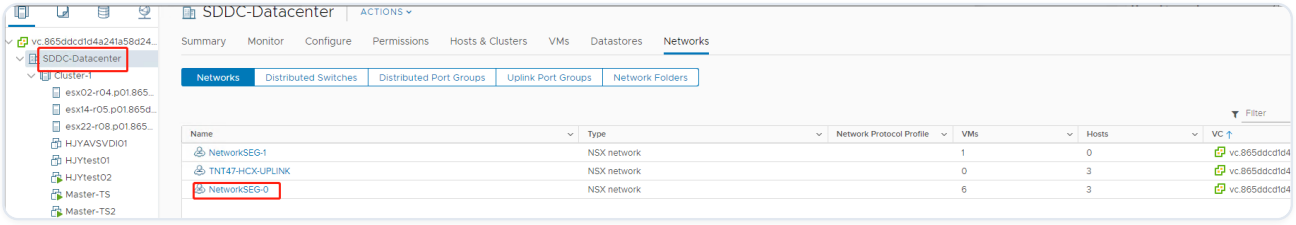
> **Importante:**
>
> Este endereço IP de segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.
>
> O intervalo DHCP deve pertencer ao endereço IP do segmento:



Selecione **Não** para recusar a opção de continuar configurando o segmento:

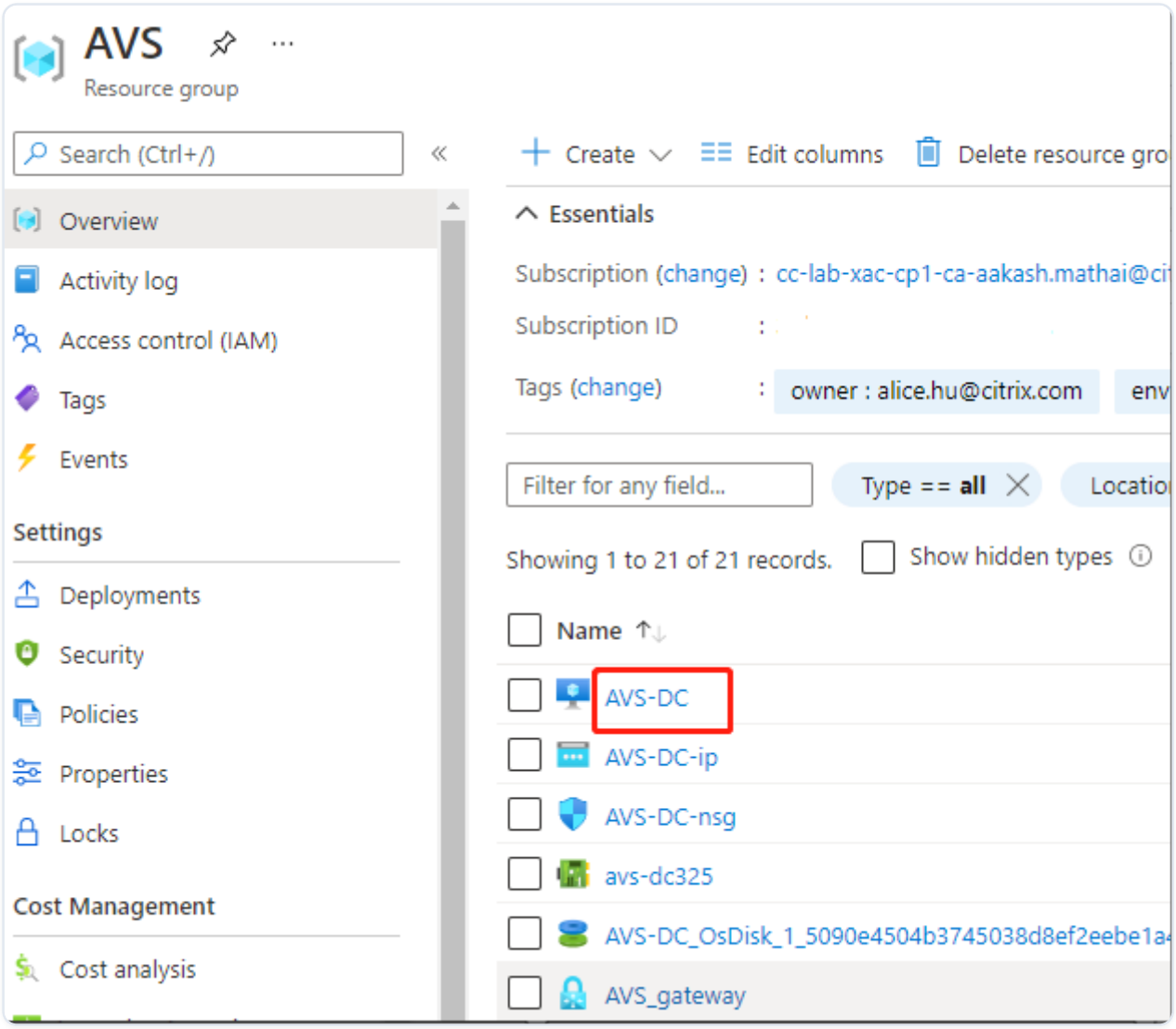


No vCenter, selecione **Networking > SDDC-Datacenter**:

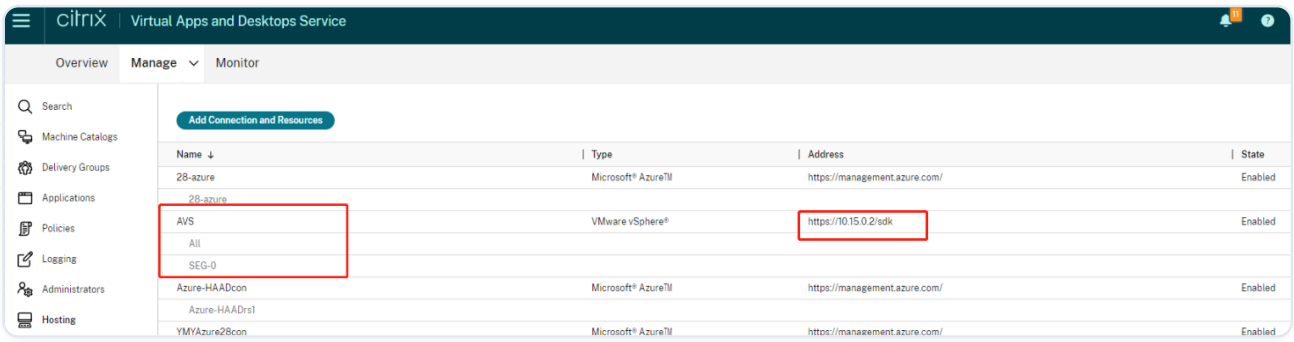


VERIFICAR O AMBIENTE AZURE AVS

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 Virtual Apps and Desktops permite migrar cargas de trabalho Citrix locais baseadas em VMware para o Google Cloud VMware Engine.

Configurar o Google Cloud VMware Engine

O procedimento a seguir descreve como adquirir e configurar um cluster no Google Cloud VMware Engine.

ACESSAR O PORTAL DO VMWARE ENGINE

1. No **Google Cloud Console**, clique no menu de navegação.
2. Na seção **Compute**, clique em **VMware Engine** para abrir o VMware Engine em uma nova guia do navegador.

REQUISITOS PARA CRIAR A PRIMEIRA NUVEM PRIVADA

Você deve ter acesso ao Google Cloud VMware Engine, cota de nó do VMware Engine disponível e uma função IAM apropriada. Prepare os seguintes requisitos antes de continuar a criar sua nuvem privada:

1. Solicite acesso à API e cota de nó. Para obter mais informações, consulte Solicitando acesso à API e cota.
2. Anote os intervalos de endereço que você deseja usar para os dispositivos de gerenciamento VMware e a rede de implantação HCX. Para obter mais informações, consulte Requisitos de rede.
3. Obtenha a função IAM de Administrador de Serviço do VMware Engine.

CRIE SUA PRIMEIRA NUVEM PRIVADA

1. Acesse o portal do VMware Engine.
2. Na página inicial do VMware Engine, clique em **Criar uma nuvem privada**. O local de hospedagem e os tipos de nó de hardware são listados.
3. Selecione o número de nós para a nuvem privada. Pelo menos três nós são necessários.
4. Insira um intervalo de Roteamento Entre Domínios Sem Classe (CIDR) para a rede de gerenciamento VMware.
5. Insira um intervalo CIDR para a rede de implantação HCX.

> **Importante:**
>
> O intervalo CIDR não deve se sobrepor a nenhuma de suas sub-redes locais ou na nuvem. O intervalo CIDR deve ser /27 ou superior.

6. Selecione **Revisar e criar**.
7. Revise as configurações. Para alterar qualquer configuração, clique em **Voltar**.
8. Clique em **Criar** para começar a criar a nuvem privada.

À medida que o VMware Engine cria sua nova nuvem privada, ele implanta vários componentes VMware e configura políticas iniciais de Autoscale™ para clusters na nuvem privada. A criação da nuvem privada pode levar de 30 minutos a 2 horas. Após a conclusão do provisionamento, você receberá um e-mail.

CONFIGURAR O GATEWAY VPN DO GOOGLE CLOUD VMWARE ENGINE

Para estabelecer uma conectividade inicial com o Google Cloud VMware Engine, você pode usar um gateway VPN. Este é um VPN de cliente baseado em OpenVPN, através do qual você pode se conectar ao seu vCenter do VMware Software Defined Data Center (SDDC) e realizar qualquer configuração inicial necessária.

Antes de implantar o gateway VPN, configure o intervalo de **Edge Services** para a região onde seu SDDC está implantado. Para fazer isso:

1. Faça login no portal **Google Cloud VMware Engine** e vá para **Rede > Configurações Regionais**. Clique em **Adicionar Região**.
2. Escolha a região onde seu SDDC está implantado e habilite **Acesso à Internet** e **Serviço de IP Público**.
3. Forneça o intervalo de Serviços de Borda anotado durante o planejamento e clique em **Enviar**. A habilitação desses serviços leva de 10 a 15 minutos.

   Uma vez concluído, os Serviços de Borda aparecem como **Habilitados** na página Configurações Regionais. A habilitação dessas configurações permite que IPs Públicos sejam alocados ao seu SDDC, o que é um requisito para implantar um gateway VPN.

Para implantar um gateway VPN:

1. No portal **Google Cloud VMware Engine**, vá para **Rede > Gateways VPN**. Clique em **Criar Novo Gateway VPN**.
2. Forneça o nome para o gateway VPN e a sub-rede do cliente reservada durante o planejamento. Clique em **Avançar**.
3. Selecione os usuários para conceder acesso VPN. Clique em **Avançar**.
4. Especifique as redes que devem ser acessíveis via VPN. Clique em **Avançar**.
5. Uma tela de resumo é exibida. Verifique as seleções e clique em **Enviar** para criar o Gateway VPN. A página Gateways VPN é exibida com o status do novo gateway VPN como **Criando**.
6. Depois que o status mudar para **Operacional**, clique no novo gateway VPN.
7. Clique em **Baixar minha configuração VPN** para baixar um arquivo ZIP contendo perfis OpenVPN pré-configurados para o gateway VPN. Perfis para conexão via UDP/1194 e TCP/

443 estão disponíveis. Escolha sua preferência e importe-a para o Open VPN e, em seguida, conecte-se.

8. Vá para **Recursos** e selecione seu SDDC.

CONECTAR A VPN

1. Estabeleça uma conexão ponto a site entre sua rede local e a nuvem privada por meio da configuração do Gateway VPN. Consulte Configurar o Gateway VPN do Google Cloud VMware Engine.
2. Carregue a configuração VPN baixada em Configurar o Gateway VPN do Google Cloud VMware Engine.
3. Importe para seu cliente VPN, por exemplo, OpenVPN Connect.

Para obter mais informações, consulte Conectando usando VPN.

CRIAR PRIMEIRA SUB-REDE

Acessar o NSX-T Manager no portal do VMware Engine
O processo de criação de uma sub-rede ocorre no NSX-T, que você acessa por meio do VMware Engine. Faça o seguinte para acessar o NSX-T Manager.

1. Faça logon no portal **Google Cloud VMware Engine**.
2. Na navegação principal, vá para **Recursos**.
3. Clique no **nome da nuvem privada** correspondente à nuvem privada onde você deseja criar a sub-rede.
4. Na página de detalhes da sua nuvem privada, clique na guia **vSphere Management Network**.
5. Clique no **FQDN** correspondente ao NSX-T Manager.
6. Quando solicitado, insira suas credenciais de login. Se você configurou o vIDM e o conectou a uma fonte de identidade, como o Active Directory, use suas credenciais de fonte de identidade.

> **Lembrete:**
>
> Você pode recuperar as credenciais geradas na página de detalhes da nuvem privada.

Configurar o serviço DHCP para a sub-rede
Antes de criar uma sub-rede, configure um serviço DHCP:

No NSX-T Manager:

1. Vá para **Rede > DHCP**. O painel de rede mostra que o serviço DHCP cria um gateway Tier-0 e um gateway Tier-1.
2. Para começar a provisionar um servidor DHCP, clique em **Adicionar Servidor**.
3. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
4. Clique em **Salvar** para criar o serviço DHCP.

Faça o seguinte para anexar este serviço DHCP ao gateway Tier-1 relevante. Um gateway Tier-1 padrão já é provisionado pelo serviço DHCP:

1. Selecione **Gateways Tier 1**, selecione as reticências verticais no gateway Tier-1 e, em seguida, selecione **Editar**.
2. No campo **Gerenciamento de Endereços IP**, selecione **Nenhum Conjunto de Alocação de IP**.
3. Selecione **Servidor DHCP Local** para o **Tipo**.
4. Selecione o servidor DHCP que você criou para o **Servidor DHCP**.
5. Clique em **Salvar**.
6. Clique em **Fechar Edição**.

Agora você pode criar um segmento de rede no NSX-T. Para obter mais informações sobre DHCP no NSX-T, consulte a documentação da VMware para DHCP.

Criar um segmento de rede no NSX-T

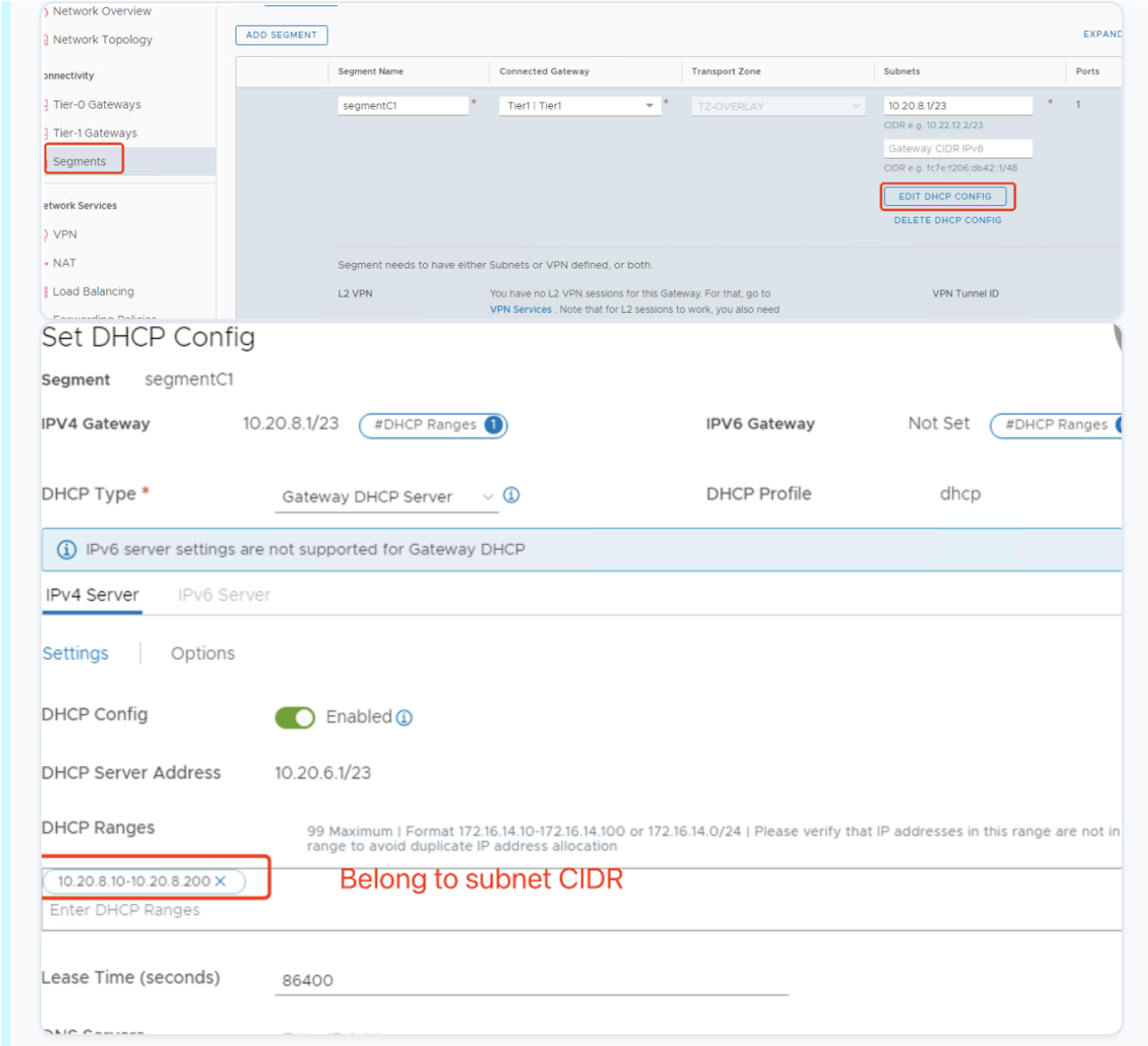
Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede NSX-T para sua nuvem privada:

1. No NSX-T Manager, vá para **Rede > Segmentos**.
2. Clique em **Adicionar Segmento**.
3. Insira um nome para o segmento.
4. Selecione o **Tier-1** como o **Gateway Conectado** e deixe o Tipo como **Flexível**.
5. Clique em **Definir Sub-redes**.
6. Clique em **Adicionar Sub-redes**.
7. Insira o intervalo da sub-rede em **Gateway IP/Prefix Length**. Especifique o intervalo da sub-rede com **.1** como o último octeto. Por exemplo, **10.12.2.1/24**.
8. Especifique os intervalos DHCP e clique em **ADD**.
9. Em **Transport Zone**, selecione **TZ-OVERLAY** na lista suspensa.

10. Clique em **Salvar**. Agora você pode selecionar este segmento de rede no vCenter ao criar uma VM.

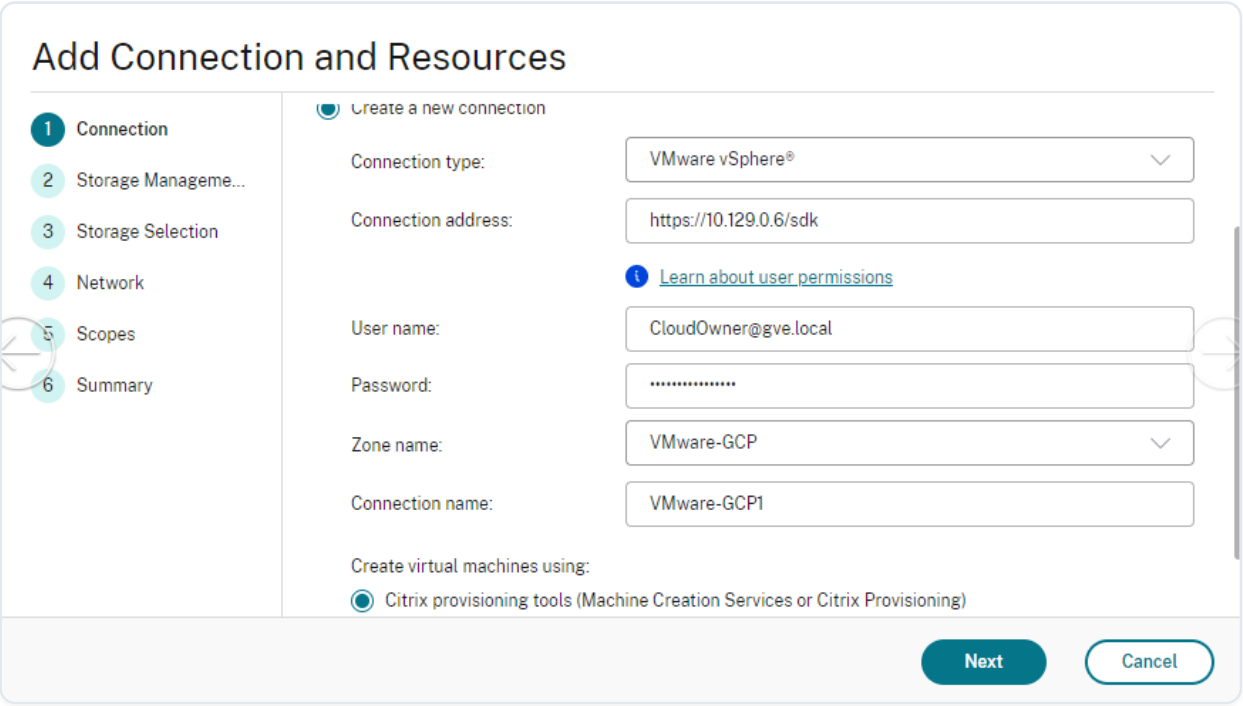
Em uma determinada região, você pode configurar no máximo 100 rotas exclusivas do VMware Engine para sua rede VPC usando acesso a serviços privados. Isso inclui, por exemplo, intervalos de endereços IP de gerenciamento de nuvem privada, segmentos de rede de carga de trabalho NSX-T e intervalos de endereços IP de rede HCX. Este limite inclui todas as nuvens privadas na região.

> **Nota:**
>
> Há um problema de configuração do Google Cloud devido ao qual você precisa configurar a definição do intervalo DHCP várias vezes. Portanto, certifique-se de configurar a definição do intervalo DHCP após a configuração do Google Cloud. Clique em **EDIT DHCP CONFIG** para configurar os intervalos DHCP.



CRIAR A CONEXÃO GOOGLE CLOUD VMWARE NO CITRIX STUDIO

1. Crie uma máquina no vCenter.
2. Inicie o Citrix Studio.
3. Selecione o nó de hospedagem e clique em **Adicionar Conexão e Recursos**.
4. Na tela **Conexão**, selecione **Criar uma nova Conexão** e os seguintes detalhes:



a. Selecione **Tipo de conexão** como **VMware vSphere**.

b. No **Endereço de conexão**, insira o endereço IP privado do vCenter.

c. Insira as credenciais do vCenter.

d. Insira um nome de conexão.

e. Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Rede**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

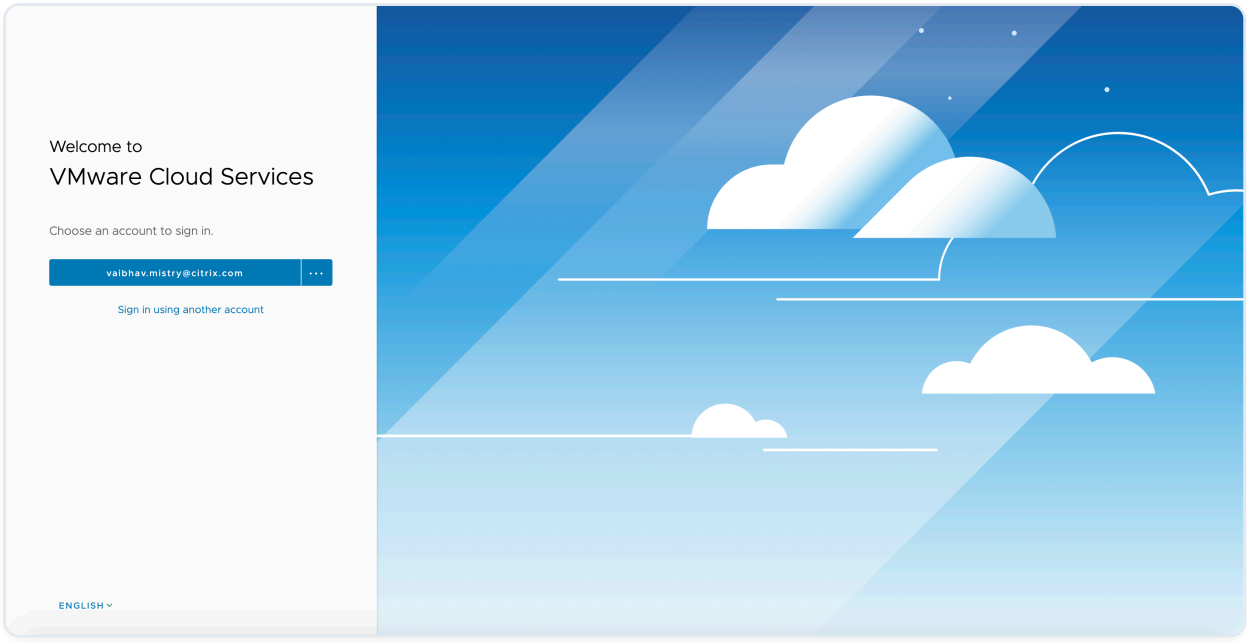
VMware Cloud no Amazon Web Services (AWS)

O VMware Cloud no Amazon Web Services (AWS) permite migrar cargas de trabalho Citrix locais baseadas em VMware para a AWS Cloud.

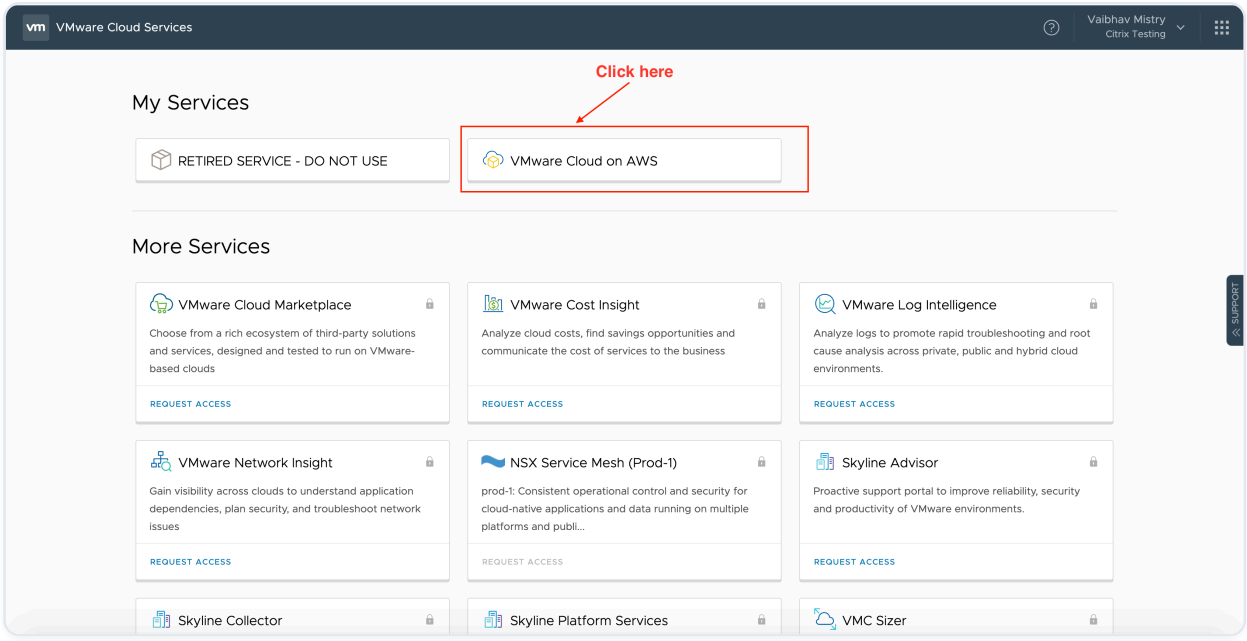
Este artigo descreve o procedimento para configurar um VMware Cloud no AWS.

Acessar o ambiente VMware Cloud

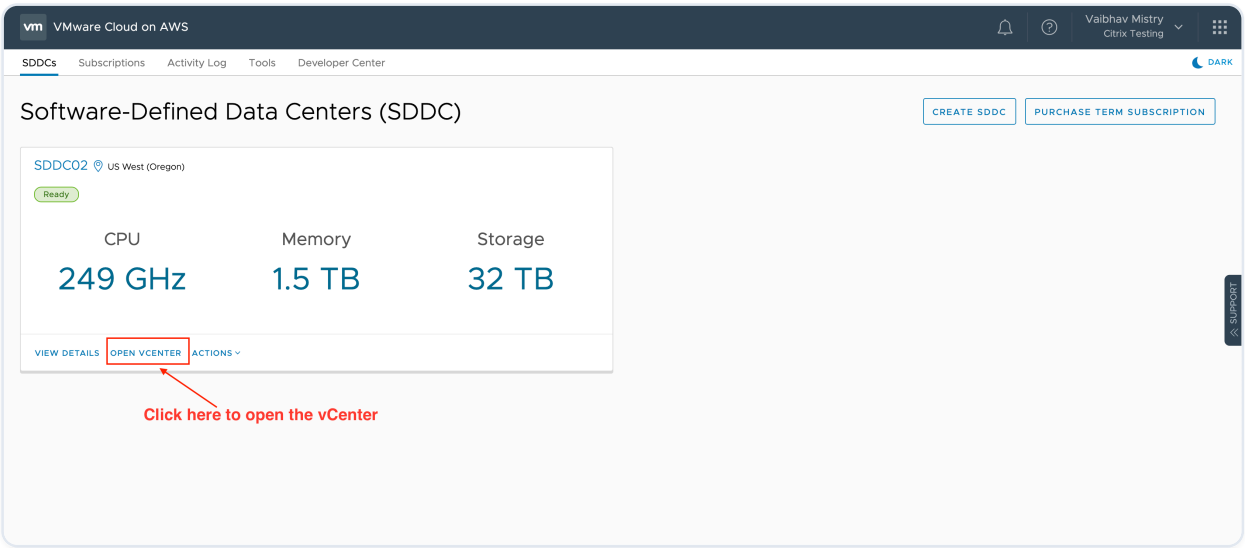
1. Faça login nos serviços de nuvem VMware usando o URL `<https://console.cloud.vmware.com/>`.

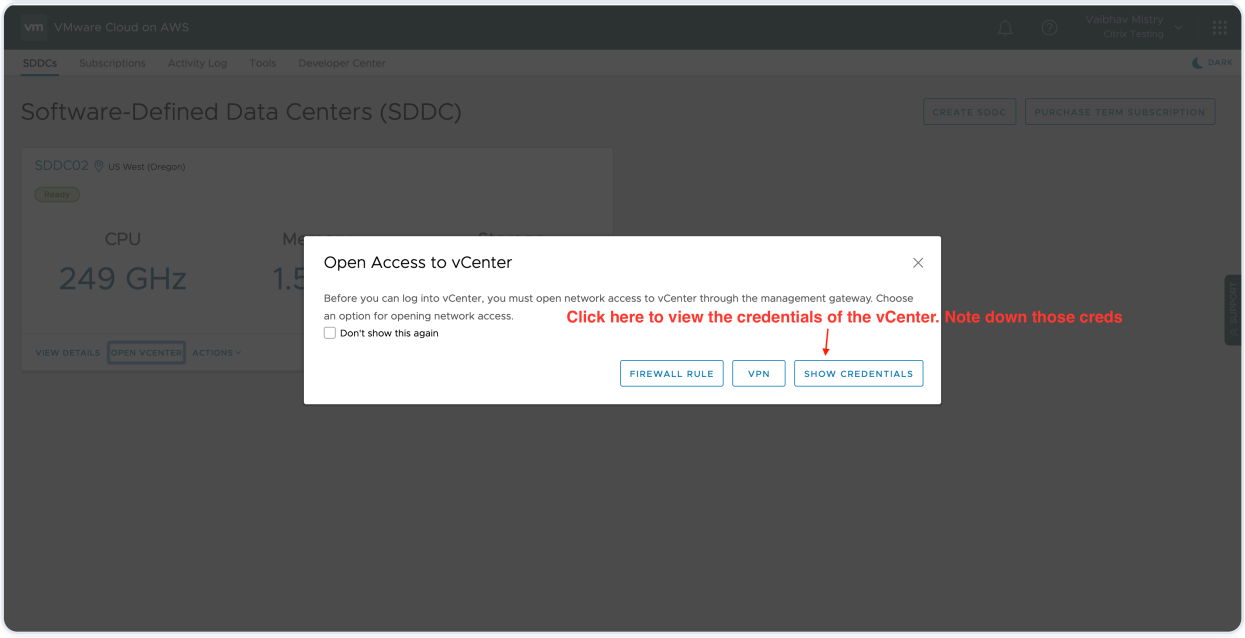


2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

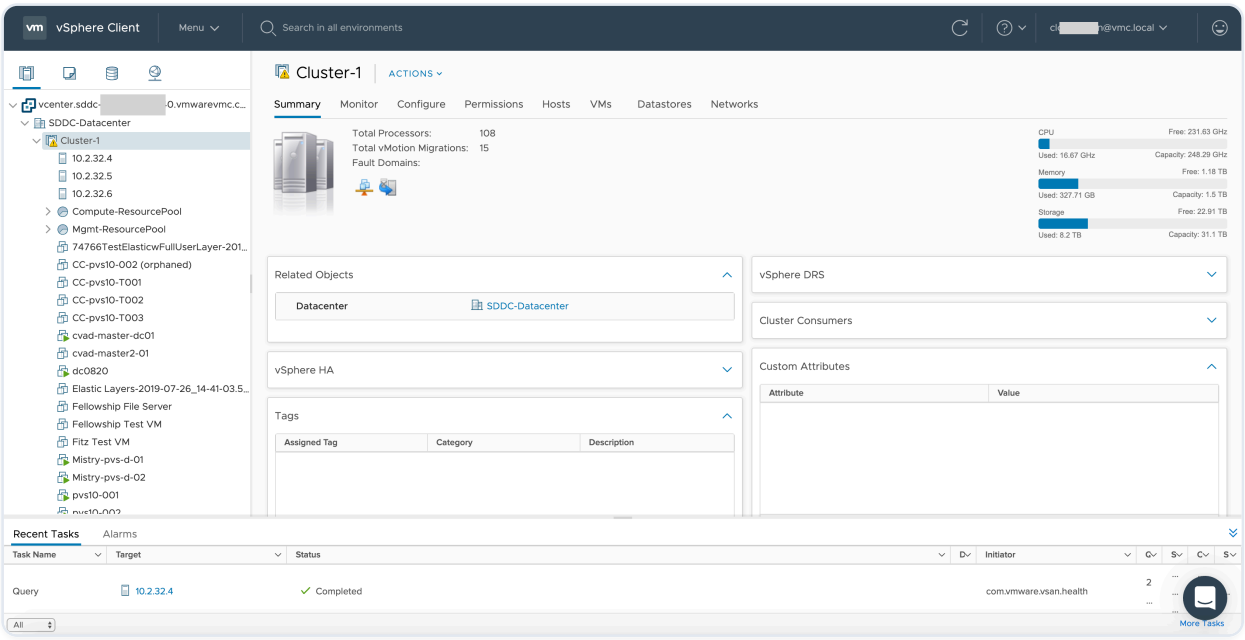


3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Anote as credenciais para uso posterior.





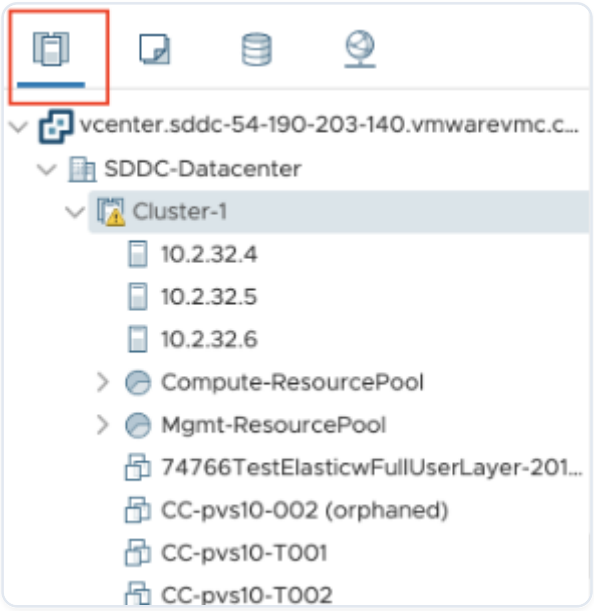
4. Abra um navegador da Web e insira o URL do vSphere Web Client.
5. Insira as credenciais conforme observado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



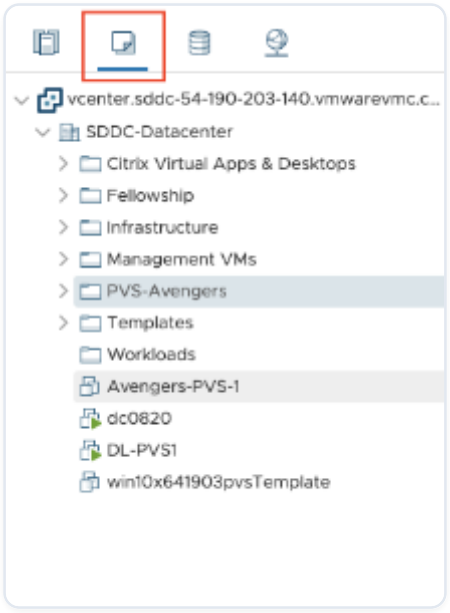
Sobre o ambiente de nuvem VMware

Existem quatro visualizações na página da Web do cliente vSphere.

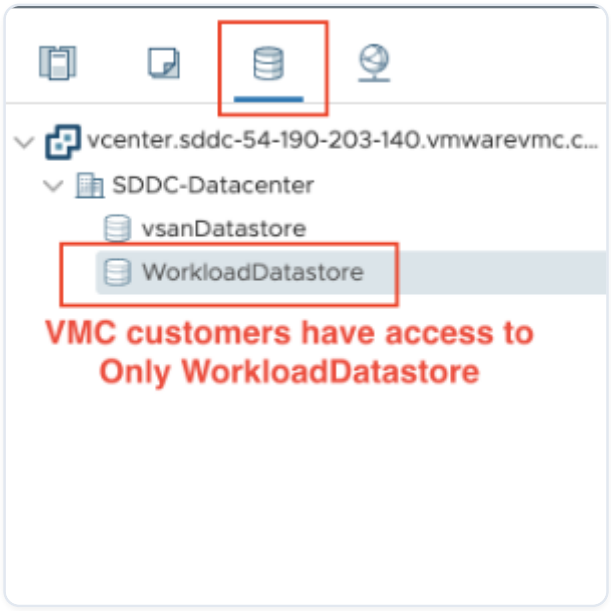
- Visualização de Host e Cluster: Você não pode criar um novo Cluster, mas o administrador da nuvem pode criar vários pools de recursos.



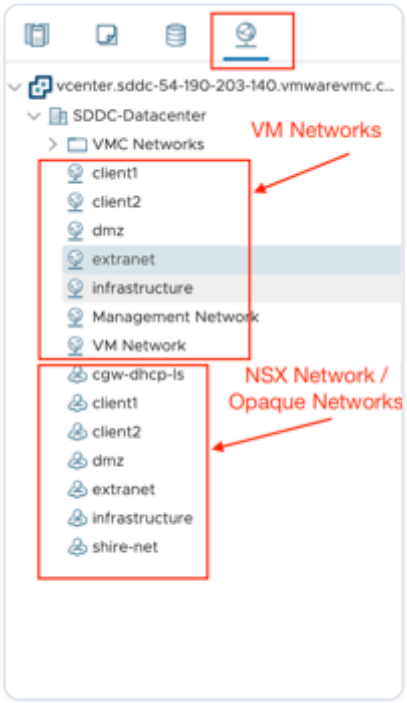
- Visualização de VM e Modelo: O administrador da nuvem pode criar muitas pastas.



- Visualização de Armazenamento: Selecione o armazenamento **WorkloadDatastore** ao adicionar a unidade de hospedagem no Citrix Studio porque você tem acesso apenas ao Workload Datastore.



- Visualização de Rede: Os ícones são diferentes para redes de nuvem VMware e redes opacas.



Depois de configurar o cluster, consulte Ambientes de virtualização VMware para adicionar conexões e recursos.

Próximos passos

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão, consulte Conexão com soluções de nuvem e parceiros VMware

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Instalar componentes principais

> **Importante:**
>
> A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade de licença. Para obter mais informações, consulte Dados de Licenciamento da Citrix.

> Os componentes principais são o Citrix Delivery Controller™, Citrix Studio, Web Studio, Citrix Director e Citrix License Server.

> **Observação:**
>
> O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio — um console de gerenciamento baseado na web que oferece paridade total de recursos com o Citrix Studio. Para obter mais informações sobre o Web Studio, consulte Instalar o Web Studio.

> (Em versões anteriores a 2003, os componentes principais incluíam o Citrix StoreFront. Você ainda pode instalar o StoreFront clicando no bloco **Citrix StoreFront** ou executando o comando disponível na mídia de instalação.)

Antes de iniciar uma instalação, revise este artigo e Preparar para instalar.

Este artigo descreve a sequência do assistente de instalação ao instalar os componentes principais. Equivalentes de linha de comando são fornecidos. Para obter mais informações, consulte Instalar usando a linha de comando.

Etapa 1. Baixe o software do produto e inicie o assistente

Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.

Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.

Faça logon na máquina onde você está instalando os componentes principais, usando uma conta de administrador local.

Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não iniciar automaticamente, clique duas vezes no aplicativo **AutoSelect** ou na unidade montada.

Etapa 2. Escolha qual produto instalar

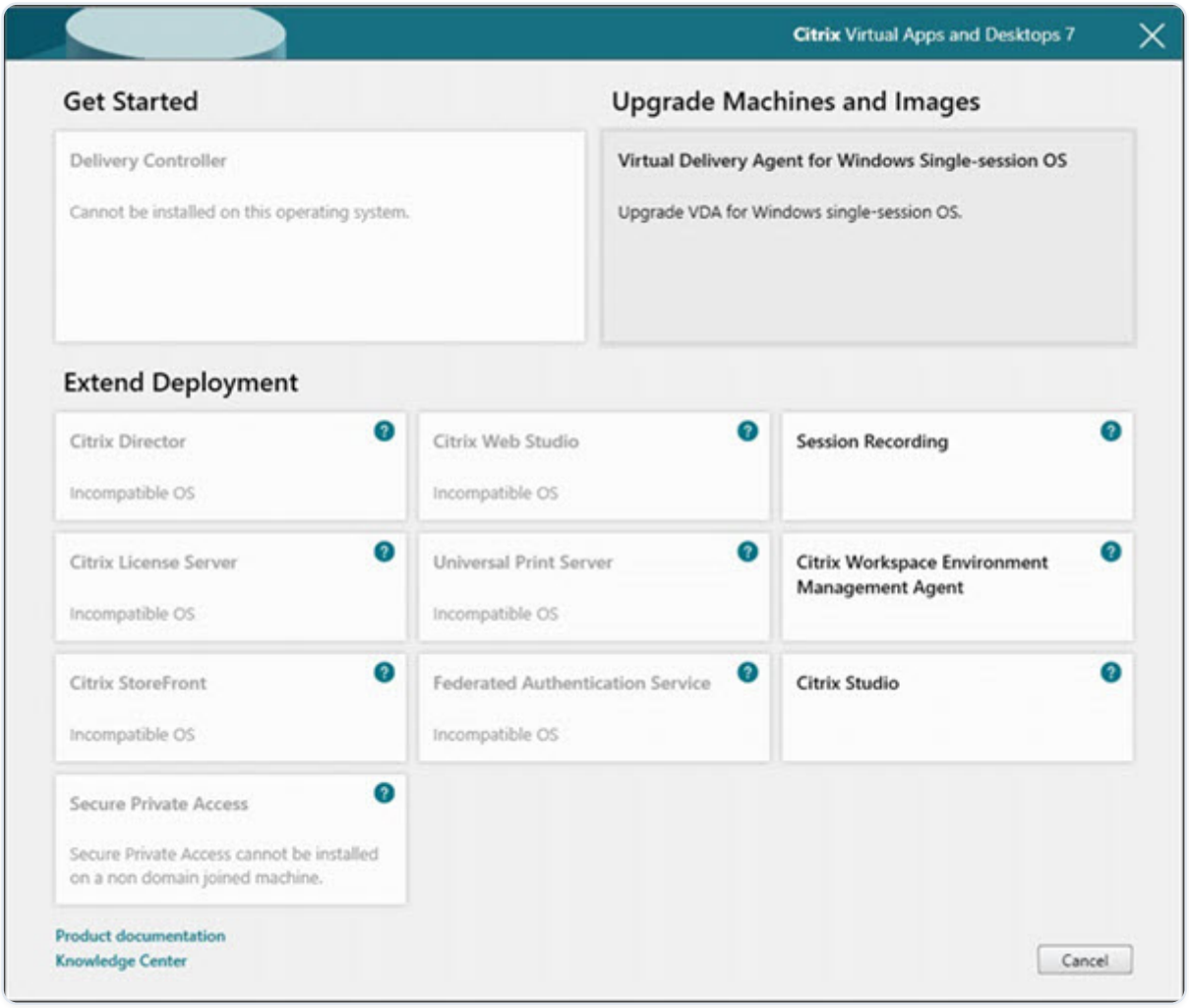


Clique em **Iniciar** ao lado do produto a ser instalado: Virtual Apps ou Virtual Apps and Desktops.

(Se a máquina já tiver componentes do Citrix Virtual Apps and Desktops instalados, esta página não aparecerá.)

Opção de linha de comando: `/xenapp` para instalar o Citrix Virtual Apps. O Citrix Virtual Apps and Desktops será instalado se a opção for omitida.

Etapa 3. Escolha o que instalar

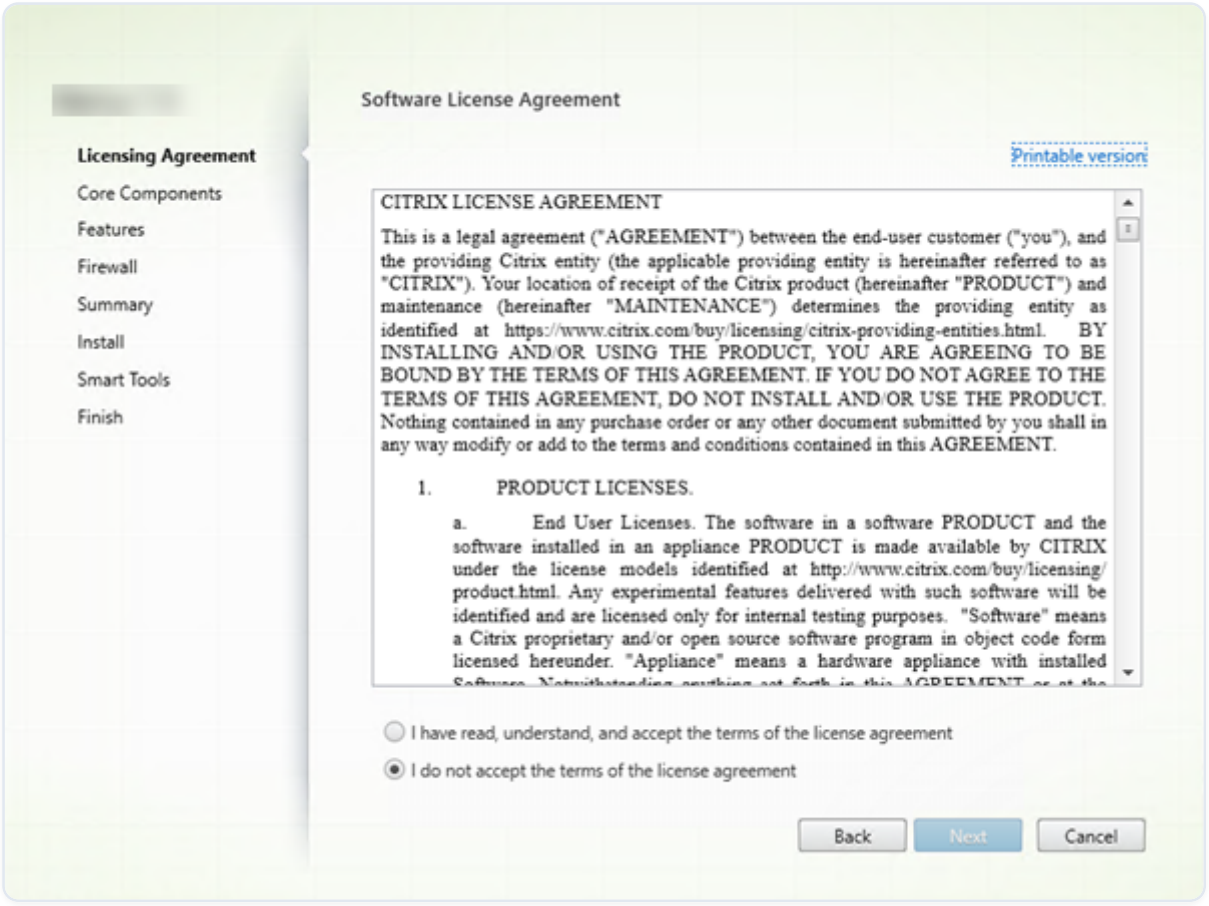


Se você está apenas começando, selecione **Delivery Controller**. (Em uma página posterior, você selecionará os componentes específicos a serem instalados nesta máquina.)

Se você já instalou um Controller (nesta máquina ou em outra) e deseja instalar outro componente, selecione o componente na seção **Estender Implantação**.

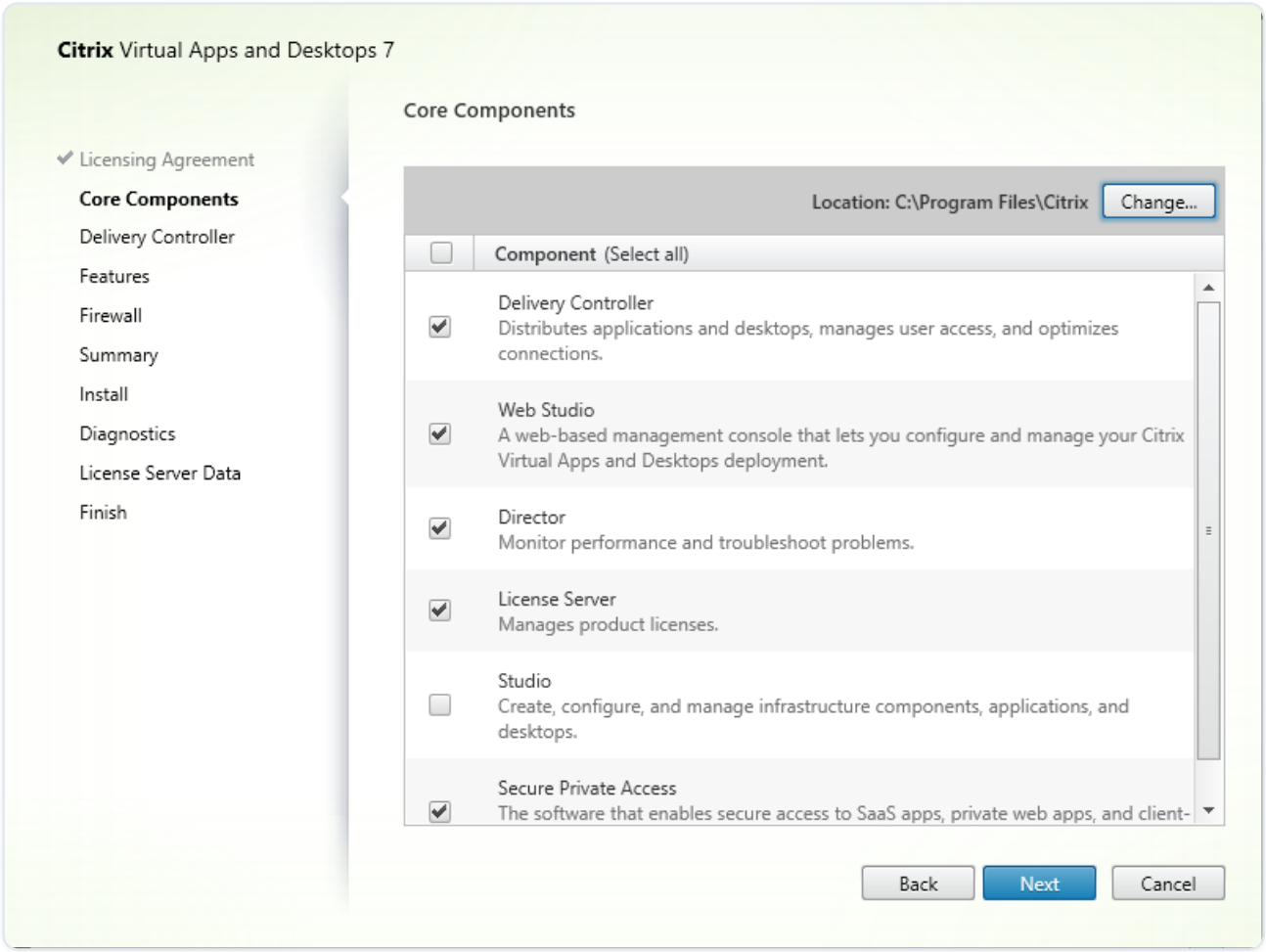
Opção de linha de comando: `/components`

Etapa 4. Leia e aceite o contrato de licença



Na página **Contrato de Licença**, depois de ler o contrato de licença, indique que você o leu e aceitou. Em seguida, clique em **Avançar**.

Etapa 5. Selecione os componentes a serem instalados e o local de instalação



Na página **Componentes principais**:

- **Local:** Por padrão, os componentes são instalados em `C:\Program Files\Citrix`. O padrão é adequado para a maioria das implantações. Se você especificar um local diferente, ele deverá ter permissões de execução para o serviço de rede.
- **Componentes:** Por padrão, as caixas de seleção de todos os componentes principais são selecionadas. A instalação de todos os componentes principais em um servidor é adequada para prova de conceito, teste ou pequenas implantações de produção. Para ambientes de produção maiores, a Citrix recomenda instalar o Director, StoreFront, Secure Private Access e o License Server em servidores separados.

> **Observação:**
>
> Se você estiver instalando componentes em mais de um servidor, instale o Citrix License Server e as licenças primeiro, antes de instalar outros componentes em outros servidores. Para obter orientação, consulte a seção Instalação automática do Guia de Licenciamento para Citrix Virtual Apps and Desktops.

> Um ícone o alerta quando você opta por não instalar um componente principal obrigatório nesta máquina. Esse alerta o lembra de instalar esse componente, embora não necessariamente nesta máquina.

Clique em **Avançar**.

Opções de linha de comando: `/installdir`, `/components`, `/exclude`

Verificação de hardware

Ao instalar ou atualizar um Delivery Controller, o hardware é verificado. O instalador o alerta se a máquina tiver menos do que a quantidade recomendada de RAM (5 GB), o que pode afetar a estabilidade do site. Para obter mais informações, consulte Requisitos de hardware.

Interface gráfica: Uma caixa de diálogo é exibida.

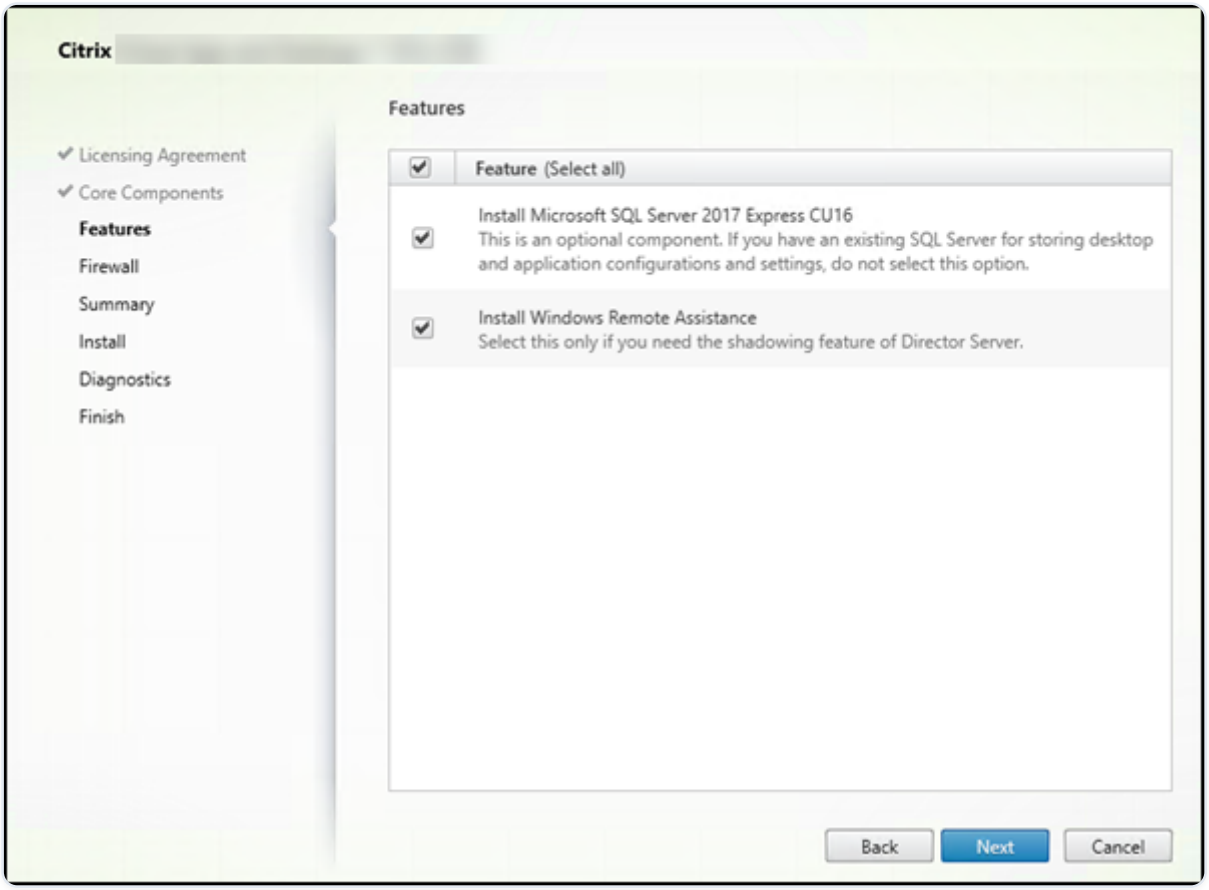
- Recomendado: Clique em **Cancelar** para interromper a instalação. Adicione mais RAM à máquina e inicie a instalação novamente.
- Alternativamente, clique em **Avançar** para continuar com a instalação. O site pode apresentar problemas de estabilidade.

Interface de linha de comando: A instalação/atualização é encerrada. Os logs de instalação contêm uma mensagem que descreve o que foi encontrado e as opções disponíveis.

- Recomendado: Adicione mais RAM à máquina e execute o comando novamente.
- Alternativamente, execute o comando novamente com a opção `/ignore_hw_check_failure` para ignorar o aviso. Seu site pode apresentar problemas de estabilidade.

Ao atualizar, você também é notificado se a versão do SO ou do SQL Server não é mais suportada. Consulte Atualizar uma implantação.

Etapa 6. Habilitar ou desabilitar recursos



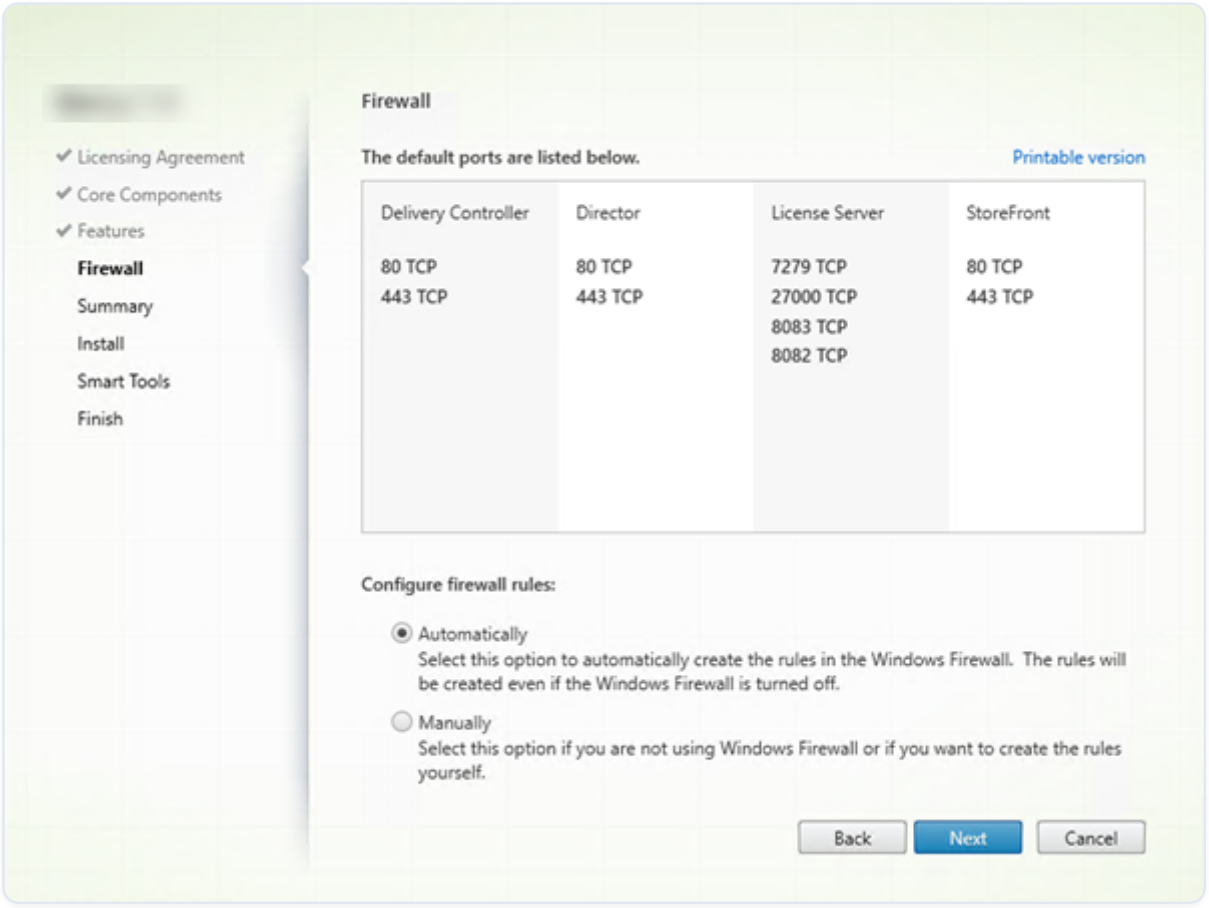
Na página **Recursos**:

- Escolha se deseja instalar o Microsoft SQL Server Express para usar como banco de dados do site. Por padrão, esta seleção está ativada. Se você não estiver familiarizado com os bancos de dados do Citrix Virtual Apps and Desktops, revise Bancos de dados.
- Ao instalar o Director, o Assistência Remota do Windows é instalado automaticamente. Você escolhe se deseja habilitar o shadowing na Assistência Remota do Windows para uso com o shadowing de usuário do Director. Habilitar o shadowing abre a porta TCP 3389. Por padrão, este recurso está habilitado. A configuração padrão é adequada para a maioria das implantações. Este recurso aparece apenas quando você está instalando o Director.

Clique em **Avançar**.

Opções de linha de comando: `/nosql` (para evitar a instalação), `/no_remote_assistance` (para evitar a habilitação)

Etapa 7. Abrir portas do firewall do Windows



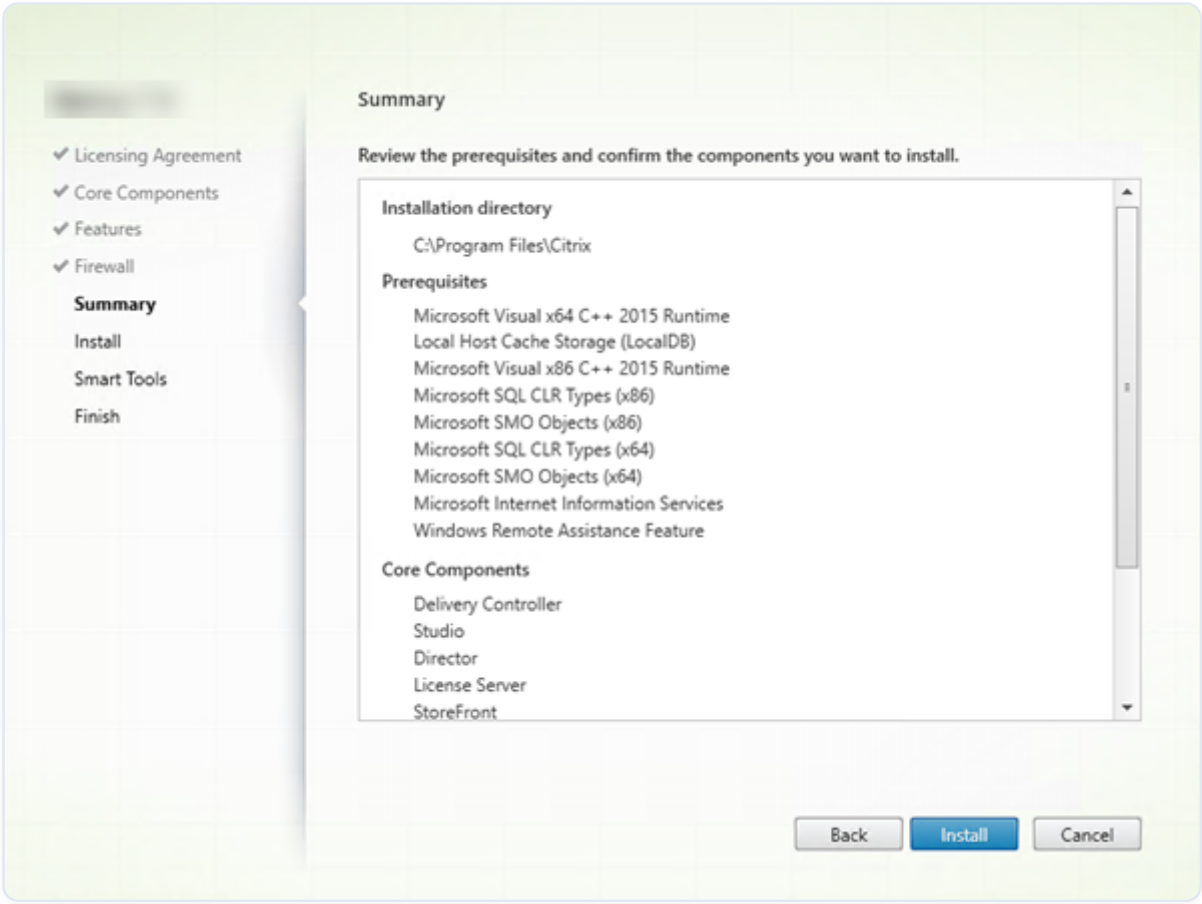
Por padrão, as portas na página **Firewall** são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja habilitado. A configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

(O gráfico mostra as listas de portas quando você instala todos os componentes principais nesta máquina. Esse tipo de instalação geralmente é apenas para implantações de teste.)

Opção de linha de comando: `/configure_firewall`

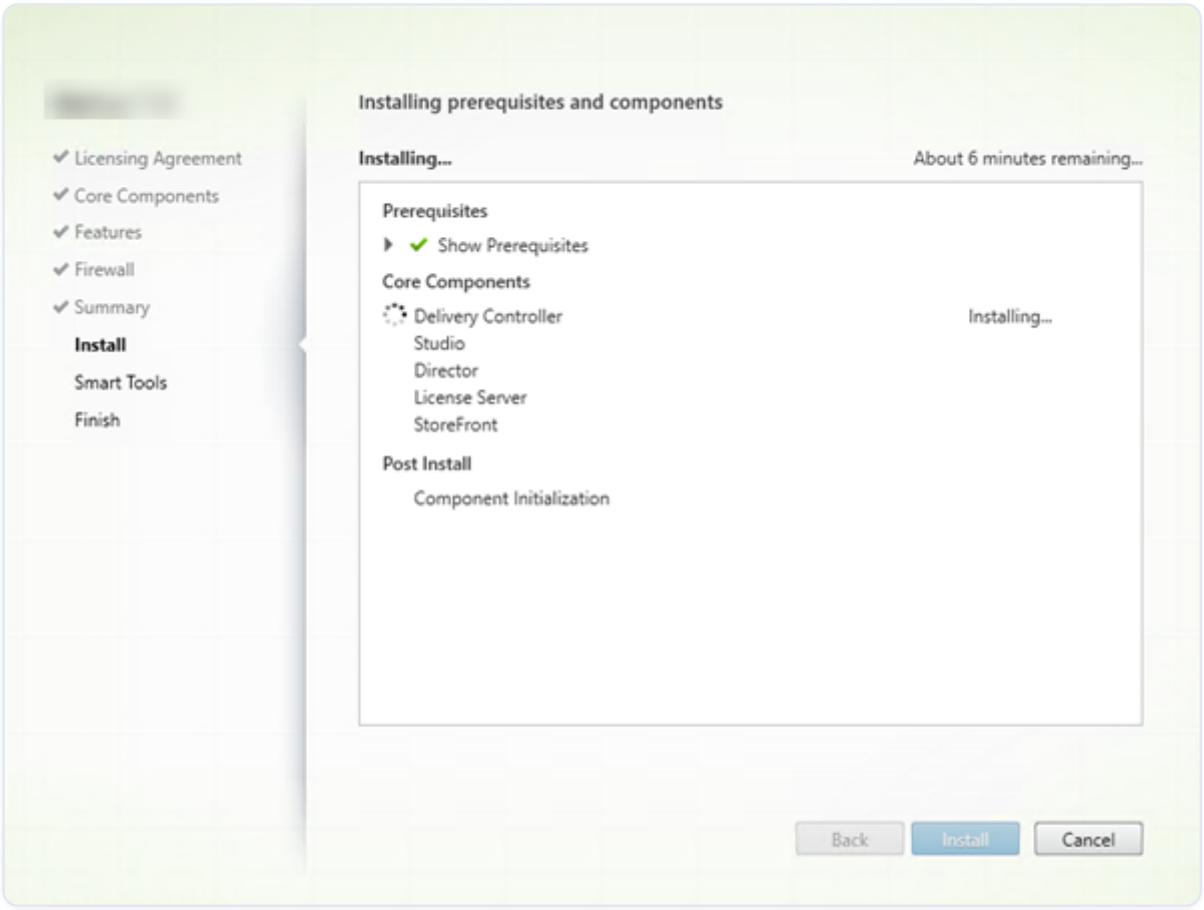
Etapa 8. Revisar pré-requisitos e confirmar a instalação



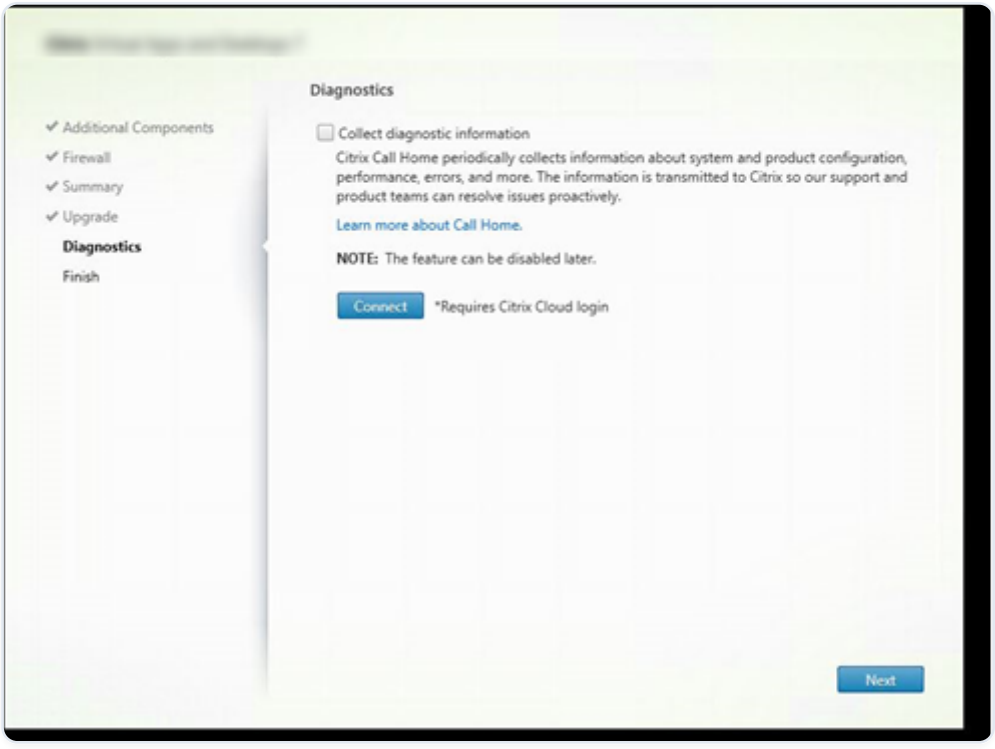
A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções, se necessário.

Quando estiver pronto, clique em **Instalar**.

A tela mostra o progresso da instalação:



Etapa 9. Compartilhando informações de diagnóstico com o Cloud Software Group



Na página **Diagnóstico**, escolha se deseja participar do Citrix Call Home.

Esta página aparece ao instalar um Delivery Controller usando a interface gráfica. Ao instalar o StoreFront (mas não um Controller), o assistente exibe esta página. Ao instalar outros componentes principais (mas não um Controller ou StoreFront), o assistente não exibe esta página.

Durante uma atualização, esta página não aparece se o Call Home já estiver ativado ou se o instalador encontrar um erro relacionado ao Serviço de Telemetria Citrix.

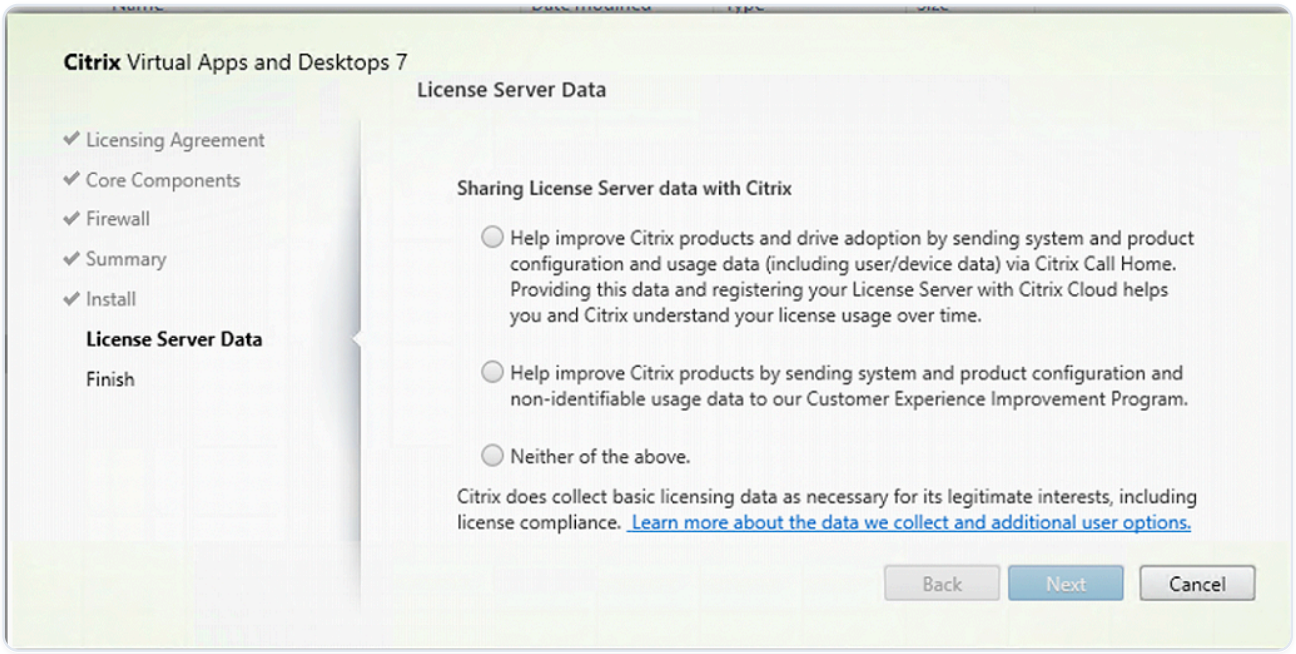
Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix. Você pode alterar sua escolha de inscrição posteriormente, após a instalação.

Depois que suas credenciais forem validadas (ou se você optar por não participar), clique em **Avançar**.

Se você clicar em **Conectar** na página **Diagnóstico** sem primeiro selecionar **Coletar informações de diagnóstico**, depois de fechar a caixa de diálogo **Conectar aos Serviços Citrix Insight**, o botão **Avançar** será desativado. Você não pode ir para a próxima página. Para reativar o botão **Avançar**, selecione e desmarque imediatamente **Coletar informações de diagnóstico**.

Para obter mais informações, consulte Call Home.

Etapa 10. Compartilhamento de dados do License Server com o Cloud Software Group



Na página **Dados do License Server**, solicitamos que você compartilhe dados do Call Home ou dados do Programa de Melhoria da Experiência do Cliente (CEIP) para nos ajudar. Além disso, o

Cloud Software Group também exige a coleta de dados básicos de licenciamento, incluindo conformidade de licença, conforme necessário para seus interesses legítimos.

A página **Dados do License Server** aparece quando você instalou o License Server:

- Como autônomo.
- Como um componente principal, durante a instalação de um Delivery Controller.

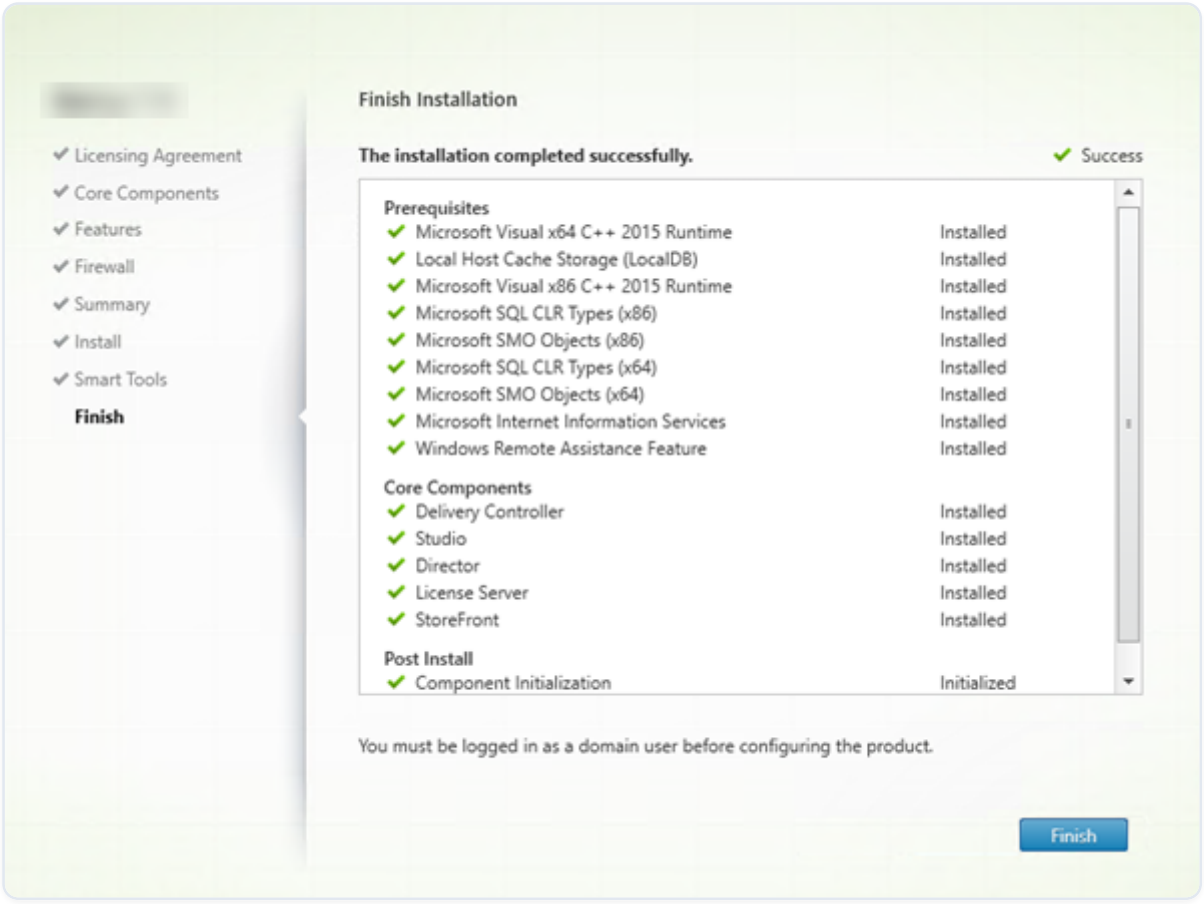
Durante uma atualização, esta página não aparece se a configuração já estiver definida no arquivo `/CITRIX.opt:`.

O License Server monitora vários tipos de dados do usuário, como dados de licenciamento, dados do Call Home e dados do CEIP. Para habilitar a coleta de dados do Call Home e do CEIP, você deve optar por participar (opt in).

Para obter mais informações sobre como habilitar a coleta de dados do Call Home e do CEIP ao instalar usando a linha de comando, consulte Opções de linha de comando para instalar componentes principais.

Para obter mais informações sobre a coleta de dados de licenciamento do Cloud Software Group, consulte Programas de coleta de dados de licenciamento Citrix.

Etapa 11. Concluir esta instalação



A página **Concluir** contém marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com êxito.

Clique em **Concluir**.

Etapa 12. Instalar os componentes principais restantes em outras máquinas

Se você instalou todos os componentes principais em uma máquina, continue com Próximas etapas. Caso contrário, execute o instalador em outras máquinas para instalar outros componentes. Você também pode instalar mais Controllers em outros servidores.

Próximas etapas

Depois de instalar todos os componentes necessários, use o Studio para criar um site.

Após criar o site, instale os VDAs.

A qualquer momento, você pode usar o instalador completo do produto para estender sua implantação com os seguintes componentes:

- **Componente de servidor do Universal Print Server:** Inicie o instalador no seu servidor de impressão.

a. Selecione **Universal Print Server** na seção **Estender Implantação**.

b. Aceite o contrato de licença.

c. Na página **Firewall**, por padrão, as portas TCP 7229 e 8080 são abertas no firewall se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Você pode desativar essa ação padrão se quiser abrir as portas manualmente.

Para instalar este componente a partir da linha de comando, consulte Opções de linha de comando para instalar um Universal Print Server.

- Serviço de Autenticação Federada.
- Gravação de Sessão.
- Gerenciamento do Ambiente de Trabalho.

Instalar o Web Studio

Introdução

O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio — um console de gerenciamento baseado na web que oferece paridade total de recursos com o Citrix Studio. Com a mesma aparência e funcionalidade da interface do Citrix DaaS Studio, o Web Studio moderniza sua experiência de gerenciamento, fornecendo uma experiência web nativa.

Você pode implantar o Web Studio em qualquer servidor Windows com o Internet Information Service (IIS) instalado. Existem duas opções de implantação:

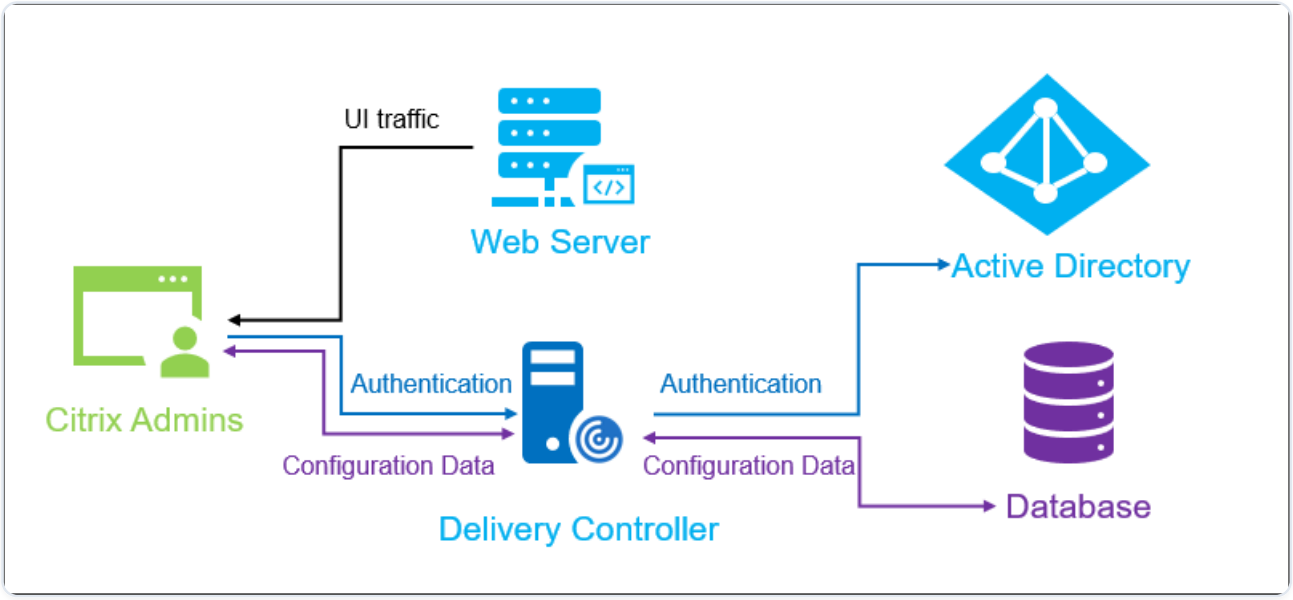
- Instalado em um servidor dedicado:

  Para ambientes maiores onde o desempenho e a escalabilidade são críticos, recomendamos instalar o Web Studio em um servidor dedicado. Este servidor também pode, opcionalmente, hospedar o Director.

- Integrado a um Delivery Controller™:

  Para implantações rápidas e ambientes mais simples, instale o Web Studio diretamente em um Delivery Controller. Essa abordagem é ideal para implantações menores, onde minimizar a sobrecarga administrativa é uma prioridade.

O diagrama a seguir mostra a arquitetura do Web Studio:



Um fluxo de trabalho geral para colocar o Web Studio em funcionamento é o seguinte:

1. Instalar o Web Studio.
2. Configurar um site.
3. Adicionar Delivery Controllers ao Web Studio para gerenciamento.
4. Fazer logon no Web Studio.

Para configurar uma implantação do Web Studio com balanceamento de carga, consulte este artigo.

Novos recursos disponíveis no Web Studio

Consulte o artigo Novidades.

Requisitos do sistema

Sistemas operacionais suportados:

- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter, e com a opção Server Core
- Windows Server 2016, edições Standard e Datacenter, e com a opção Server Core

Navegadores suportados:

- Microsoft Edge 92
- Firefox ESR (Extended Support Release) 90
- Google Chrome 92
- Safari 14

A resolução de tela ideal recomendada para visualizar o Web Studio é 1440 x 1024.

Pré-requisitos

Esta versão do Web Studio é compatível com implantações do Citrix Virtual Apps and Desktops™ 2212 e posteriores.

Para implantações anteriores a 2212, primeiro atualize para 2212 e depois instale o Web Studio.

Limitações conhecidas

Se você usar o Web Studio e o Citrix Studio de forma intercambiável, considere a seguinte limitação: Um modelo criado no Web Studio não é exibido no Citrix Studio, e vice-versa. Isso ocorre porque o Web Studio usa um banco de dados diferente do Citrix Studio para armazenar modelos. Como solução alternativa, crie uma política a partir de um modelo no Web Studio e, em seguida, crie um modelo a partir dessa política no Citrix Studio, e vice-versa.

- Para garantir uma instalação bem-sucedida do Web Studio, não altere o nome do site padrão (**Default Web Site**) no Gerenciador de Serviços de Informações da Internet (IIS). Quaisquer alterações no nome do site padrão resultam em falhas de instalação.

Instalar o Web Studio

As informações a seguir são um suplemento às orientações em Instalar componentes principais. Para instalar o Web Studio:

- Instale o Web Studio usando o instalador ISO completo do produto para Citrix Virtual Apps and Desktops. O instalador ISO verifica os pré-requisitos, instala quaisquer componentes ausentes, configura o site do Web Studio (no Delivery Controller, se incluído na instalação do Delivery Controller) e executa a configuração básica.
- Se o Web Studio não foi incluído durante a instalação, use o instalador para adicionar o Web Studio.
- Ao instalar o Web Studio, você será solicitado a digitar o endereço de um Delivery Controller.

> **Observação:**
>
> - Você pode adicionar mais de um Delivery Controller. O Web Studio tenta se conectar a eles em ordem aleatória. Se o Delivery Controller ao qual o Web Studio está tentando se conectar estiver inacessível, o Web Studio automaticamente recorrerá a outros Delivery Controllers.

- Se o Director foi selecionado em **Componentes Principais** e instalado, os Delivery Controllers que você adicionar aqui serão usados tanto para o Web Studio quanto para o Director.
- Se você não tiver o certificado de confiança pública externo configurado e não quiser solicitar o certificado de uma CA corporativa, você só precisará configurar o FQDN do seu Delivery Controller.
- Se você tiver o certificado de confiança pública externo e puder configurar o DNS público para o seu Delivery Controller, você pode digitar o nome DNS como o endereço do Delivery Controller.
- Se você puder solicitar o certificado da sua CA corporativa e puder especificar seu DNS pessoal, você pode adicionar seu DNS pessoal como o endereço do Delivery Controller.

Adicionar Delivery Controller(/en-us/citrix-virtual-apps-desktops/2407/media/add-delivery-controller.png)

- Para proteger as comunicações entre o navegador e o servidor web e entre o navegador e o Delivery Controller, a criptografia TLS deve ser habilitada no site do IIS que hospeda o Web Studio e no Delivery Controller. Se nenhum certificado TLS for configurado para o Delivery Controller, o instalador cria um certificado autoassinado, com o FQDN do Delivery Controller e localhost como o certificado de nome DNS. Se um certificado TLS for configurado, o instalador não fará nenhuma alteração. Para obter mais informações sobre criptografia TLS, consulte Proteger uma implantação do Web Studio (opcional).
- Na página **Concluir**, a caixa de seleção **Iniciar Gerenciador de Sites** é selecionada por padrão para que o Citrix Site Manager seja aberto automaticamente. Para iniciá-lo mais tarde, abra o menu Iniciar da sua área de trabalho e selecione **Citrix > Citrix Site Manager**. Antes de iniciar o Web Studio, você precisa usar o Citrix Site Manager para criar um site ou ingressar em um site existente. Para obter mais informações, consulte Configurar um site.

  Iniciar Gerenciador de Sites(/en-us/citrix-virtual-apps-desktops/2407/media/launch-site-manager.png)

Observação:

Você também pode usar a linha de comando para instalar o Web Studio. Exemplo: `.\XenDesktopServerSetup.exe /components webstudio /controllers`

> `"ddc1.studio.local" /configure_firewall /quiet`. Para obter mais informações, consulte Instalar usando a linha de comando.

Configurar um site

Para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como um site), use a ferramenta Citrix Site Manager. A ferramenta é instalada automaticamente com um Delivery Controller.

Para configurar um site, siga estas etapas:

1. Em um Delivery Controller, abra o menu Iniciar da área de trabalho e selecione **Citrix > Citrix Site Manager**.
2. No Citrix Site Manager, selecione **Criar um site**. O assistente de Configuração do Site é exibido.
3. Crie um site e configure suas definições da seguinte forma:
   - Na página **Introdução**, digite um nome para o site.
   - A página **Bancos de Dados** contém seleções para configurar os bancos de dados de site, monitoramento e registro de configuração. Para obter mais informações, consulte Etapa 3. Bancos de Dados.
   - Na página **Licenciamento**, especifique o endereço do Servidor de Licenças e, em seguida, indique qual licença usar (instalar). Para obter mais informações, consulte Etapa 4. Licenciamento.
4. Na página **Resumo**, verifique todas as configurações e clique em **Enviar**.

   O endereço IP deste Controller é adicionado automaticamente ao site.

   > **Observação:**
   >
   > O usuário que cria um site se torna um administrador completo para ele. Para obter mais informações, consulte Administração delegada.

Se você instalar um novo Controller após criar um site, deverá adicionar o Controller ao site. As etapas detalhadas são as seguintes:

1. Execute o Citrix Site Manager neste novo Controller.

2. Selecione **Ingressar em um site existente**.
3. Digite o endereço de um Controller que já foi adicionado ao site.
4. Clique em **Enviar**.

Adicionar Delivery Controllers ao Web Studio para gerenciamento

Use a ferramenta de configuração do Studio para adicionar os Delivery Controllers ao Web Studio para gerenciamento. Esta ferramenta está disponível na pasta de instalação do Web Studio.

Por padrão, a ferramenta é instalada na seguinte pasta padrão.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Suponha que você queira configurar os dois Delivery Controllers a seguir para o site que você deseja gerenciar com o Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Execute o seguinte comando PowerShell:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Observação:**
>
> - A ferramenta requer permissões de administrador do computador.
> - As alterações de configuração do Delivery Controller podem não ter efeito imediatamente devido às configurações de cache no servidor IIS. Para efeito imediato, vá para o servidor Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegar para Página Inicial > Sites > Site Padrão e selecione **Reiniciar** no painel Gerenciar Site.
> - Para visualizar todos os parâmetros suportados, execute `StudioConfig.exe --help`.

Configurar o Web Studio como um proxy para Delivery Controllers (opcional)

Por padrão, ao gerenciar sua implantação usando o console do Web Studio, você se conecta tanto ao servidor Web Studio quanto aos Delivery Controllers através do navegador da web. Nós fornecemos uma opção para configurar o servidor Web Studio como um proxy para os Delivery Controllers. Como resultado, você se conecta apenas ao servidor Web Studio ao gerenciar sua implantação.

Esta seção o orienta a configurar um servidor Web Studio como um proxy para Delivery Controllers. Assumimos que o Web Studio e os Delivery Controllers estão instalados em servidores diferentes.

Antes de começar, verifique se você tem todos os componentes principais necessários instalados em sua implantação. Para obter mais informações, consulte Instalar componentes principais.

Para habilitar o modo proxy para o Web Studio, siga estas etapas:

1. No servidor Web Studio, execute o Windows PowerShell como administrador.
2. Execute o seguinte comando onde você substitui `fqdn_of_webstudio_machine` pelo FQDN do seu servidor Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Observação:**
   >
   > Se você tiver uma implantação do Web Studio com balanceamento de carga, substitua `fqdn_of_webstudio_machine` pelo FQDN do servidor de balanceamento de carga (também conhecido como servidor virtual). Para obter mais informações, consulte Configurar uma implantação do Web Studio com balanceamento de carga.

Para desabilitar o modo proxy para o Web Studio, execute este comando PowerShell:

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> **Observação:**
>
> Como prática recomendada, recomendamos que você proteja sua implantação do Web Studio usando um certificado de confiança pública externo ou um certificado de uma Autoridade de Certificação (CA) corporativa. Para obter mais informações, consulte Proteger uma implantação do Web Studio.

Fazer logon no Web Studio

O site do Web Studio está localizado em `https://<address of the server hosting Web Studio>/Citrix/Studio`.

Para fazer logon no Web Studio, abra o menu Iniciar da sua área de trabalho e selecione **Citrix > Citrix Web Studio™**. Os administradores com permissões para o Web Studio devem ser usuários de domínio do Active Directory. Ao fazer logon no Web Studio, considere os seguintes cenários:

- Se você ainda não especificou os Delivery Controllers para o site. Você será solicitado a especificar um Delivery Controller para que receba acesso temporário ao Web Studio.
- Se os Delivery Controllers especificados estiverem atualmente inacessíveis, você não poderá fazer logon no Web Studio. Teste suas conexões para garantir que esses Delivery Controllers estejam acessíveis. Ou especifique um Delivery Controller alternativo para que você receba acesso temporário ao Web Studio.

Próximas etapas

1. Instalar VDAs
2. Use o Web Studio para entregar aplicativos e desktops virtuais aos seus usuários por meio de:
    a. Criação de um catálogo de máquinas
    b. Criação de um grupo de entrega
    c. Criação de um grupo de aplicativos (opcional)

Instalar usando a linha de comando

> **Importante:**
>
> - Se você estiver atualizando e sua versão atual usar ou tiver o software Personal vDisk ou AppDisks instalado, consulte Removendo PvD, AppDisks e hosts não suportados.
> - A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade de licenciamento. Para obter mais informações, consulte Dados de Licenciamento da Citrix.

Introdução

Este artigo se aplica à instalação de componentes em máquinas com sistemas operacionais Windows. Para obter informações sobre VDAs para sistemas operacionais Linux, consulte Agentes de Entrega Virtual Linux.

Este artigo descreve como emitir comandos de instalação do produto. Antes de iniciar qualquer instalação, revise Preparar para instalar. Esse artigo inclui descrições dos instaladores disponíveis.

Para ver o progresso da execução do comando e os valores de retorno, você deve ser o administrador original ou usar **Executar como administrador**. Para obter mais informações, consulte a documentação de comando da Microsoft.

Como complemento ao uso direto dos comandos de instalação, scripts de exemplo são fornecidos no ISO do produto que instalam, atualizam ou removem VDAs em máquinas no Active Directory. Para obter detalhes, consulte Instalar VDAs usando scripts.

Se você tentar instalar ou atualizar em uma versão do sistema operacional Windows que não é suportada para esta versão do Citrix Virtual Apps and Desktops, uma mensagem o guiará para informações sobre suas opções. Consulte Sistemas operacionais anteriores.

Para obter informações sobre como a Citrix relata os resultados das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.

Usar o instalador completo do produto

Para acessar a interface de linha de comando do instalador completo do produto:

1. Baixe o pacote do produto da Citrix. As credenciais da conta Citrix são necessárias para acessar o site de download.
2. Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.
3. Faça logon no servidor onde você está instalando os componentes, usando uma conta de administrador local.
4. Insira o DVD na unidade ou monte o arquivo ISO.
5. No diretório `\x64\XenDesktop Setup` na mídia, execute o comando apropriado.

   Para instalar componentes principais: Execute `XenDesktopServerSetup.exe`, com as opções listadas em Opções de linha de comando para instalar componentes principais.

Para instalar um VDA: Execute `XenDesktopVDASetup.exe` com as opções listadas em Opções de linha de comando para instalar um VDA.

Para instalar o StoreFront: Execute `CitrixStoreFront-x64.exe` na pasta `x64 > StoreFront` na mídia de instalação.

Para instalar o Universal Print Server: Siga as orientações em Opções de linha de comando para instalar um Universal Print Server.

Para instalar o Federated Authentication Service: A Citrix recomenda usar a interface gráfica.

Para instalar o Session Recording: Siga as orientações em Session Recording.

Para instalar o Workspace Environment Management: Siga as orientações em Workspace Environment Management.

Para instalar o Secure Private Access: Execute `XenDesktopSPASetup.exe` na pasta `x64 > XenDesktop` Setup na mídia de instalação. Siga as orientações em Opções de linha de comando para instalar um Secure Private Access.

Opções de linha de comando para instalar componentes principais

As seguintes opções de parâmetro são válidas ao instalar componentes principais com o comando `XenDesktopServerSetup.exe`. Para mais detalhes sobre as opções, consulte Instalar componentes principais.

Observação:

- Não use `/exclude` ao usar opções de linha de comando para instalar componentes principais.
- Se você atualizar um componente usando `/components`, outros componentes também poderão ser atualizados. Isso é para evitar possíveis problemas de compatibilidade entre diferentes componentes.
- Se você quiser atualizar apenas um componente, use o instalador individual desse componente. Consulte Atualizar uma implantação.

- **/ceipoptin** *ceipoptin* etc.

Habilita a coleta de dados do Call Home e dados do Programa de Melhoria da Experiência do Cliente (CEIP). Os valores válidos são:

- `DIAGNOSTIC`: Escolha este valor para permitir que o Citrix Licensing colete dados do Call Home.
- `ANONYMOUS`: Escolha este valor para permitir que o Citrix Licensing colete dados CEIP não identificados (que não identificam usuários).
- `NONE`: Escolha este valor para desabilitar a coleta de dados CEIP pelo Citrix Licensing.

Para obter mais informações sobre a coleta de dados do Call Home, consulte Citrix Licensing Call Home.

Para obter mais detalhes sobre a coleta de dados CEIP, consulte Citrix Licensing Customer Experience Improvement Program.

Para obter mais detalhes sobre os dados CEIP, consulte Citrix Licensing CEIP data elements.

Para obter mais detalhes sobre os dados de licenciamento do License Server, consulte Citrix Licensing Data.

- **/components** *componente* ...

  Lista de componentes separados por vírgula para instalar ou remover. Os valores válidos são:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server
  - `SECUREPRIVATEACCESS`: Secure Private Access

  Se esta opção for omitida, todos os componentes são instalados (ou removidos, se a opção `/remove` também for especificada).

  (Em versões anteriores a 2003, os valores válidos incluíam `STOREFRONT`. Para a versão 2003 e posterior, use o comando de instalação dedicado do StoreFront mencionado em Use o instalador completo do produto).

- **somente-pré-requisitos**

Somente os pré-requisitos para os componentes selecionados serão instalados. Nenhum componente de produto Citrix será instalado.

- **/configure_firewall**

  Abre todas as portas no firewall do Windows usadas pelos componentes que estão sendo instalados, se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall de terceiros ou nenhum firewall, deverá abrir as portas manualmente.

- **/desabilitarmétricasdeexperiência**

  Impede o upload automático de análises coletadas durante a instalação, atualização ou remoção para a Citrix.

- **/help** ou **/h**

  Exibe a ajuda do comando.

- **/ignore_hw_check_failure**

  Permite que a instalação ou atualização do Delivery Controller continue, mesmo que as verificações de hardware falhem (por exemplo, devido a RAM insuficiente). Para obter mais informações, consulte Verificação de hardware.

- **/ignore_site_test_failure**

  Válido apenas durante a atualização do Controller. Geralmente, quaisquer falhas no teste do site são ignoradas e a atualização prossegue. Se omitido (ou definido como falso), qualquer falha no teste do site faz com que o instalador falhe, sem realizar a atualização. Padrão = falso

  Durante uma atualização, esta opção é ignorada se uma versão não suportada do SQL Server for detectada. Para obter detalhes, consulte Verificação de versão do SQL Server.

- **diretorioinstalacao *diretório***

  Diretório vazio existente onde os componentes serão instalados. Padrão = `c:\Program Files\Citrix`.

- **/logpath *caminho***

  Local do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

Válido apenas ao instalar o Director. Desativa o recurso de sombreamento de usuário que usa a Assistência Remota do Windows.

- **/semreinicialização**

  Impede uma reinicialização após a instalação. (Para a maioria dos componentes principais, uma reinicialização não é habilitada por padrão.)

- **/semretomar**

  Por padrão, quando uma reinicialização da máquina é necessária durante uma instalação, o instalador é retomado automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso pode ser útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/NoSQL**

  Impede a instalação do Microsoft SQL Server Express no servidor onde você está instalando o Controller. Se esta opção for omitida, o SQL Server Express será instalado para ser usado como banco de dados do site.

  Esta opção não afeta a instalação do SQL Server Express LocalDB usado para o Local Host Cache.

- **/quiet** ou **/passive**

  Nenhuma interface de usuário aparece durante a instalação. A única evidência do processo de instalação está no Gerenciador de Tarefas do Windows. Se esta opção for omitida, a interface gráfica será iniciada.

- **/remover**

  Remove os componentes principais especificados com a opção `/components`.

- **/removertudo**

  Remove todos os componentes principais instalados.

- **/SKIPHDXDRIVERCHECK**

  Ignora a verificação dos drivers HDX™ para o Meta-instalador do VDA.

- **/enviarmetricasdeexperiencia**

  Envia automaticamente análises coletadas durante a instalação, atualização ou remoção para a Citrix. Se esta opção for omitida (ou `/disableexperiencemetrics` for especificado), as análises são coletadas localmente, mas não são enviadas automaticamente.

- **dirtemp** *diretório*

  Diretório que contém arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

- **/XenApp**

  Instala o Citrix Virtual Apps. Se esta opção for omitida, o Citrix Virtual Apps and Desktops™ será instalado.

Exemplos de instalação de componentes principais

O comando a seguir instala um Delivery Controller™, Studio, Citrix Licensing e SQL Server Express em um servidor. As portas de firewall necessárias para as comunicações dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

O comando a seguir instala um Citrix Virtual Apps™ Controller, Studio e SQL Server Express no servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

O comando a seguir instala um Delivery Controller, Secure Private Access e SQL Server Express em um servidor. As portas de firewall necessárias para a comunicação dos componentes são abertas automaticamente.

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall
```

Usar um instalador VDA autônomo

As credenciais da conta Citrix são necessárias para acessar o site de download. Você deve ter privilégios administrativos elevados antes de iniciar a instalação ou usar **Executar como administrador**.

1. Baixe o pacote apropriado da Citrix:
   - Agente de Entrega Virtual de SO multi-sessão: `VDAServerSetup_xxxx.exe`
   - Agente de Entrega Virtual de SO de sessão única: `VDAWorkstationSetup_xxxx.exe`

- Agente de Entrega Virtual de Serviços Principais de SO de sessão única: `VDAWorkstationCoreSetup_xxxx.exe`

2. Extraia os arquivos do pacote para um diretório existente primeiro e, em seguida, execute o comando de instalação, ou simplesmente execute o pacote.

   Para extrair os arquivos antes de instalá-los, use `/extract` com o caminho absoluto, por exemplo `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. O diretório deve existir. Caso contrário, a extração falha. Em seguida, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

   - Para `VDAServerSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
   - Para `VDAWorkstationCoreSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
   - Para `VDAWorkstationSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

   Para executar o pacote baixado, execute seu nome: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Use as opções válidas listadas neste artigo.

Se você está familiarizado com o instalador completo do produto:

- Execute o instalador autônomo `VDAServerSetup.exe` ou `VDAWorkstationSetup.exe` como se fosse o comando `XenDesktopVdaSetup.exe` em tudo, exceto no nome.
- O instalador `VDAWorkstationCoreSetup.exe` é diferente, pois oferece suporte a um subconjunto das opções disponíveis para os outros instaladores.

Opções de linha de comando para instalar um VDA

As opções a seguir são válidas com um ou mais dos seguintes comandos (instaladores): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` e `VDAWorkstationCoreSetup_xxxx.exe`.

Para obter mais detalhes sobre as opções, consulte Instalar VDAs.

- **/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 para Windows, especifique `/components vda,plugins` ou não especifique nenhum componente. Se nenhum componente for especificado, somente o VDA será instalado por padrão.

Para instalar apenas o VDA e excluir a instalação do aplicativo Citrix Workspace, especifique `/components vda`.

Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup_xxxx.exe`. Esse instalador não pode instalar o aplicativo Citrix Workspace.

- **apenas pré-requisitos**

  Somente os pré-requisitos para os componentes selecionados serão instalados. Nenhum componente do produto Citrix será instalado.

- **controladores** "*controlador* \[*controlador*\]"

  FQDNs de Controllers separados por espaço com os quais o VDA pode se comunicar, entre aspas retas. Não especifique as opções `/site_guid` e `/controllers`.

- **/desabilitarmétricasdeexperiência**

  Impede o upload automático de análises coletadas durante a instalação, atualização ou remoção para a Citrix.

- **/enable_hdx_ports**

  Abre as portas no firewall do Windows exigidas pelo VDA e pelos recursos habilitados (exceto Assistência Remota do Windows), se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

  Para abrir as portas UDP que o transporte adaptativo HDX usa, especifique a opção `/enable_hdx_udp_ports`, além desta opção `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

Abre as portas UDP no firewall do Windows que o transporte adaptativo HDX usa, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

Para abrir portas extras que o VDA usa, especifique a opção `/enable_hdx_ports`, além desta opção `/enable_hdx_udp_ports`.

- **/enable_hdx_tls_dtls**

  Abre as portas TCP e UDP 443 para HDX Direct V1.

- **/enable_real_time_transport**

  Habilita ou desabilita o uso de UDP para pacotes de áudio (RealTime Audio Transport para áudio). Habilitar este 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 de Firewall do Windows for detectado.

- **/enable_remote_assistance**

  Habilita o recurso de sombreamento no Assistência Remota do Windows para uso com o Director. Se você especificar esta opção, o Assistência Remota do Windows abrirá as portas dinâmicas no firewall.

- **/enablerestore** ou **/enablerestorecleanup**

  (Válido apenas para VDAs de sessão única) Habilita o retorno automático ao ponto de restauração, se a instalação ou atualização do VDA falhar.

  Se a instalação/atualização for concluída com êxito:

  - `/enablerestorecleanup` instrui o instalador a remover o ponto de restauração.
  - `/enablerestore` instrui o instalador a reter o ponto de restauração, mesmo que não tenha sido usado.

  Para obter detalhes, consulte Restaurar em caso de falha na instalação ou atualização.

- **/ENABLE_SECURE_DEFAULTS**

  Altera a configuração padrão para vários recursos de habilitado para desabilitado para uma configuração mais segura pronta para uso. Os recursos relevantes são: redirecionamento de unidade cliente, redirecionamento de pasta especial, arrastar e soltar, redirecionamento de dispositivo TWAIN cliente, redirecionamento de dispositivo USB Plug and Play cliente,

redirecionamento de impressora cliente, redirecionamento de área de transferência cliente e redirecionamento de microfone cliente.

- **/enable_ss_ports**

  Abre as portas no Firewall do Windows que são necessárias para o compartilhamento de tela, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente.

- **/exclude** "*componente*"\[,"*componente*"\]

  Impede a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas simples. Por exemplo, instalar ou atualizar um VDA em uma imagem que não é gerenciada pelo MCS não requer o componente Machine Identity Service. Os valores válidos são os seguintes:

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA	SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Universal Print Client`
`Citrix Profile Management`	`Citrix Profile Management`	`Citrix Vda Log Capture Service`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`	`CSE Component`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`	`Director VDA Plug-in`

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA	SERVIÇOS PRINCIPAIS DO SO DE SESSÃO ÚNICA
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA

Excluir o Citrix Profile Management da instalação (`/exclude "Citrix Profile Management"`) afeta o monitoramento e a solução de problemas de VDAs com o Citrix Director. Nas páginas **Detalhes do usuário** e **Ponto de extremidade**, o painel Personalização e o painel Duração do logon falham. Nas páginas **Painel** e **Tendências**, o painel Duração média do logon exibe dados apenas para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Serviço Citrix Profile Management. A habilitação do Serviço Citrix Profile Management não é obrigatória.

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, esse componente não será instalado.

Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente muitos desses itens.

- **/h** ou **/help**

  Exibe a ajuda do comando.

- **/includeadditional** "*componente*"\[,"*componente*"\]

  Inclui a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas simples. Esta opção pode ser útil ao criar uma implantação de Acesso Remoto a PC e desejar instalar outros componentes que não são incluídos por padrão. Os valores válidos são os seguintes:

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`

SO MULTISSESSÃO	SO DE SESSÃO ÚNICA
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, esse componente não será instalado.

- **/installdir** *diretório*

  Diretório vazio existente onde os componentes serão instalados. Padrão = `c:\Program Files\Citrix`.

- **/install_mcsio_driver**

  Não use. Em vez disso, use `/includeadditional "Citrix MCS IODriver"` ou `/exclude "Citrix MCS IODriver"`

- **/logpath** *caminho*

  Local do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = "`%TEMP%\Citrix\XenDesktop Installer`"

  Esta opção não está disponível na interface gráfica.

- **/imagem mestre**

  Válido apenas ao instalar um VDA em uma VM. Configura o VDA como uma imagem a ser usada para criar outras máquinas. Esta opção é equivalente a `/mastermcsimage`.

  Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup_xxxx.exe`.

- **/imagem mestre mcs**

  Especifica que esta máquina será usada como uma imagem com o Machine Creation Services. Esta opção é equivalente a `/masterimage`.

- **/imagem mestre pvs**

Especifica que esta máquina será usada como uma imagem com o Citrix Provisioning™ ou uma ferramenta de provisionamento de terceiros (como o Microsoft System Center Configuration Manager) para provisionar VMs.

- **/websockettoken** *TokenWebSocket*

  Cria um VDA de Web Socket. O WebSocketToken é para o token que é necessário.

- **/websockettokenfile** *ArquivoContendoTokenWebSocket*

  Cria um VDA de Web Socket. O *FileContainingWebSockToken* é para o arquivo que contém o token necessário.

- **/websockettokenstdin** <*TokenWebSocket*

  Cria um VDA de Web Socket. O <*WebSocketToken* é para o token necessário que é passado via STDIN.

- **/no_mediafoundation_ack**

  Reconhece que o Microsoft Media Foundation não está instalado e que vários recursos multimídia HDX não serão instalados e não funcionarão. Se esta opção for omitida e o Media Foundation não estiver instalado, a instalação do VDA será encerrada, pois as pré-condições não foram atendidas. A maioria das edições compatíveis do Windows já vem com o Media Foundation instalado, exceto as edições N. Se você habilitar Recursos do Windows > Recursos de Mídia *manualmente*, a chave do registro procurada pelo Citrix Meta Installer pode não ter um valor definido. Verifique a chave do registro `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` antes de iniciar o processo de instalação para confirmar que o valor existe e não está vazio.

- **/semexperiênciadedesktop**

  O recurso Experiência de Área de Trabalho Aprimorada não está mais disponível. Esta opção (e configuração de política) é ignorada, se especificada.

  Válido apenas ao instalar um VDA para SO multissessão. Impede a habilitação do recurso Experiência de Área de Trabalho Aprimorada. Este recurso também é controlado pela configuração de política Citrix de Experiência de Área de Trabalho Aprimorada.

- **/semreinicialização**

  Impede uma reinicialização após a instalação. O VDA não pode ser usado antes de uma reinicialização.

- **/semretomar**

  Por padrão, quando uma reinicialização da máquina é necessária durante uma instalação, o instalador é retomado automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso pode ser útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/máquinafísica**

  Use este argumento junto com `/remotepc` para a instalação do RemotePC. Caso contrário, o VDA pode não se comportar como esperado em certos cenários de usuário.

- **/númerodaporta** *porta*

  Válido apenas quando a opção `/reconfig` é especificada. Número da porta a ser habilitada para comunicações entre o VDA e o Controller. A porta configurada anteriormente é desabilitada, a menos que seja a porta 80.

- **/proxyconfig** "*endereço ou caminho do arquivo PAC*"

  Se você planeja usar o protocolo Rendezvous com serviços como o Gateway Service em seu ambiente e tiver um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Apenas proxies HTTP são suportados. O endereço ou caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Esta linha de comando instalará automaticamente o Citrix Rendezvous V2 como se /includeadditional "Citrix Rendezvous V2" tivesse sido usado. Para detalhes do recurso, consulte protocolo Rendezvous.

  - Formato do endereço do proxy: `http://<url-or-ip>:<port>`
  - Formato do arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** ou **/passive**

  Nenhuma interface de usuário aparece durante a instalação. A única evidência do processo de instalação e configuração está no Gerenciador de Tarefas do Windows. Se esta opção for omitida, a interface gráfica será iniciada.

- **/reconfigurar**

  Personaliza as configurações do VDA configuradas anteriormente quando usado com as opções `/portnumber`, `/controllers` ou `/enable_hdx_ports`. Se você especificar esta opção sem também especificar a opção `/quiet`, a interface gráfica para personalizar o VDA será iniciada.

- **/pcremoto**

Válido apenas para implantações de Acesso para PC Remoto (SO de sessão única) ou conexões intermediadas (SO multissessão). Exclui a instalação de quaisquer componentes adicionais (consulte as listas de componentes com as opções `/exclude` e `/includeadditional`).

Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente a instalação desses componentes.

`/remotepc` não é compatível com a opção `/servervdi`.

- **/remover**

  Remove os componentes especificados com a opção `/components`.

- **/remove_appdisk_ack**

  Autoriza o instalador do VDA a desinstalar o plug-in AppDisks™ VDA, se estiver instalado.

- **/remove_pvd_ack**

  Autoriza o instalador do VDA a desinstalar o Personal vDisk, se estiver instalado.

- **/removertudo**

  Remove o VDA. Não remove o aplicativo Citrix Workspace (se instalado).

- **/REMOVEALLWITHCWA**

  Remove o CWA junto com o VDA.

- **/enviarmetricasdeexperiencia**

  Envia automaticamente análises coletadas durante a instalação, atualização ou remoção para a Citrix. Se esta opção for omitida (ou a opção `/disableexperiencemetrics` for especificada), as análises são coletadas localmente, mas não são enviadas automaticamente.

- **servidorvdi**

  Instala um VDA para SO de sessão única em uma máquina Windows multissessão suportada. Omita esta opção ao instalar um VDA para SO multissessão em uma máquina Windows multissessão.

  Antes de usar esta opção, consulte Server VDI.

  Use esta opção apenas com o instalador VDA de produto completo.

- **local_guid** *guid*

Identificador Globalmente Único da Unidade Organizacional (OU) do Active Directory do site. Isso associa uma área de trabalho virtual a um site quando você está usando o Active Directory para descoberta (a atualização automática é o método de descoberta recomendado e padrão). O GUID do site é uma propriedade do site exibida no Studio. Não especifique as opções `/site_guid` e `/controllers`.

- **dirtemp** *diretório*

  Diretório para armazenar arquivos temporários durante a instalação. Padrão = `c:\Windows\Temp`.

  Esta opção não está disponível na interface gráfica.

- **máquinavirtual**

  Válido apenas ao instalar um VDA em uma VM. Substitui a detecção pelo instalador de uma máquina física, onde as informações do BIOS passadas para as VMs as fazem parecer máquinas físicas.

  Esta opção não está disponível na interface gráfica.

- **xendesktopnuvem**

  Indica que o VDA está instalado em uma implantação do Citrix DaaS (Citrix Cloud™).

Exemplos de instalação de um VDA

Instalar um VDA com o instalador de produto completo:

O comando a seguir instala um VDA para SO de sessão única e o aplicativo Citrix Workspace no local padrão em uma VM. Este VDA será usado como uma imagem e usará o MCS para provisionar VMs. O VDA se registrará inicialmente com o Controller no servidor chamado `Contr-Main` no domínio `mydomain`. O VDA usará a camada de personalização do usuário e o Assistência Remota do Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional "user personalization layer" /mastermcsimage /enable_remote_assistance
```

Instalar um VDA de SO de sessão única com o instalador autônomo VDAWorkstationCoreSetup:

O comando a seguir instala um VDA de Serviços Principais em um SO de sessão única para uso em uma implantação de Acesso Remoto para PC ou VDI. O aplicativo Citrix Workspace e outros

serviços não essenciais não são instalados. O endereço de um Controller é especificado, e as portas no Serviço de Firewall do Windows serão abertas automaticamente. O administrador manipular os reinícios.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

Personalizar um VDA

Depois de instalar um VDA, você pode personalizar várias configurações. No diretório `\x64\XenDesktop Setup` na mídia do produto, execute `XenDesktopVdaSetup.exe`, usando uma ou mais das seguintes opções, que são descritas em Opções de linha de comando para instalar um VDA.

- `/reconfigure` (obrigatório ao personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Solucionar problemas de VDAs

- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou uma área de trabalho aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Opções de linha de comando para instalar um Universal Print Server

A seguinte opção é válida com o comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

Quando esta opção não é especificada, o instalador exibe a página **Firewall** da interface gráfica. Selecione **Automaticamente** para que o instalador adicione automaticamente as regras de firewall do Windows, ou **Manualmente** para permitir que o administrador configure o firewall manualmente.

Após instalar o software em seus servidores de impressão, configure o Universal Print Server usando as orientações em Provisionar impressoras.

Opções de linha de comando para instalar um Secure Private Access

As seguintes opções são válidas com ambos:

1. Instalador CVAD: `XenDesktopSPASetup.exe`
2. Instalador SPA on-prem: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Abre as portas no firewall do Windows exigidas pelo Secure Private Access, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

- **/sem-sql**

  Impede a instalação do Microsoft SQL Server Express no servidor onde você está instalando o Secure Private Access. Se esta opção for omitida, o SQL Server Express será instalado para ser usado como o banco de dados do site.

- **/help ou /h ou /?**

  Exibe a ajuda do comando

- **/semreinicialização**

  Impede uma reinicialização após a instalação. O Secure Private Access não pode ser usado antes de uma reinicialização.

- **/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.

- **/remover**

  Remove o Secure Private Access.

Para mais detalhes sobre as opções, consulte Secure Private Access installer.

Mais informações

Para obter informações sobre como o Citrix relata o resultado das instalações de componentes, consulte Citrix installation return codes.

Instalar VDAs

> **Importante:**
>
> - Se você estiver atualizando e sua versão atual tiver o software Personal vDisk ou AppDisks instalado, consulte Removendo PvD, AppDisks e hosts não suportados.
> - Os binários distribuídos pela Citrix® agora são assinados. Binários assinados indicam que são validados por certificados gerados pela Citrix ou por certificados autênticos de terceiros.

> Existem dois tipos de VDAs para máquinas Windows: VDA para SO multi-sessão e VDA para SO de sessão única. (Para obter informações sobre VDAs para máquinas Linux, consulte a documentação Linux Virtual Delivery Agent.)

Antes de iniciar uma instalação, revise Preparar para instalar e conclua todas as tarefas de preparação.

Antes de instalar os VDAs, instale os componentes principais. Você também pode criar o site antes de instalar os VDAs.

Este artigo descreve a sequência do assistente de instalação ao instalar um VDA. Equivalentes de linha de comando são fornecidos. Para obter detalhes, consulte Instalar usando a linha de comando.

Etapa 1. Baixe o software do produto e inicie o assistente

Se você estiver usando o instalador completo do produto:

1. Se você ainda não baixou a ISO do produto:
   - Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops™. Baixe o arquivo ISO do produto.

- Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.

2. Use uma conta de administrador local na imagem ou máquina onde você está instalando o VDA. Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não iniciar automaticamente, clique duas vezes no aplicativo **AutoSelect** na unidade montada.

   O assistente de instalação é iniciado.

Se você estiver usando um pacote autônomo:

1. Use suas credenciais de conta Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o pacote apropriado:

   - `VDAServerSetup_2308.exe`: VDA para SO multi-sessão *versão*
   - `VDAWorkstationSetup_2308.exe`: VDA para SO de sessão única *versão*
   - `VDAWorkstationCoreSetup_2308.exe`: VDA de Serviços Principais de SO de sessão única *versão*

2. Clique com o botão direito do mouse no pacote e escolha **Executar como administrador.**

   O assistente de instalação é iniciado.

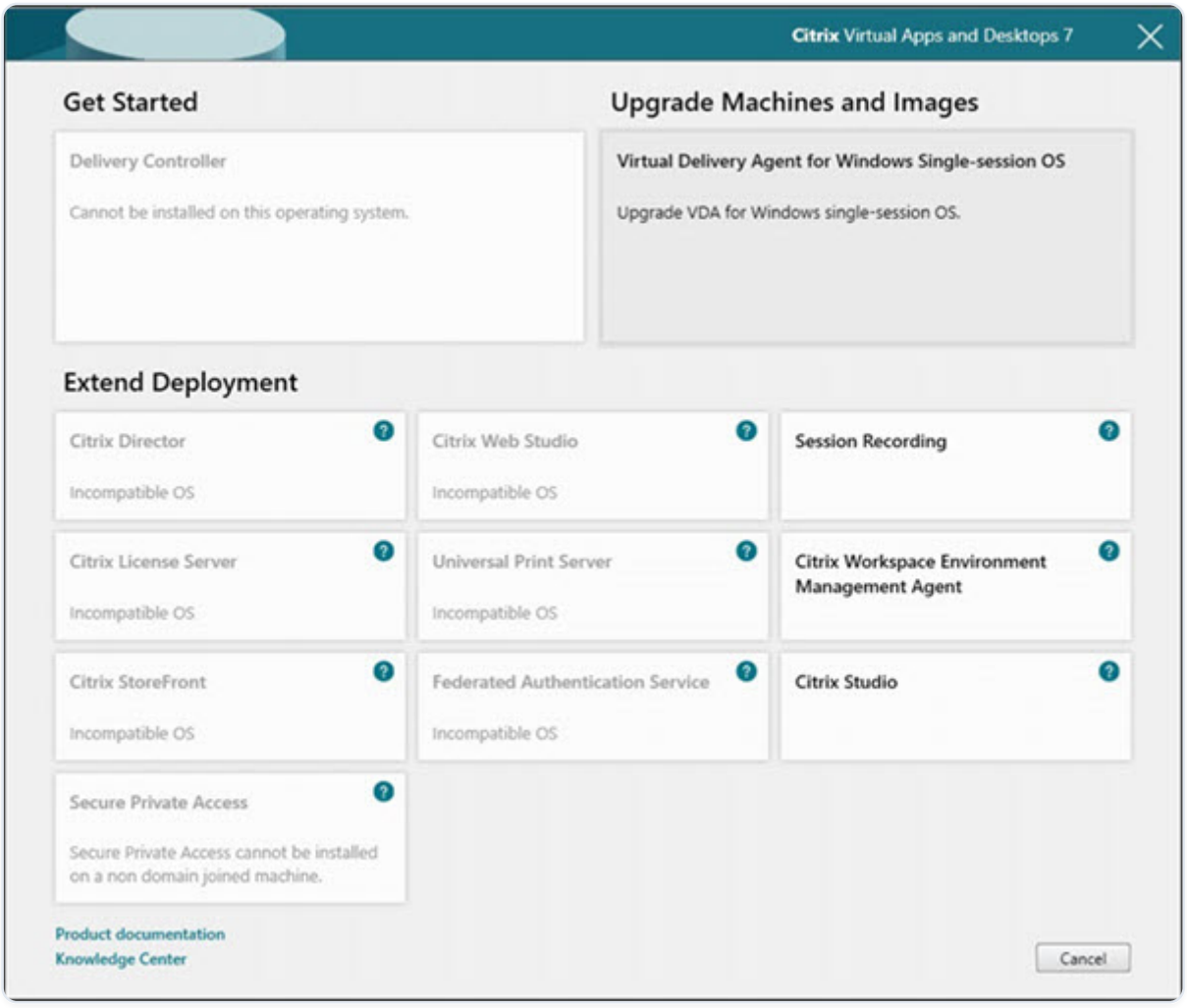
Etapa 2. Escolha qual produto instalar



Clique em **Iniciar** ao lado do produto a ser instalado: Citrix Virtual Apps ou Citrix Virtual Desktops. (Se a máquina já tiver um componente Citrix Virtual Apps ou Citrix Virtual Desktops instalado, esta página não aparecerá.)

Opção de linha de comando: `/xenapp` para instalar o Citrix Virtual Apps. O Citrix Virtual Desktops é instalado se esta opção for omitida.

Etapa 3. Selecione o VDA

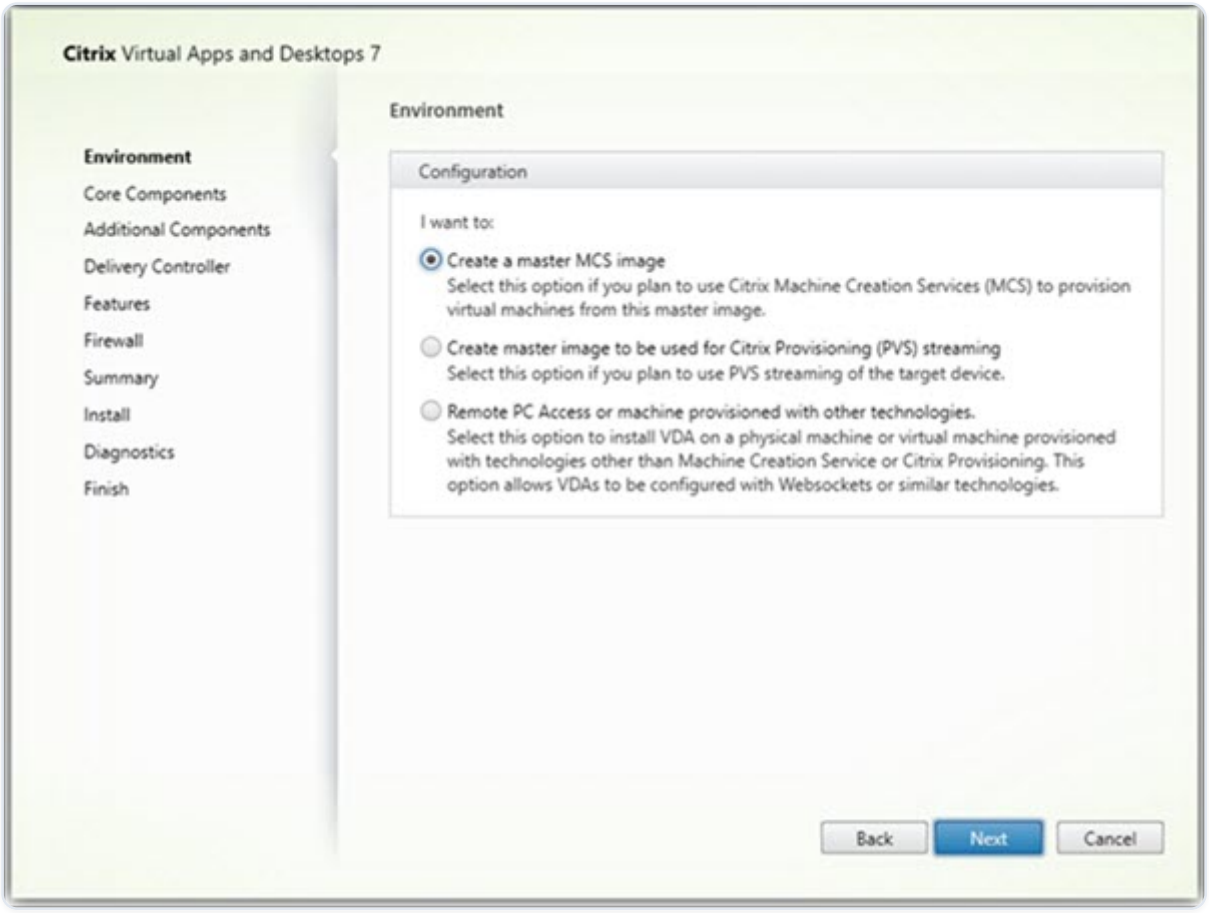


Selecione a entrada **Virtual Delivery Agent**. O instalador sabe se está sendo executado em um SO de sessão única ou multi-sessão, portanto, oferece apenas o tipo de VDA apropriado.

Por exemplo, ao executar o instalador em uma máquina Windows Server 2019, a opção VDA para SO multi-sessão está disponível. A opção VDA para SO de sessão única não é oferecida.

Se você tentar instalar (ou atualizar para) um VDA do Windows em um SO que não seja compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem o guiará para informações sobre as opções.

Etapa 4. Especifique como o VDA será usado



Na página **Ambiente**, especifique como você planeja usar o VDA, indicando se você usa esta máquina como uma imagem para provisionar mais máquinas.

A opção que você escolher afeta quais ferramentas Citrix Provisioning™ são instaladas automaticamente (se houver) e os valores padrão na página Componentes Adicionais do instalador do VDA.

Vários MSIs (de provisionamento e outros) são instalados automaticamente quando você instala um VDA. A única maneira de evitar a instalação é com a opção `/exclude` em uma instalação de linha de comando.

Escolha uma das seguintes opções:

- **Criar uma imagem mestre MCS:** Selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar o 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`

> **Importante:**

> A mídia de instalação ou imagem ISO deve ser montada localmente. Montar uma imagem ISO de um drive de rede para fins de instalação de software não é suportado.

- **Criar uma imagem mestre usando Citrix Provisioning ou ferramentas de provisionamento de terceiros:** 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) para provisionar VMs.

  Opção de linha de comando: `/masterpvsimage`

- (Aparece apenas em máquinas de SO multi-sessão) **Habilitar conexões intermediadas a um servidor:** Selecione esta opção para instalar um VDA em uma máquina física ou virtual que não será usada como uma imagem para provisionar outras máquinas.

  Opção de linha de comando: `/remotepc`

- (Aparece apenas em máquinas de SO de sessão única) **Habilitar Acesso Remoto para PC:** Selecione esta opção para instalar um VDA em uma máquina física para uso com o Acesso Remoto para PC.

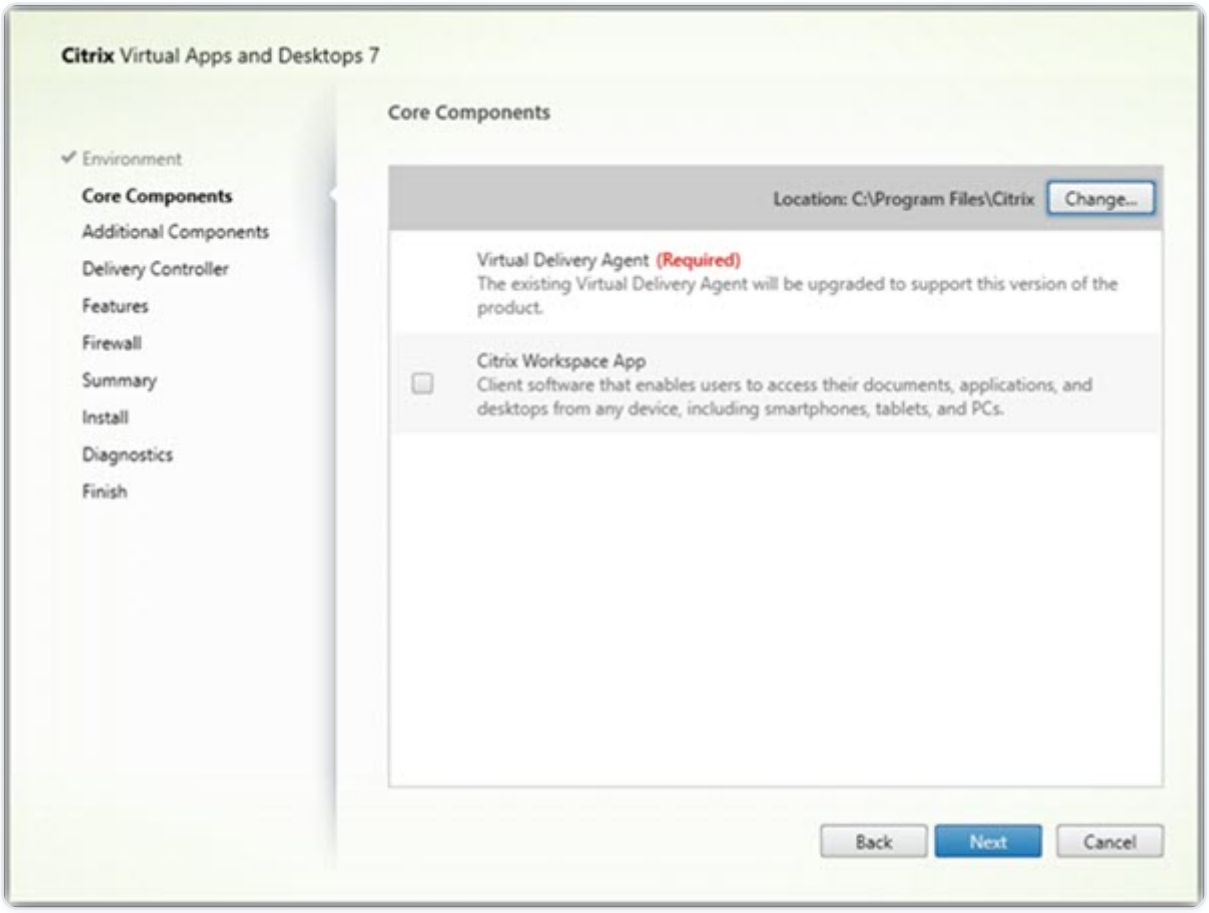
  Opção de linha de comando: `/remotepc`

Clique em **Avançar**.

Esta página não aparece:

- Se você estiver atualizando um VDA
- Se você estiver usando o instalador `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` ou `VDAWorkstationSetup_2308.exe`

Etapa 5. Selecione os componentes a serem instalados e o local de instalação



Na página **Componentes principais**:

- **Local:** 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, esse local deverá ter permissões `execute` para o serviço de rede.
- **Componentes:** Por padrão, o Citrix Workspace App para Windows não é instalado com o VDA. Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`, o Citrix Workspace App para Windows nunca será instalado, portanto, esta caixa de seleção não é exibida.

Clique em **Avançar**.

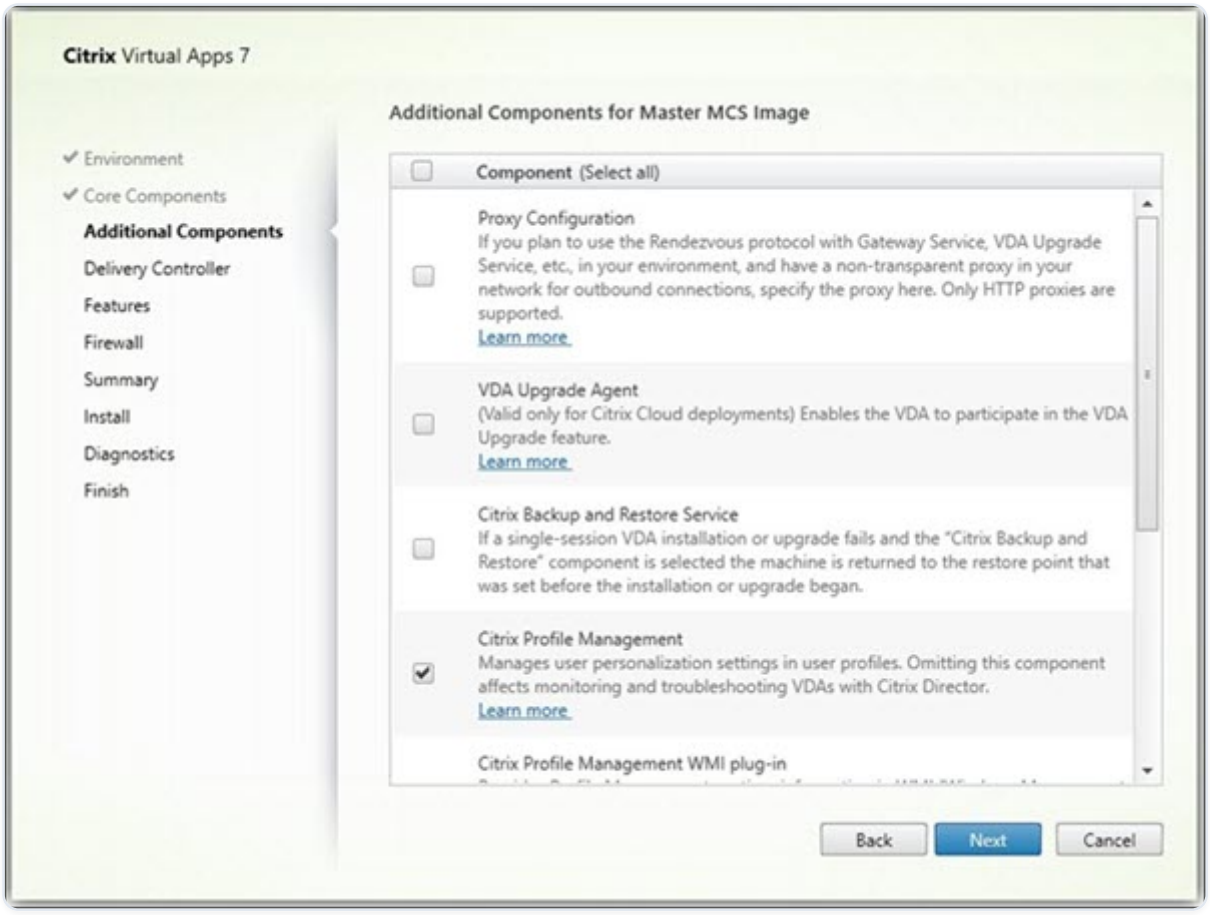
Opções de linha de comando: `/installdir`, `/components vda,plugin` para instalar o VDA e o Citrix Workspace App para Windows

> **Observação:**

> Você pode optar por instalar, atualizar ou desinstalar o Citrix Workspace™ App durante uma instalação, atualização ou desinstalação do VDA nos seguintes cenários:

- Durante uma instalação do VDA, você pode optar por instalar o Citrix Workspace App. Por padrão, o Citrix Workspace App não é instalado durante a instalação do VDA.
- Durante uma atualização do VDA, se o Citrix Workspace App ainda não estiver instalado no VDA, você poderá optar por instalar o Citrix Workspace App.
- Durante uma atualização do VDA, se a versão do Citrix Workspace App puder ser atualizada, a opção de atualizar o Citrix Workspace App será exibida.
- Durante uma desinstalação do VDA, você pode optar por não desinstalar o Citrix Workspace App. Por padrão, o Citrix Workspace App é desinstalado durante a desinstalação do VDA.

Etapa 6. Instalar componentes adicionais



A página **Componentes Adicionais** contém caixas de seleção para habilitar ou desabilitar 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 expressamente um ou mais componentes disponíveis:

- **/includeadditional** "*componente*"\[,"*componente*"\] ...

- **/exclude** "*componente*"\<,"*componente*"\> ...

A tabela a seguir indica a configuração padrão dos itens nesta página. A configuração padrão depende da opção que você selecionou na página **Ambiente**.

PÁGINA COMPONENTES ADICIONAIS	PÁGINA AMBIENTE: "IMAGEM MESTRE COM MCS" OU "IMAGEM MESTRE COM CITRIX PROVISIONING" SELECIONADO	PÁGINA AMBIENTE: "HABILITAR CONEXÕES INTERMEDIADAS AO SERVIDOR" (PARA SO MULTI-SESSÃO) OU "ACESSO REMOTO AO PC" (PARA SO DE SESSÃO ÚNICA) SELECIONADO
Citrix Personalização para App-V - VDA	Não selecionado	Não selecionado
Camada de Personalização do Usuário	Não selecionado	Não exibido porque não é válido para este caso de uso.
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 e Restauração	Não selecionado	Não selecionado
Citrix MCS IODriver	Não selecionado	Não selecionado
Citrix Rendezvous V2	Não selecionado	Não selecionado

Esta página não aparece se:

- Você está usando o instalador `VDAWorkstationCoreSetup.exe`. Além disso, as opções de linha de comando para os componentes adicionais não são válidas com esse instalador.
- Você está atualizando um VDA 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.

Selecione ou desmarque as seguintes caixas de seleção. (Os componentes podem aparecer em uma ordem diferente no instalador.)

- **Citrix Personalization for App-V:** Instale este componente se você usar aplicativos de pacotes Microsoft App-V. Para obter detalhes, consulte Implantar e entregar aplicativos App-V.

  Opção de linha de comando: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar a instalação do componente, `/exclude "Citrix Personalization for App-V – VDA"` para impedir a instalação do componente.

- **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 apenas ao instalar um VDA em uma máquina Windows 10 de sessão única.

  Opção de linha de comando: `/includeadditional "User Personalization Layer"` para habilitar a instalação do componente, `/exclude "User Personalization Layer"` para impedir a instalação do componente.

- **Citrix Profile Management:** Este componente gerencia as configurações de personalização do usuário em perfis de usuário. Para obter detalhes, consulte Gerenciamento de Perfis.

  Excluir o Citrix Profile Management da instalação afeta o monitoramento e a solução de problemas de VDAs com o Citrix Director. Nas páginas **Detalhes do usuário** e **Ponto final**, o painel **Personalização** e o painel **Duração do logon** falham. Nas páginas **Painel** e **Tendências**, o painel **Duração média do logon** exibe dados apenas para máquinas que têm o Profile Management instalado.

  Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Serviço de Gerenciamento de Perfil da Citrix. A ativação do Serviço de Gerenciamento de Perfil da Citrix não é obrigatória.

  Opção de linha de comando: `/includeadditional "Citrix Profile Management"` para habilitar a instalação do componente, `/exclude "Citrix Profile Management"` para impedir a instalação do componente.

- **Citrix Profile Management WMI Plug-in:** Este plug-in fornece informações de tempo de execução do Profile Management em objetos WMI (Windows Management Instrumentation) (por exemplo, provedor de perfil, tipo de perfil, tamanho e uso de disco). Os objetos WMI fornecem informações de sessão ao Director.

  Opção de linha de comando: `/includeadditional "Citrix Profile Management WMI Plug-in"` para habilitar a instalação do componente, `/exclude "Citrix Profile Management WMI Plug-in"` para impedir a instalação do componente.

- **VDA Upgrade Agent:** Aplicável apenas a implantações do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops). Permite que o VDA participe do recurso de atualização do VDA. 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 este agente não estiver instalado, você pode atualizar um VDA executando o instalador do VDA na máquina.

  Opções de linha de comando: `/includeadditional "Citrix VDA Upgrade Agent"` para habilitar a instalação do componente, `/exclude "Citrix VDA Upgrade Agent"` para impedir a instalação do componente.

- **MCSIO write cache for storage optimization:** Instala o driver Citrix MCS I/O. 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 habilitar a instalação do componente, `/exclude "Citrix MCS IODriver"` para impedir a instalação do componente.

- **Proxy Configuration:** Instale este componente se você planeja usar o protocolo Rendezvous com o Gateway Service, VDA Upgrade Service e assim por diante, em seu ambiente, e você tem um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Apenas proxies HTTP são suportados.

  Se você instalar este componente, especifique o endereço do proxy ou o caminho do arquivo PAC na página **Configuração de Proxy Rendezvous**. Para obter detalhes do recurso, consulte protocolo Rendezvous.

  Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para habilitar a instalação do componente, `/exclude "Citrix Rendezvous V2"` para impedir a instalação do componente.

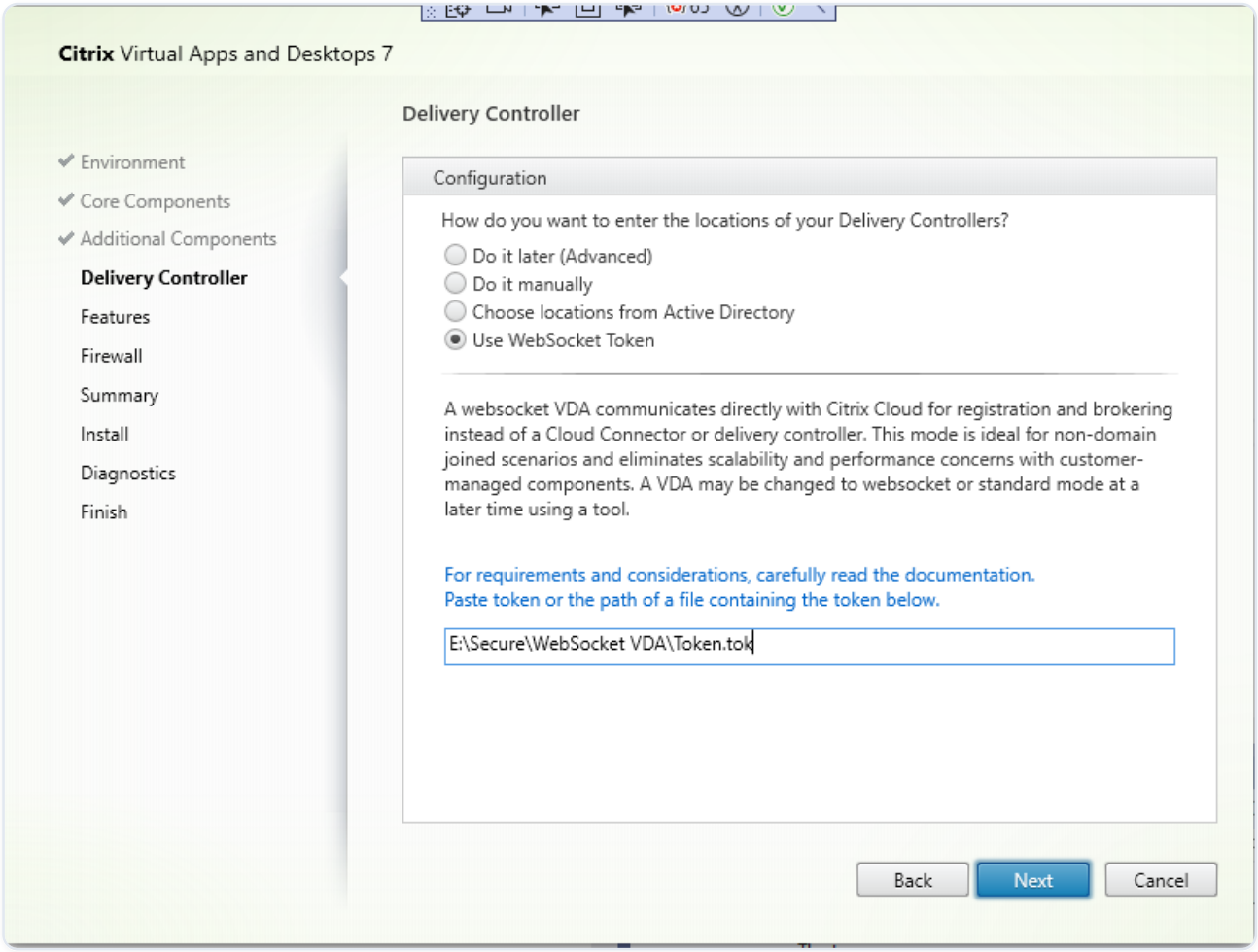
- **Citrix Backup and Restore:** Se uma instalação ou atualização de VDA falhar, este componente pode retornar a máquina a um backup que foi feito antes da instalação ou atualização.

  Certifique-se de que os pré-requisitos da Microsoft sejam atendidos conforme mencionado em Preparar para instalar.

  Opção de linha de comando: `/includeadditional "Citrix Backup and Restore"` para habilitar a instalação do componente, `/exclude "Citrix Backup and Restore"` para impedir a instalação do componente.

> **Observação:**
>
> Se a otimização de armazenamento do MCS estiver habilitada, o backup ou a restauração para o sistema operacional de servidor ou desktop Windows pode falhar. Para resolver isso, desabilite a opção de otimização de armazenamento do MCS no meta instalador.

Etapa 7. Endereços do Delivery Controller™



Na página **Delivery Controller**, escolha como deseja inserir os endereços dos Controllers instalados. A Citrix recomenda que você especifique os endereços durante a instalação do VDA (**Fazer manualmente**). O VDA não pode se registrar em um Controller até que tenha essas informações. Se um VDA não puder se registrar, os usuários não poderão acessar aplicativos e desktops nesse VDA.

- **Fazer manualmente:** (padrão) Insira o FQDN de um Controller instalado e clique em **Adicionar**. Se você instalou mais Controllers, adicione seus endereços.

- **Fazer mais tarde (Avançado):** Se você escolher esta opção, o assistente solicitará que você confirme o que deseja fazer antes de continuar. Para especificar endereços mais tarde, você pode executar novamente o instalador ou usar a Política de Grupo da Citrix. O assistente também o lembrará na página **Resumo**.
- **Escolher locais do Active Directory:** Válido apenas quando a máquina está unida a um domínio e o usuário é um usuário de domínio.
- **Usar Token WebSocket (Tech Preview):** Cria um VDA WebSocket. O WebSocketToken é para o token que é necessário.
- **Deixar o Machine Creation Services fazer isso automaticamente:** Válido apenas ao usar o MCS para provisionar máquinas.

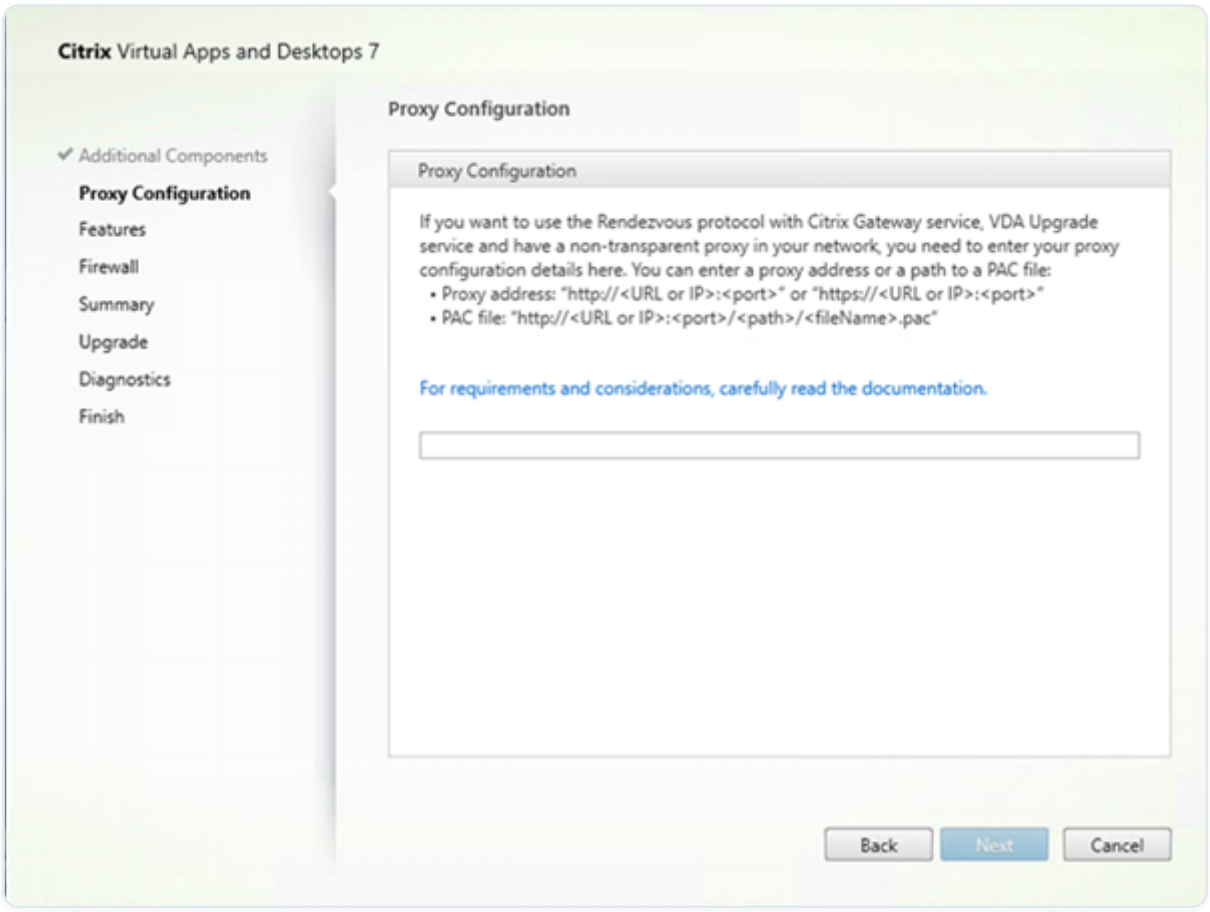
Clique em **Avançar**. Se você selecionou **Fazer mais tarde (Avançado)**, será solicitado que você confirme que especificará os endereços do Controller mais tarde.

Outras considerações:

- O endereço não pode conter caracteres não alfanuméricos.
- Se você especificar endereços durante a instalação do VDA e na Política de Grupo, as configurações da política substituirão as configurações fornecidas durante a instalação.
- O registro bem-sucedido do VDA exige que as portas do firewall usadas para se comunicar com o Controller estejam abertas. Essa ação é habilitada por padrão na página **Firewall** do assistente.
- Depois de especificar os locais do Controller (durante ou após a instalação do VDA), você pode usar o recurso de atualização automática para atualizar os VDAs quando os Controllers forem adicionados ou removidos. Para obter detalhes sobre como os VDAs descobrem e se registram nos Controllers, consulte Registro do VDA.

Opção de linha de comando: `/controllers`

Etapa 8. Configuração do Proxy



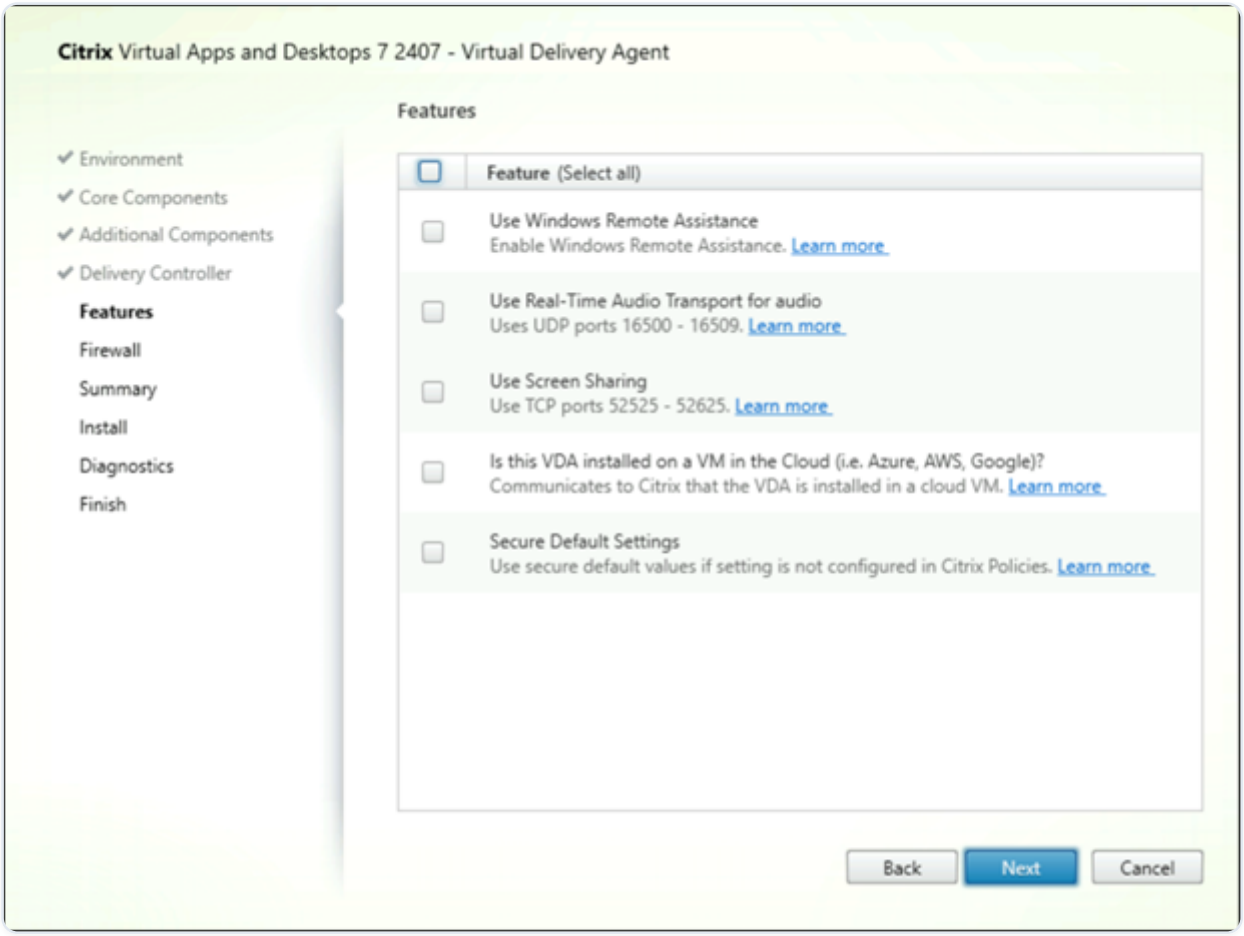
A página **Configuração do Proxy** aparece somente se você habilitou a caixa de seleção **Configuração do Proxy** na página **Componentes Adicionais**.

1. Selecione se você especificará a origem do proxy por endereço de proxy ou caminho do arquivo PAC.
2. Especifique o endereço do proxy ou o caminho do arquivo PAC.
    - Formato do endereço do proxy: `http://<url-or-ip>:<port>`
    - Formato do arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

O firewall para a porta do proxy deve estar aberto para que o teste de conexão seja bem-sucedido. Se uma conexão não puder ser feita com o proxy, você poderá escolher se deseja continuar com a instalação do VDA.

Opção de linha de comando: `/proxyconfig`

Etapa 9. Habilitar ou desabilitar recursos



Na página **Recursos**, use as caixas de seleção para habilitar ou desabilitar os recursos que você deseja usar.

- **Usar Assistência Remota do Windows:** Quando este recurso está ativado, a Assistência Remota do Windows é usada com o recurso de sombreamento de usuário do Director. A Assistência Remota do Windows abre as portas dinâmicas no firewall. (Padrão = desativado)

  Opção de linha de comando: `/enable_remote_assistance`

- **Usar Transporte de Áudio em Tempo Real para áudio:** Ative este recurso se o voice-over-IP for amplamente utilizado em sua rede. O recurso reduz a latência e melhora a resiliência do áudio em redes com perdas. Ele permite que os dados de áudio sejam transmitidos usando RTP sobre transporte UDP. (Padrão = desativado)

  Opção de linha de comando: `/enable_real_time_transport`

- **Usar compartilhamento de tela:** 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`

- **Este VDA está instalado em uma VM na nuvem:** Esta configuração ajuda a Citrix a identificar corretamente os locais de recursos para implantações de VDA locais e de serviço (Citrix Cloud™) para fins de telemetria. Este recurso não tem impacto na utilização do lado do cliente. Ative esta configuração se sua implantação usar Citrix DaaS (Padrão = desativado).

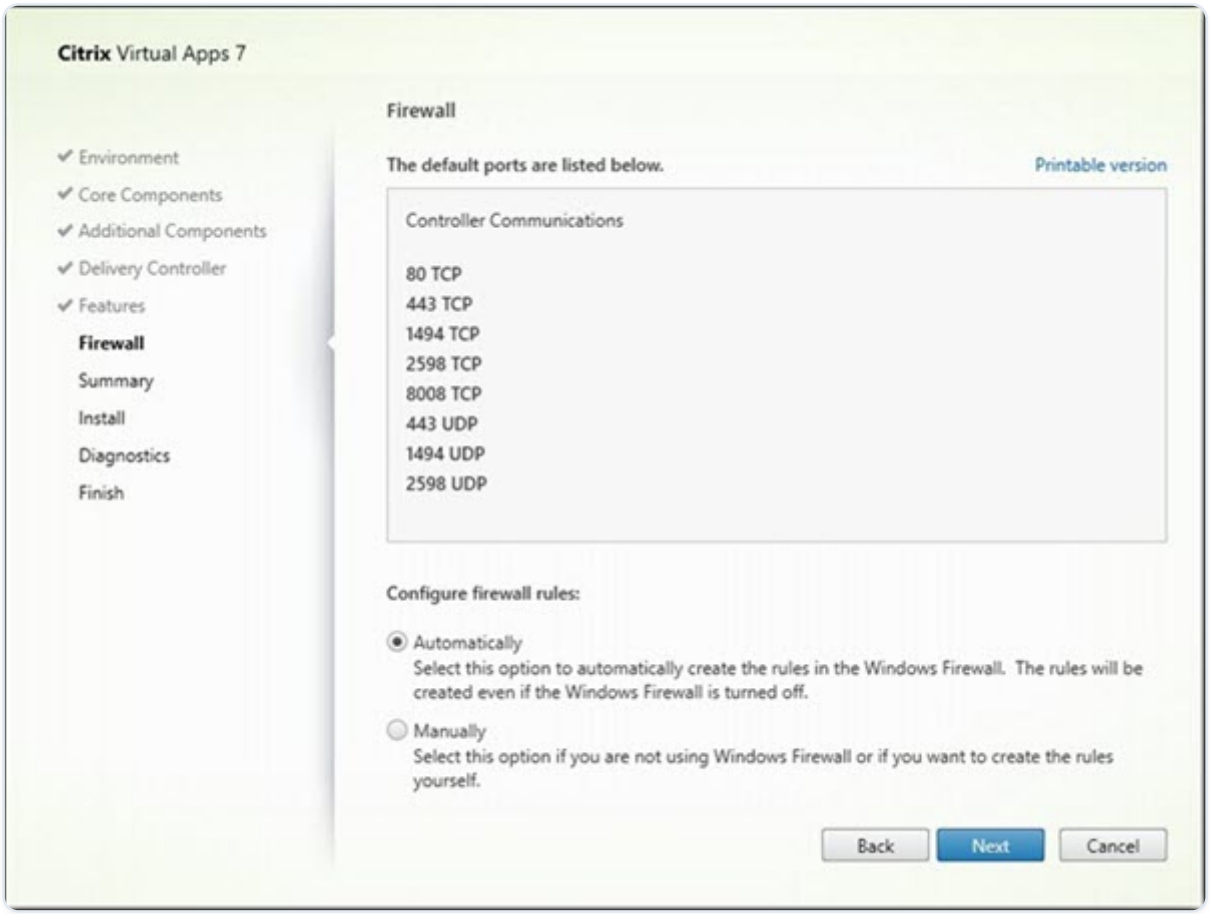
  Opção de linha de comando: `/xendesktopcloud`

- **Configurações Padrão Seguras:** Esta opção altera a configuração padrão de vários recursos de ativado para desativado para uma configuração mais segura pronta para uso. Os recursos relevantes são: redirecionamento de unidade cliente, redirecionamento de pasta especial, arrastar e soltar, redirecionamento de dispositivo TWAIN cliente, redirecionamento de dispositivo USB Plug and Play cliente, redirecionamento de impressora cliente, redirecionamento de área de transferência cliente e redirecionamento de microfone cliente.

Opção de linha de comando: `/ENABLE_SECURE_DEFAULTS`

Clique em **Avançar**.

Etapa 10. Portas do firewall



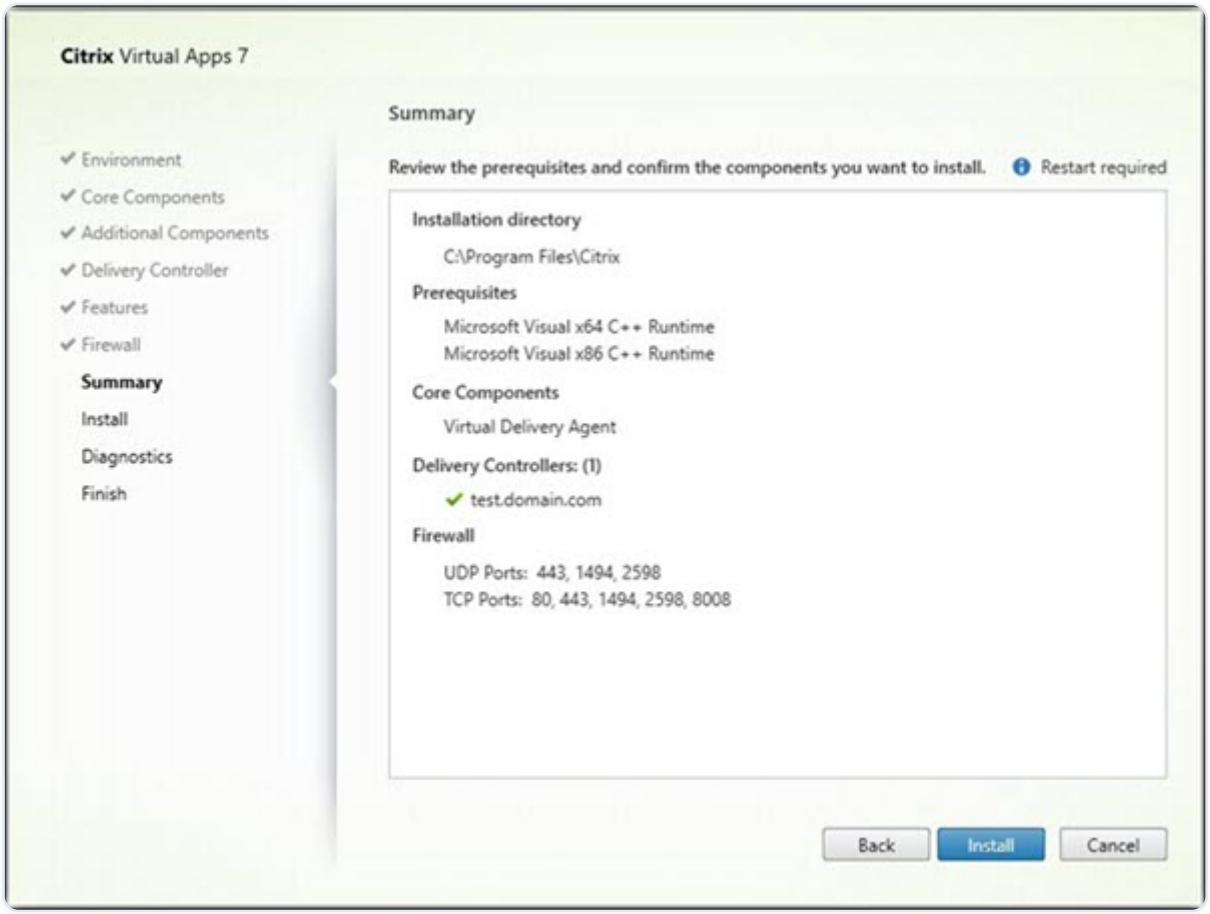
Na página **Firewall**, por padrão, as portas são abertas automaticamente se o Serviço de Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Esta configuração

padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Portas de rede.

Clique em **Avançar**.

Opção de linha de comando: `/enable_hdx_ports`

Etapa 11. Revise os pré-requisitos e confirme a instalação

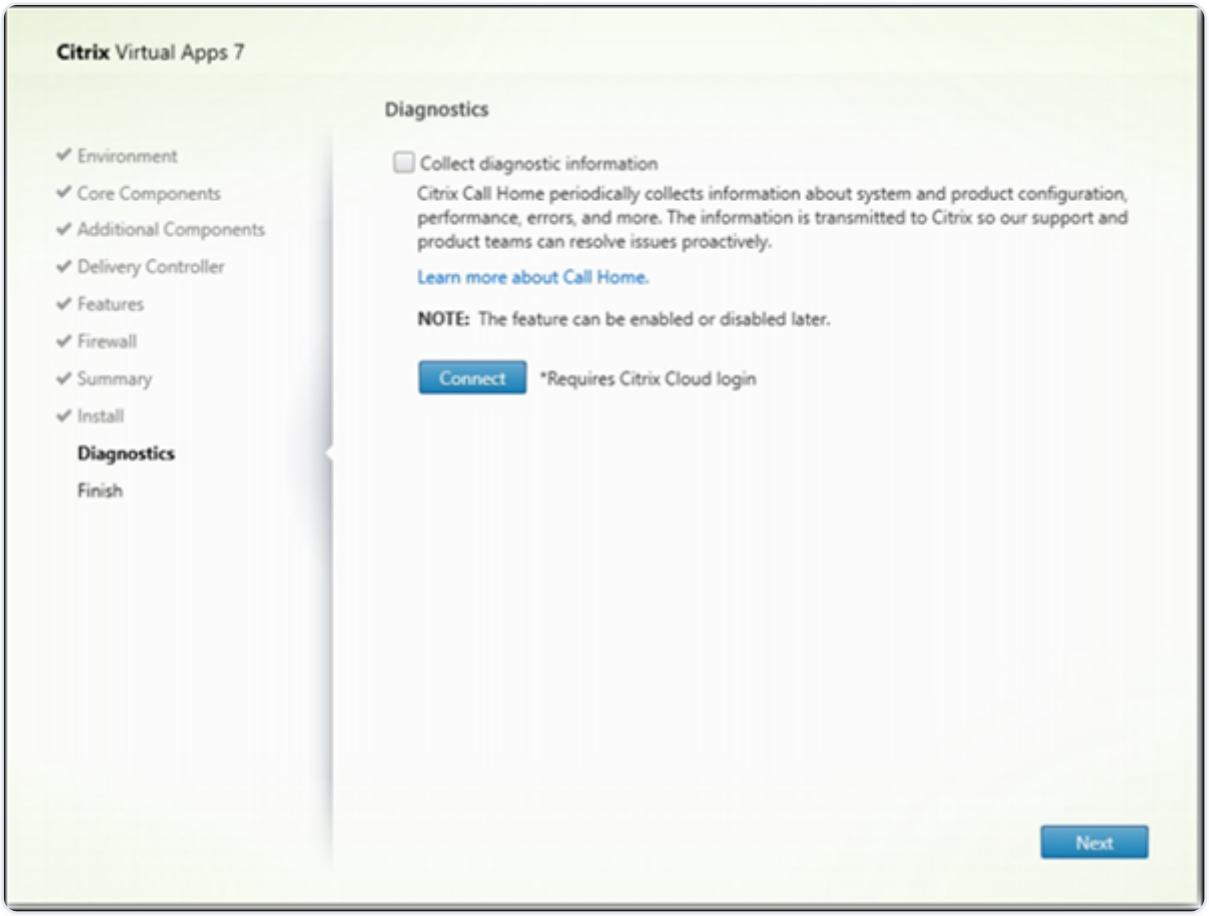


A página **Resumo** lista o que será instalado. Use o botão **Voltar** para retornar às páginas anteriores do assistente e alterar as seleções.

Quando estiver pronto, clique em **Instalar**.

Se os pré-requisitos ainda não estiverem instalados ou habilitados, a máquina pode reiniciar uma ou mais vezes. Consulte Preparar para instalar.

Etapa 12. Diagnóstico



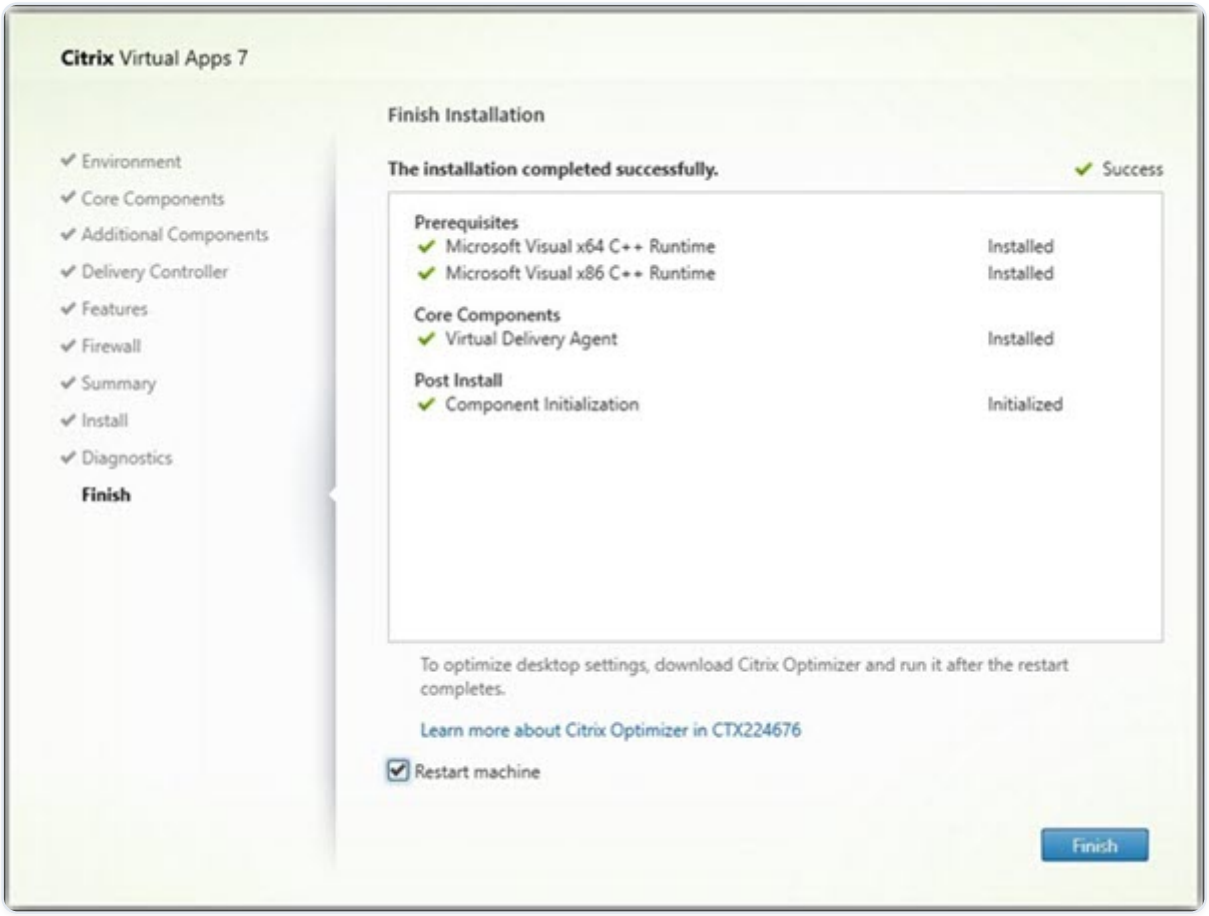
Na página **Diagnóstico**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), clique em **Conectar**. Quando solicitado, insira suas credenciais de conta Citrix.

Depois que suas credenciais forem validadas (ou se você optar por não participar), clique em **Avançar**.

Ao usar o instalador completo do produto, se você clicar em **Conectar** na página **Diagnóstico** sem primeiro selecionar **Coletar informações de diagnóstico**, depois de fechar a caixa de diálogo **Conectar aos Serviços Citrix Insight**, o botão **Avançar** é desabilitado. Você não pode ir para a próxima página. Para reabilitar o botão **Avançar**, selecione e desmarque imediatamente **Coletar informações de diagnóstico**.

Para obter mais informações, consulte Call Home.

Etapa 13. Concluir esta instalação



A página **Concluir** contém marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com sucesso.

Clique em **Concluir**. Por padrão, a máquina reinicia automaticamente. Embora você possa desabilitar esta reinicialização automática, o VDA não pode ser usado até que a máquina reinicie.

Próximas etapas

Repita o procedimento acima para instalar VDAs em outras máquinas ou imagens, se necessário.

Depois de instalar todos os VDAs, inicie o Studio. Se você ainda não criou um site, o Studio o guiará automaticamente para essa tarefa. Depois que isso for feito, o Studio o guiará para criar um catálogo de máquinas e, em seguida, um grupo de entrega. Consulte:

- Criar um site
- Criar catálogos de máquinas
- Criar grupos de entrega

Citrix Optimizer

O Citrix Optimizer é uma ferramenta para o sistema operacional Windows que ajuda os administradores Citrix a otimizar VDAs removendo e otimizando vários componentes.

Após instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Consulte CTX224676. O artigo CTX contém o pacote de download, além de instruções sobre como instalar e usar o Citrix Optimizer.

Personalizar um VDA

Para personalizar um VDA instalado:

1. No recurso do Windows para remover ou alterar programas, selecione **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Em seguida, clique com o botão direito e selecione **Alterar**.
2. Selecione **Personalizar Configurações do Virtual Delivery Agent**. Quando o instalador for iniciado, você poderá alterar:
   - Endereços do Controller
   - Porta TCP/IP para registrar com o Controller (padrão = 80)
   - Se deve abrir as portas do Firewall do Windows automaticamente

Solução de problemas

- Para obter informações sobre como a Citrix relata os resultados das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.
- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou um desktop aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Limitação conhecida

Ao usar o Citrix Workspace app para Windows versão 1912 ou anterior, a sessão é encerrada após um tempo. Esse problema foi corrigido nas versões LTSR e CR mais recentes do Citrix Workspace app. Para obter mais informações sobre as versões de lançamento suportadas,

consulte Citrix Workspace app para Windows / Citrix Receiver para Windows Long Term Service Releases.

Configurar o Controle de Acesso do Windows Defender relacionado à Instalação do VDA

Os clientes configuram as definições do Controle de Acesso do Windows Defender (WDAC) para proibir o carregamento de binários não assinados. Os binários não assinados distribuídos pelos instaladores do VDA são, portanto, proibidos, o que restringe a instalação do VDA.

A Citrix® agora assina todos os binários gerados pela Citrix com um certificado de assinatura de código da Citrix. Além disso, a Citrix também assina os binários de terceiros que são distribuídos com nosso produto com um certificado que autentica esses binários de terceiros como binários confiáveis.

Importante:

A atualização de um VDA mais antigo com binários de terceiros não assinados para uma versão mais recente do VDA com binários assinados pode nem sempre colocar os binários assinados na máquina atualizada. Isso se deve a um mecanismo dentro do sistema operacional onde a atualização do sistema não substitui binários com a mesma versão. Embora os binários de terceiros tenham sido assinados, suas versões, que são controladas por terceiros, não podem ser atualizadas pela Citrix, resultando na não atualização desses binários. Para evitar essa limitação:

1. Inclua os binários em uma lista de permissões. Isso elimina a necessidade de assinar os binários.
2. Desinstale o VDA mais antigo e instale o novo VDA. Isso se assemelha a uma instalação limpa do VDA e as versões assinadas serão instaladas.

Criar uma nova Política Base com o Assistente

O WDAC permite adicionar binários confiáveis para serem executados em seu sistema. Após a instalação do WDAC, o **Assistente de Política de Controle de Aplicativos do Windows Defender** é aberto automaticamente.

Para adicionar os binários, uma nova política base do WDAC deve ser criada. As diretrizes recomendadas pela Citrix para criar uma política base são fornecidas nesta seção.

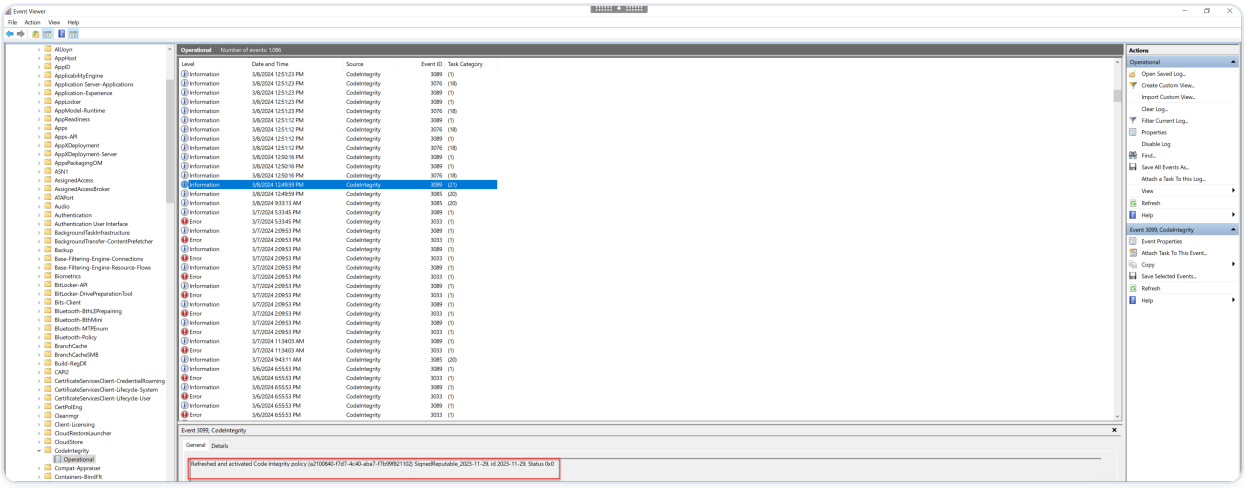
- Selecione o **Modo Assinado e Reputável** como o modelo base porque ele autoriza componentes operacionais do Windows, aplicativos instalados da Microsoft Store, todo o software assinado pela Microsoft e drivers de hardware de terceiros compatíveis com o Windows.
- **Habilite o Modo de Auditoria** porque ele permite testar novas políticas de Controle de Aplicativos do Windows Defender antes de aplicá-las.
- Adicione uma **Regra Personalizada** para **Regras de Arquivo** para especificar o nível no qual os aplicativos são identificados e confiáveis e forneça um arquivo de referência. Ao selecionar “Editor” como o tipo de regra, um arquivo de referência assinado por um dos certificados Citrix pode ser selecionado.
- Depois que as regras forem adicionadas, navegar para a pasta onde os arquivos `.XML` e `.CIP` estão salvos. O arquivo `.XML` contém todas as regras definidas na política. Ele pode ser configurado para alterar, adicionar ou remover quaisquer regras.
- Antes de implantar as políticas do WDAC, o arquivo `.XML` deve ser convertido para sua forma binária. O arquivo WDAC converte o arquivo `.XML` para o arquivo `.CIP`.
- Copie e cole o arquivo `.CIP` em: C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active e reinicie a máquina. A política gerada será aplicada no modo de auditoria.
- Para um processo passo a passo para criar uma política base, consulte Criando uma nova Política Base com o Assistente.

Quando esta política é aplicada, o WDAC não emite avisos sobre quaisquer arquivos Citrix que sejam assinados pela autoridade de editor/CA especificada.

Da mesma forma, podemos criar uma regra de nível de editor para os arquivos que foram assinados por terceiros.

Verificar a política aplicada

1. Após a reinicialização da máquina, abra o **Visualizador de Eventos** e vá para **Logs de Aplicativos e Serviços > Microsoft > Windows > CodeIntegrity > Operacional**.
2. Certifique-se de que a política aplicada esteja ativada.



3. Procure por logs que violaram a política e verifique as propriedades desse arquivo. Primeiro, confirme se ele foi assinado. Caso contrário, e se esta máquina passou por uma atualização de VDA, este é provavelmente o caso descrito na limitação acima. Se assinado, este arquivo está potencialmente assinado com o certificado alternativo, conforme descrito anteriormente.

Um exemplo de arquivo gerado pela Citrix assinado com um certificado Citrix é `C:\Windows\System32\drivers\picadm.sys`. Um exemplo de binário de terceiros assinado com o certificado de terceiros da Citrix é `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

Instalar VDAs usando scripts

> **Observação:**
>
> A Citrix não se responsabiliza por problemas causados por scripts adaptados para corresponder aos ambientes de produção do cliente. Para quaisquer problemas da Citrix relacionados à instalação, abra um caso de suporte técnico com os logs de instalação relevantes usando o portal de Suporte da Citrix.

> Este artigo se aplica à instalação de VDAs em máquinas com sistemas operacionais Windows. Para obter informações sobre VDAs para sistemas operacionais Linux, consulte a documentação do Linux Virtual Delivery Agent.

A mídia de instalação contém scripts de exemplo que instalam, atualizam ou removem Virtual Delivery Agents (VDAs) para máquinas no Active Directory. Você também pode usar os scripts para manter imagens mestre usadas pelo Machine Creation Services™ e Citrix Provisioning (anteriormente Provisioning Services).

Acesso necessário:

- Os scripts precisam de acesso de Leitura para Todos ao compartilhamento de rede onde o comando de instalação do VDA está localizado. O comando de instalação é `XenDesktopVdaSetup.exe` no ISO completo do produto, ou `VDAWorkstationSetup.exe` ou `VDAServerSetup.exe` em um instalador autônomo.
- Os detalhes de log são armazenados em cada máquina local. Para registrar os resultados centralmente para revisão e análise, os scripts precisam de acesso de Leitura e Gravação para Todos ao compartilhamento de rede apropriado.

Para verificar os resultados da execução de um script, examine o compartilhamento de log central. Os logs capturados incluem o log do script, o log do instalador e os logs de instalação do MSI. Cada tentativa de instalação ou remoção é registrada em uma pasta com carimbo de data/hora. O título da pasta indica o resultado da operação com o prefixo PASS ou FAIL. Você pode usar ferramentas de pesquisa de diretório padrão para encontrar uma instalação ou remoção com falha no compartilhamento de log central. Essas ferramentas oferecem uma alternativa à pesquisa local nas máquinas de destino.

Antes de iniciar qualquer instalação, leia e conclua as tarefas em Preparar para instalar.

Instalar ou atualizar VDAs usando o script

1. Obtenha o script de exemplo **InstallVDA.bat** de `\\Support\AdDeploy\` na mídia de instalação. A Citrix recomenda que você faça um backup do script original antes de personalizá-lo.
2. Edite o script:
   - Especifique a versão do VDA a ser instalada: `SET DESIREDVERSION`. O valor completo pode ser encontrado na mídia de instalação no arquivo ProductVersion.txt. No entanto, uma correspondência completa não é necessária.
   - Especifique o compartilhamento de rede onde o instalador será invocado. Aponte para a raiz do layout (o ponto mais alto da árvore). A versão apropriada do instalador (32 bits ou 64 bits) é chamada automaticamente quando o script é executado. Por exemplo: `SET DEPLOYSHARE=\\fileserver1\share1`.
   - Opcionalmente, especifique um local de compartilhamento de rede para armazenar logs centralizados. Por exemplo: `SET LOGSHARE=\\fileserver1\log1)`.

- Especifique as opções de configuração do VDA conforme descrito em Instalar usando a linha de comando. As opções `/quiet` e `/noreboot` são incluídas por padrão no script e são obrigatórias: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`.

3. Usando Scripts de Inicialização de Política de Grupo, atribua o script à OU que contém suas máquinas. Esta OU deve conter apenas máquinas nas quais você deseja instalar o VDA. Quando as máquinas nessa OU são reiniciadas, o script é executado em todas elas. Um VDA é instalado em cada máquina que possui um sistema operacional compatível.

Remover VDAs usando o script

1. Obtenha o script de exemplo UninstallVDA.bat de `\\Support\AdDeploy\` na mídia de instalação. A Citrix recomenda que você faça um backup do script original antes de personalizá-lo.
2. Edite o script.
   - Especifique a versão do VDA a ser removida: `SET CHECK\_VDA\_VERSION`. O valor completo pode ser encontrado na mídia de instalação no arquivo ProductVersion.txt (como 7.0.0.3018). No entanto, uma correspondência completa não é necessária.
   - Opcionalmente, especifique um local de compartilhamento de rede para armazenar logs centralizados.
3. Usando Scripts de Inicialização de Política de Grupo, atribua o script à OU que contém suas máquinas. Esta OU deve conter apenas máquinas das quais você deseja remover o VDA. Quando as máquinas na OU são reiniciadas, o script é executado em todas elas. O VDA é removido de cada máquina.

Solução de problemas

- O script gera arquivos de log internos que descrevem o progresso da execução do script. O script copia um log `Kickoff_VDA_Startup_Script` para o compartilhamento de log central em segundos após o início da implantação. Você pode verificar se o processo geral está funcionando. Se este log não for copiado para o compartilhamento de log central conforme o esperado, solucione o problema inspecionando a máquina local. O script coloca dois arquivos de log de depuração na pasta `%temp%` em cada máquina:
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Revise esses logs para garantir que o script esteja:

  - Executando conforme o esperado.
  - Detectando corretamente o sistema operacional de destino.
  - Corretamente configurado para apontar para o `ROOT` do compartilhamento `DEPLOYSHARE` (contém o arquivo chamado `AutoSelect.exe`).
  - Capaz de autenticar nos compartilhamentos `DEPLOYSHARE` e `LOG`.

- Para obter informações sobre como a Citrix relata o resultado das instalações de componentes, consulte Códigos de retorno de instalação da Citrix.
- Na exibição do Studio para um grupo de entrega, a entrada **Versão do VDA Instalada** no painel **Detalhes** pode não ser a versão instalada nas máquinas. A exibição de programas e recursos da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou um desktop aos usuários até que ele se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Métodos de implantação de VDA de terceiros

Para implantar com sucesso um Virtual Delivery Agent (VDA) usando o Microsoft System Center Configuration Manager (SCCM) ou ferramentas de distribuição de software semelhantes, como Ansible e Microsoft Intunes, a Citrix® recomenda usar o instalador do VDA em uma sequência de etapas.

> **Observação:**
>
> Os artigos a seguir descrevem apenas recomendações baseadas em como a Citrix testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

- Instalar VDAs usando SCCM
- Instalar VDAs usando Ansible
- Instalar VDAs usando Microsoft Intune

Instalar VDAs usando SCCM

Visão geral

O Microsoft Endpoint Configuration Manager, anteriormente System Center Configuration Manager (SCCM), é um produto Windows que permite o gerenciamento, implantação e segurança de dispositivos e aplicativos em uma empresa.

> **Observação:**
>
> O artigo a seguir descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

Recomendações

- Para implantar com sucesso um Virtual Delivery Agent (VDA) usando SCCM ou ferramentas de distribuição de software semelhantes, a Citrix recomenda usar o instalador do VDA em uma sequência de etapas.
- A Citrix não recomenda o uso do VDA Cleanup Utility como parte de uma instalação ou atualização do VDA. Use o VDA Cleanup Utility apenas no caso limitado em que o instalador do VDA falhou anteriormente.

Antes de começar

O número de reinicializações necessárias durante a instalação do VDA depende do ambiente. Por exemplo:

- Uma reinicialização pode ser necessária para atualizações pendentes ou reinicializações de instalações de software anteriores.
- Arquivos previamente bloqueados por outros processos podem precisar de atualizações, forçando uma reinicialização extra.
- Alguns componentes opcionais no instalador do VDA (como Citrix Profile Management e Citrix Files) podem exigir uma reinicialização.
- Ao atualizar um VDA, a máquina na qual ele está instalado deve estar em modo de manutenção, sem sessões.

- Quando uma instalação do VDA é executada pela primeira vez em uma máquina, o instalador do VDA que está sendo usado é copiado para essa máquina. Para obter mais informações sobre a instalação do VDA, consulte Instaladores.

O **SCCM Task Sequencer** gerencia todas as reinicializações necessárias.

Etapas principais para implantar VDA usando SCCM

As etapas a seguir descrevem como implantar o VDA usando SCCM na máquina virtual.

1. Instalar o VDA.
2. Criar uma unidade organizacional (OU).
3. Verificar as máquinas.
4. Usar o VDA para distribuir conteúdo.

ETAPA 1: INSTALAR O VDA

Após identificar todos os pré-requisitos, use o **SCCM Task Sequencer** para concluir as seguintes tarefas:

1. Instale o VDA a partir de uma cópia acessível da mídia de instalação ou de um dos instaladores autônomos do VDA:

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   Para obter mais informações sobre os instaladores do VDA, consulte Instaladores.

   > **Observação:**
   >
   > Ao atualizar um VDA, a máquina na qual ele está instalado deve estar no modo de manutenção, sem sessões.

2. Quando uma instalação do VDA é executada pela primeira vez em uma máquina, o instalador do VDA que está sendo usado é copiado para essa máquina.

   - Quando você usa um instalador do VDA diferente de `VDAWorkstationCoreSetup_XXXX.exe`, o instalador do VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.

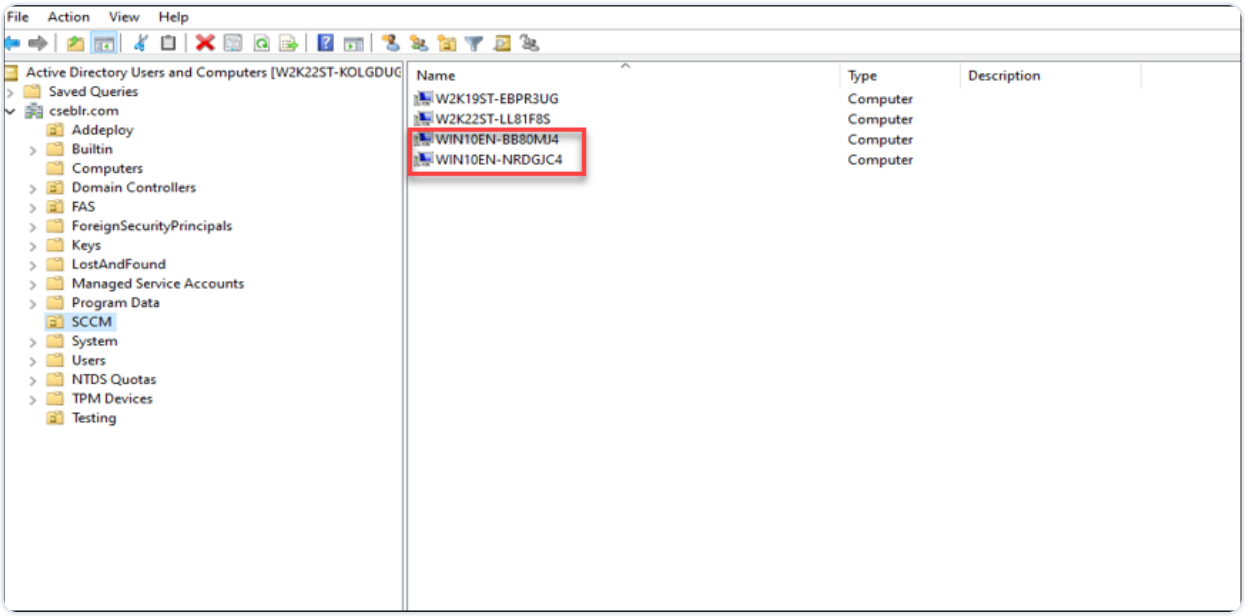
- Quando você usa `VDAWorkstationCoreSetup_XXXX.exe`, o instalador do VDA é copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`.

3. O local do diretório do instalador do VDA também é armazenado no registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall"` `"MetaInstallerInstallLocation"`.
4. Adicione as opções de linha de comando `/NOREBOOT`, `/NORESUME` e `/QUIET` às suas opções de linha de comando.

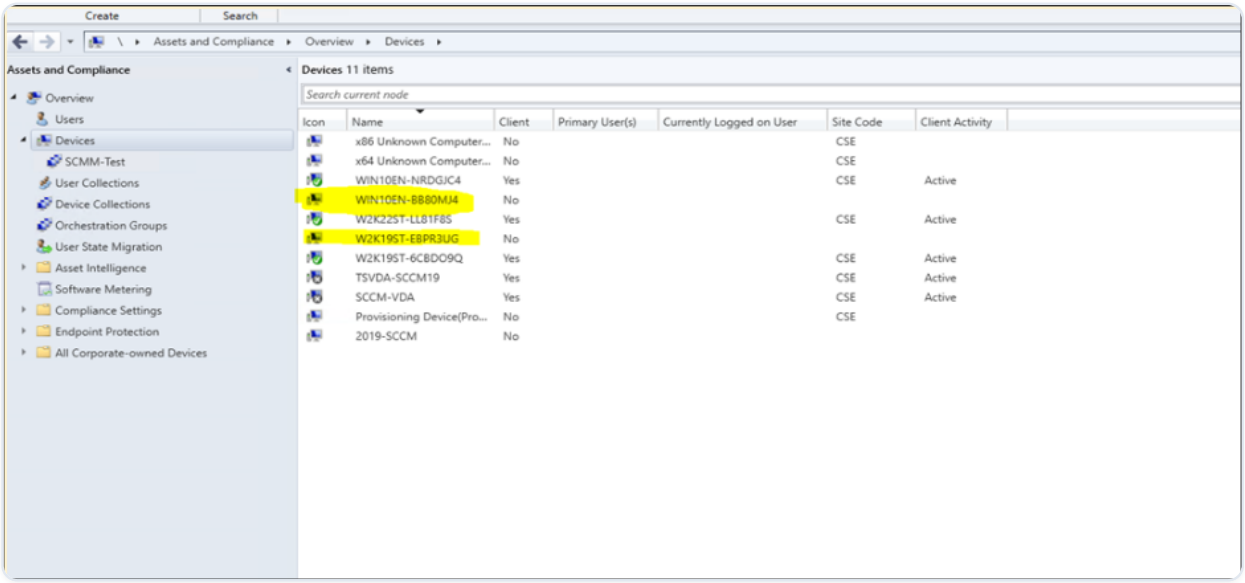
   - `/QUIET`: Não mostre a interface do usuário durante a instalação, para que o SCCM tenha controle do processo de instalação.
   - `/NOREBOOT`: Suprima o instalador do VDA de reiniciar automaticamente. O SCCM aciona reinicializações quando necessário.
   - `/NORESUME`: Geralmente, quando uma reinicialização é necessária durante a instalação, o instalador do VDA define uma chave de registro de execução única (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). O Windows usa a chave para abrir o instalador do VDA quando a máquina é reiniciada. Isso é um problema para o SCCM, porque o SCCM não consegue monitorar a instalação e capturar o código de saída.

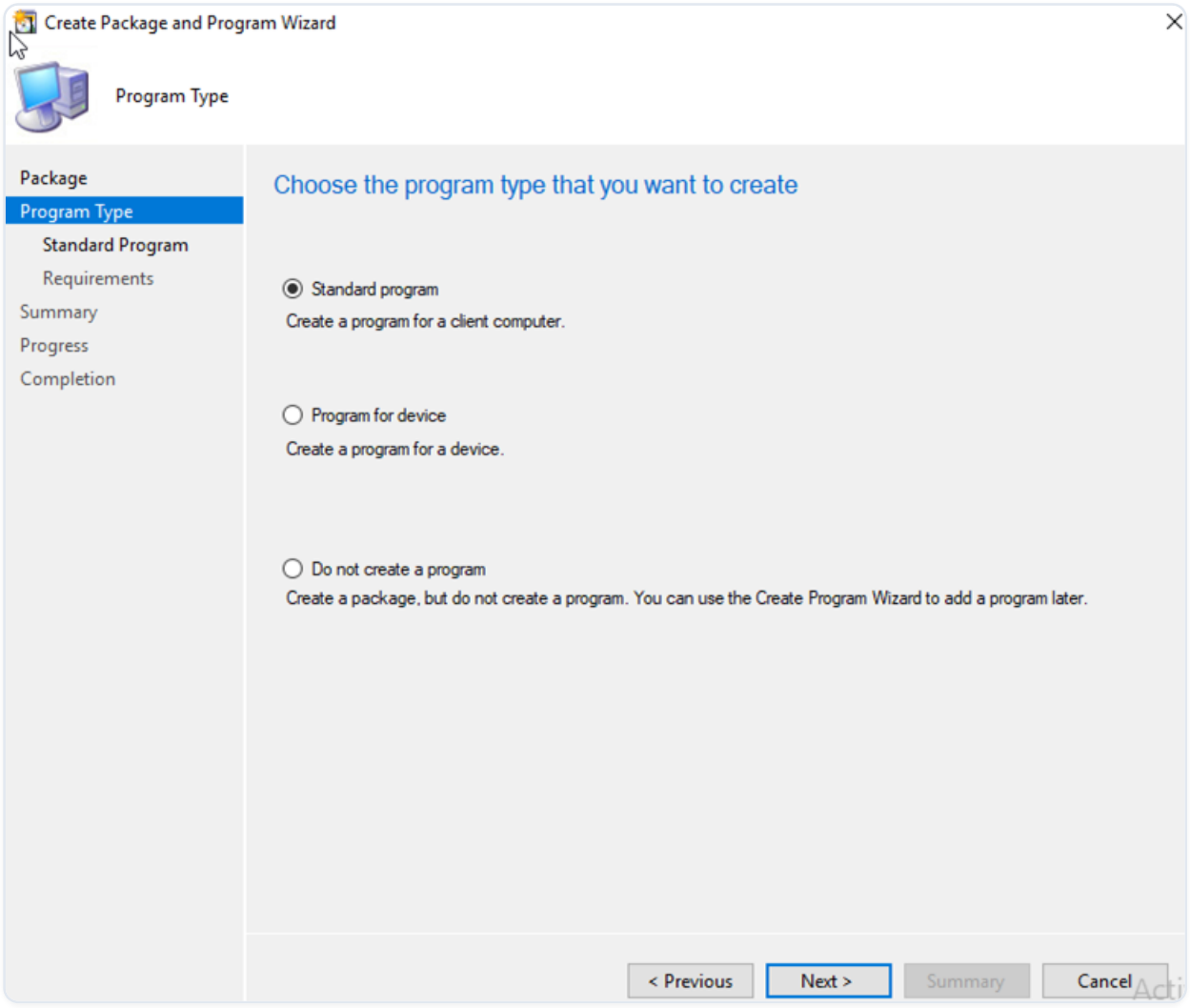
ETAPA 2: CRIAR UMA UNIDADE ORGANIZACIONAL (OU)

1. Crie duas máquinas virtuais ingressadas no domínio que você deseja adicionar à OU. Quando as máquinas virtuais são criadas inicialmente, elas estão na pasta **Computadores**. Mova as máquinas virtuais para a pasta **SCCM**. Exemplo: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

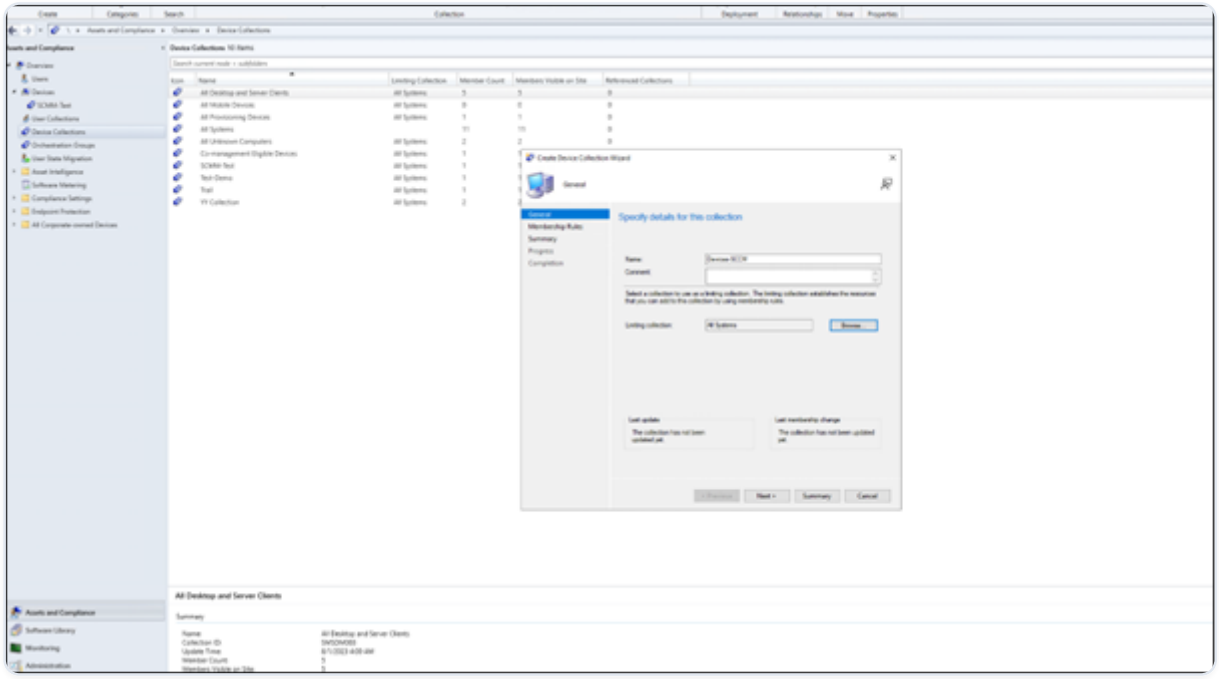


2. No Microsoft Configuration Manager, vá para `\Administration\Overview\Hierarchy Configuration\Discovery Methods\`.
3. Clique em **Active Directory System Discovery** e selecione a caixa de seleção **Enable Active Directory System Discovery** para habilitar a descoberta automática das máquinas virtuais recém-criadas.
4. Clique no ícone  para selecionar novos contêineres.
5. Na seção **Localização**, adicione o **Caminho** onde suas máquinas virtuais SCCM estão localizadas.
6. Vá para `\Administration\Overview\Site Configuration\Sites` e clique com o botão direito do mouse no SCCM VDA.
7. Selecione **Client Installation Settings > Client Push Installation**. A janela **Client Push Installation Properties** é aberta.
8. Assim que as VMs forem definidas como `Enabled`, você poderá ver a lista de VMs conforme ilustrado nas imagens a seguir.

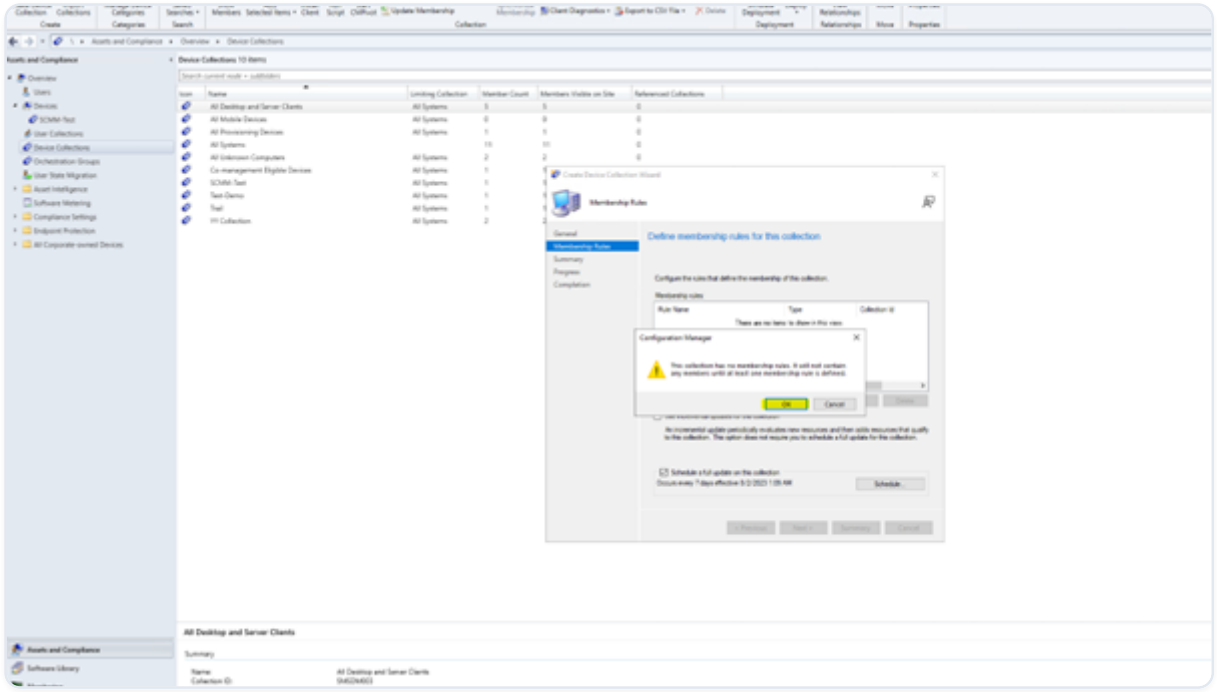




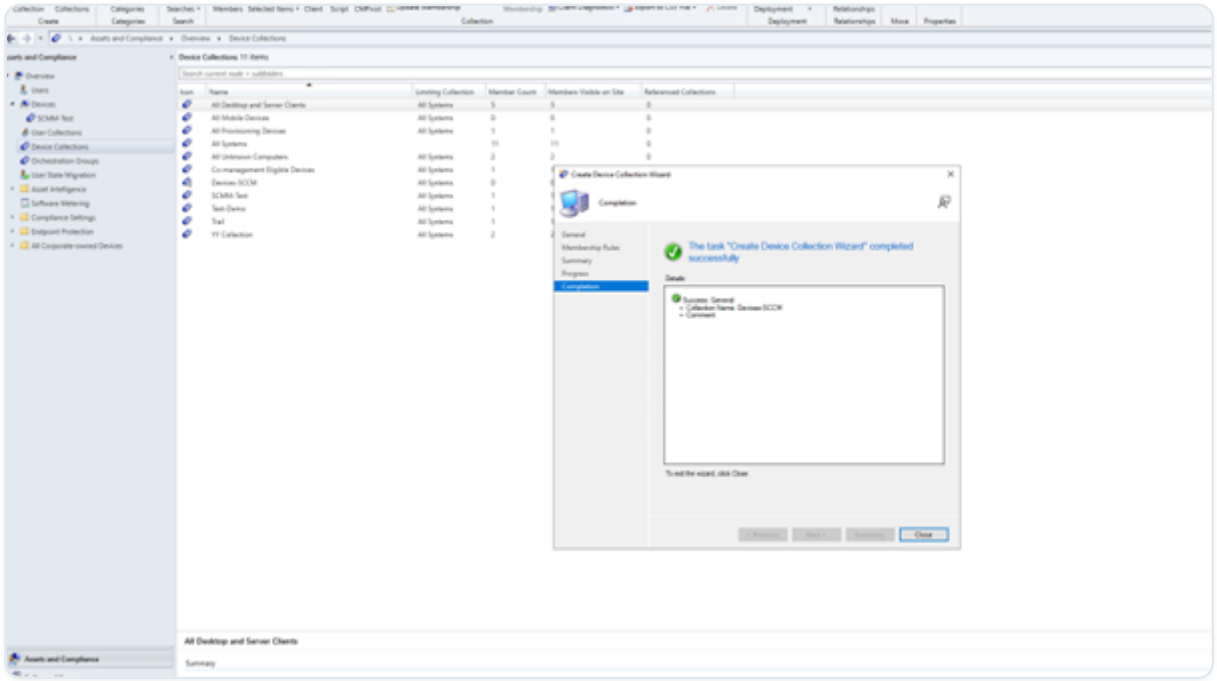
9. Crie uma **Coleção de dispositivos** para criar a OU. Insira o **Nome** da Coleção.



10. Siga as instruções do assistente.

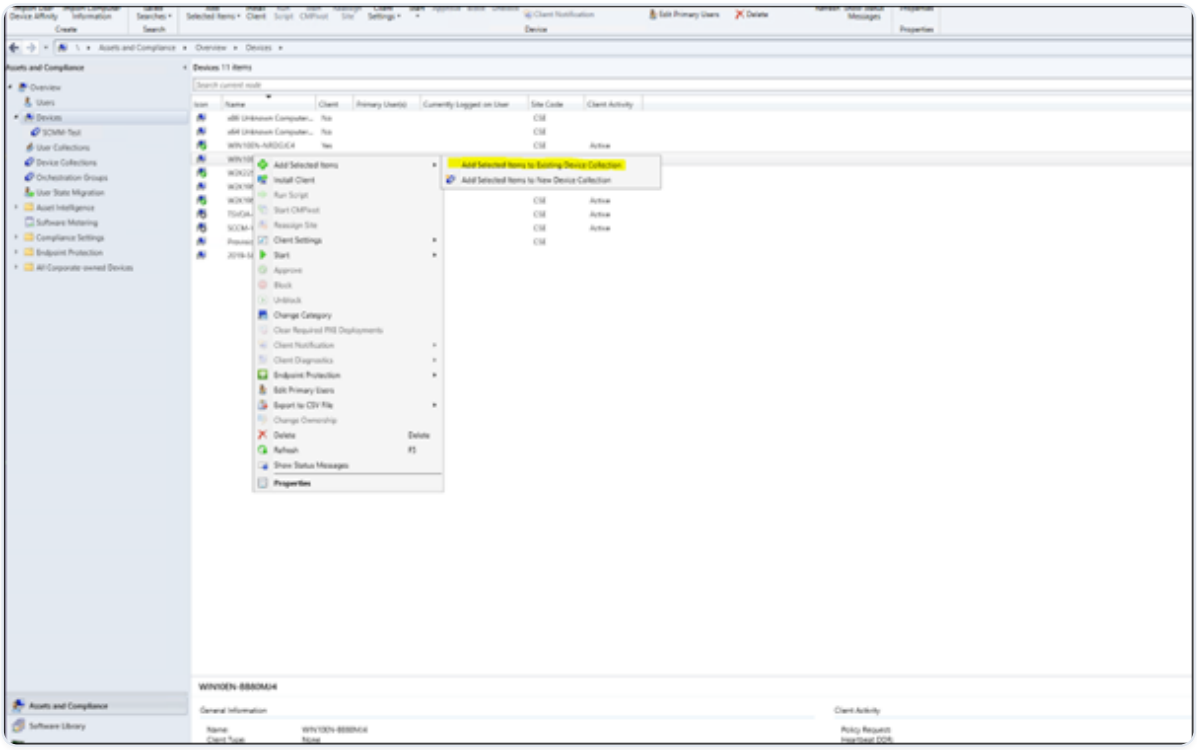


A OU é criada.

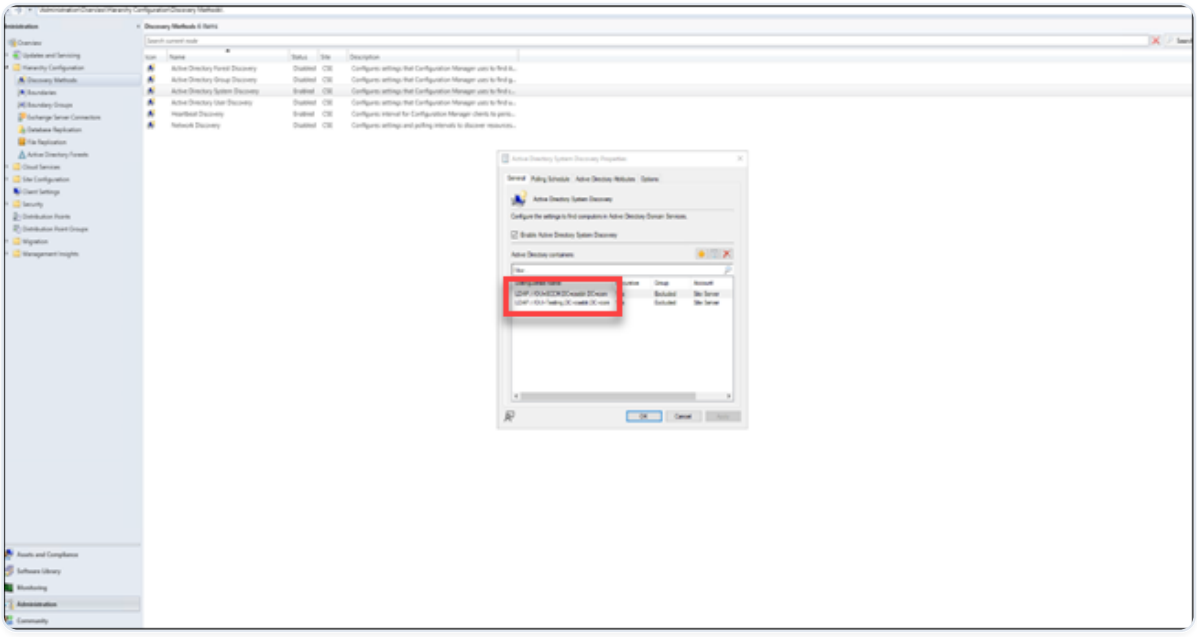


11. Adicione as VMs criadas à Coleção de Dispositivos recém-criada.

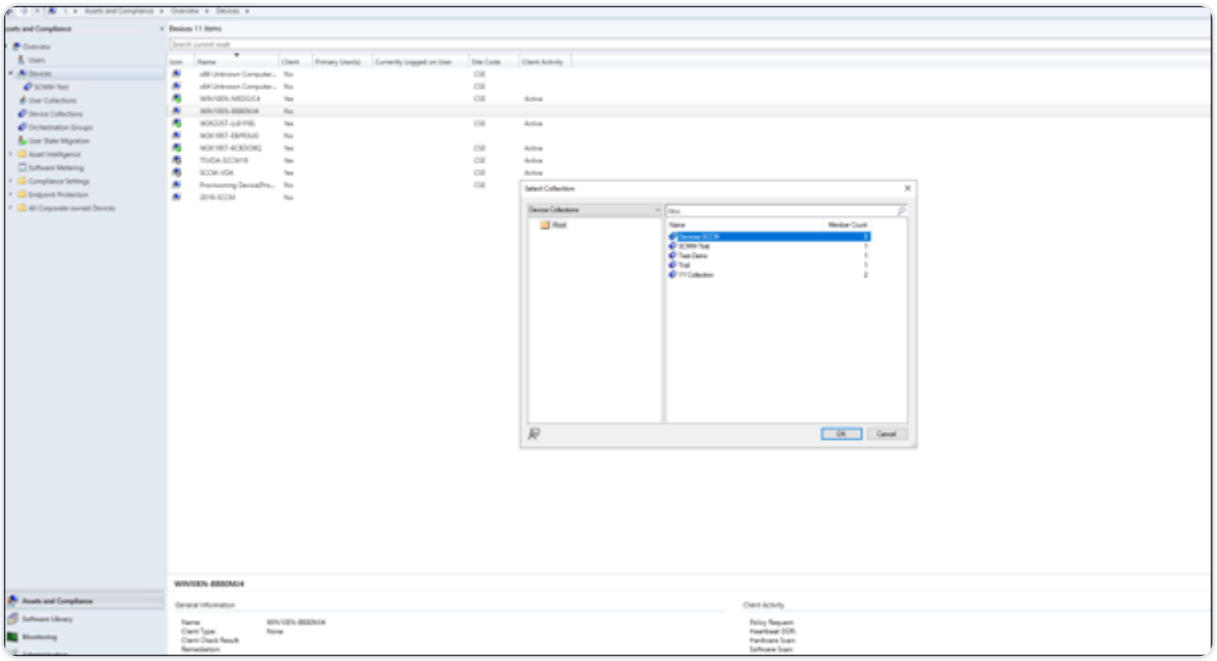
    a. Clique com o botão direito na VM. Selecione **Adicionar Itens Selecionados > Adicionar Itens Selecionados à Coleção de Dispositivos Existente**.



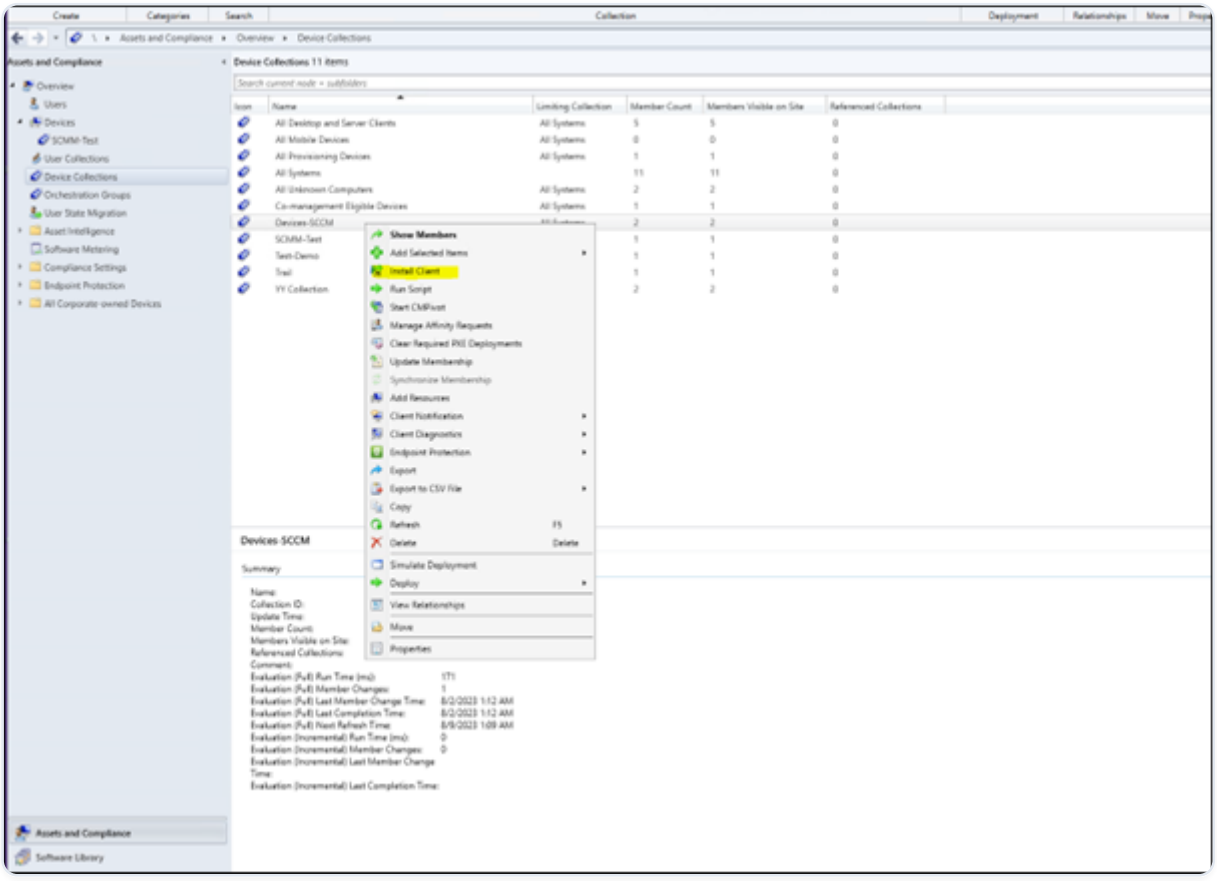
b. Na janela **Selecionar Coleção**, selecione o nome do dispositivo necessário. Neste exemplo, é `Devices-SCCM`.



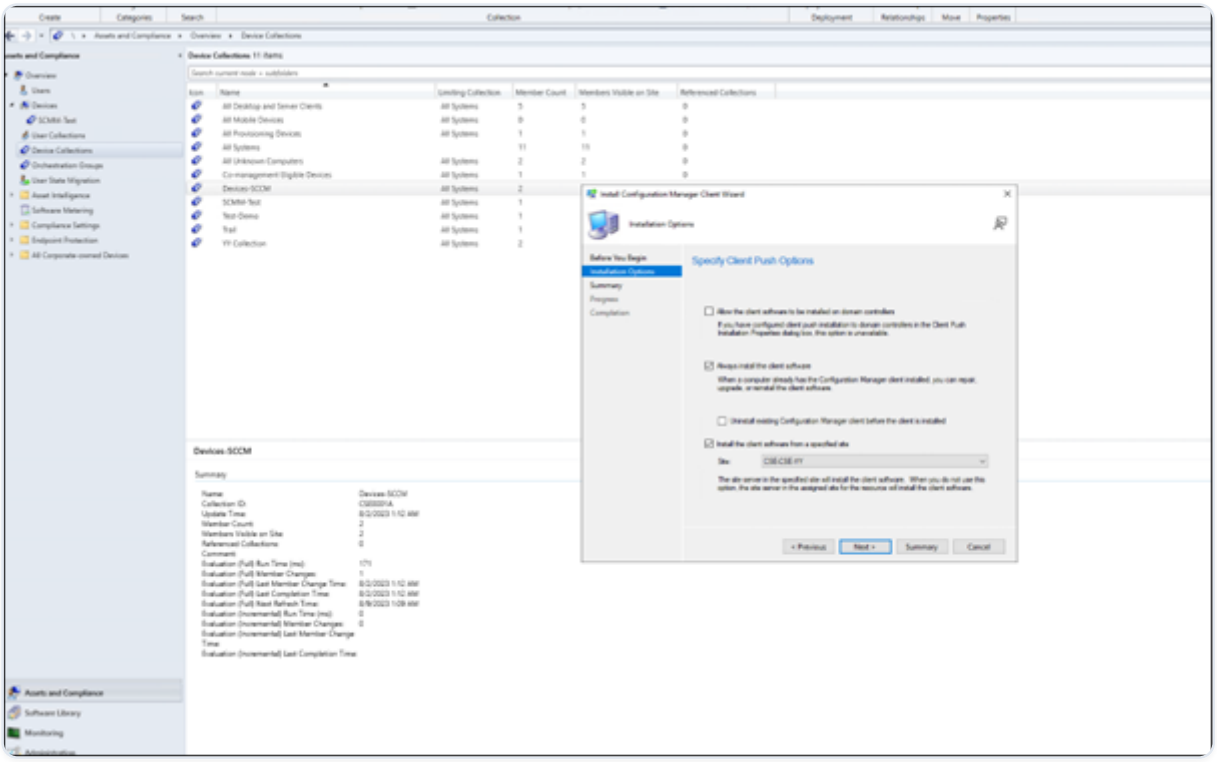
`Devices-SCCM` está listado em **Ativos e Conformidade > Visão Geral > Coleções de Dispositivos**.



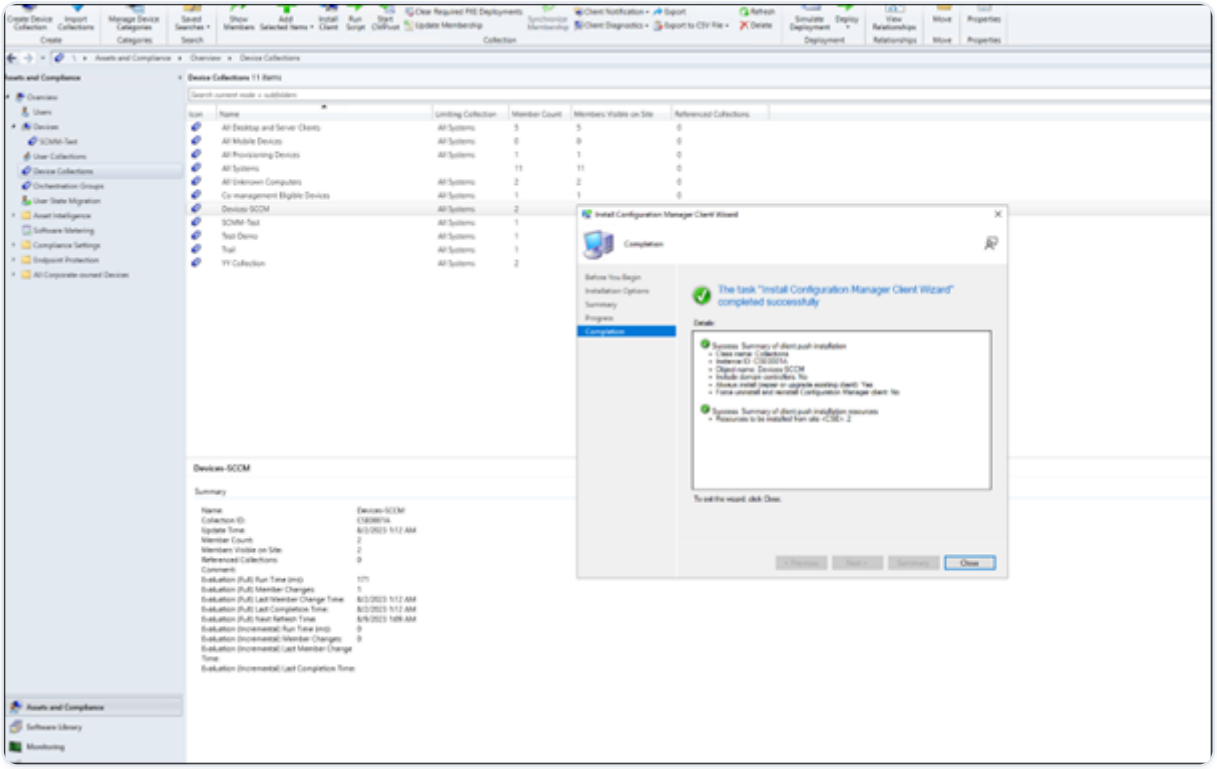
12. Selecione **Instalar Cliente** no Coletor de Dispositivos.



13. Selecione o **Site** de instalação necessário.



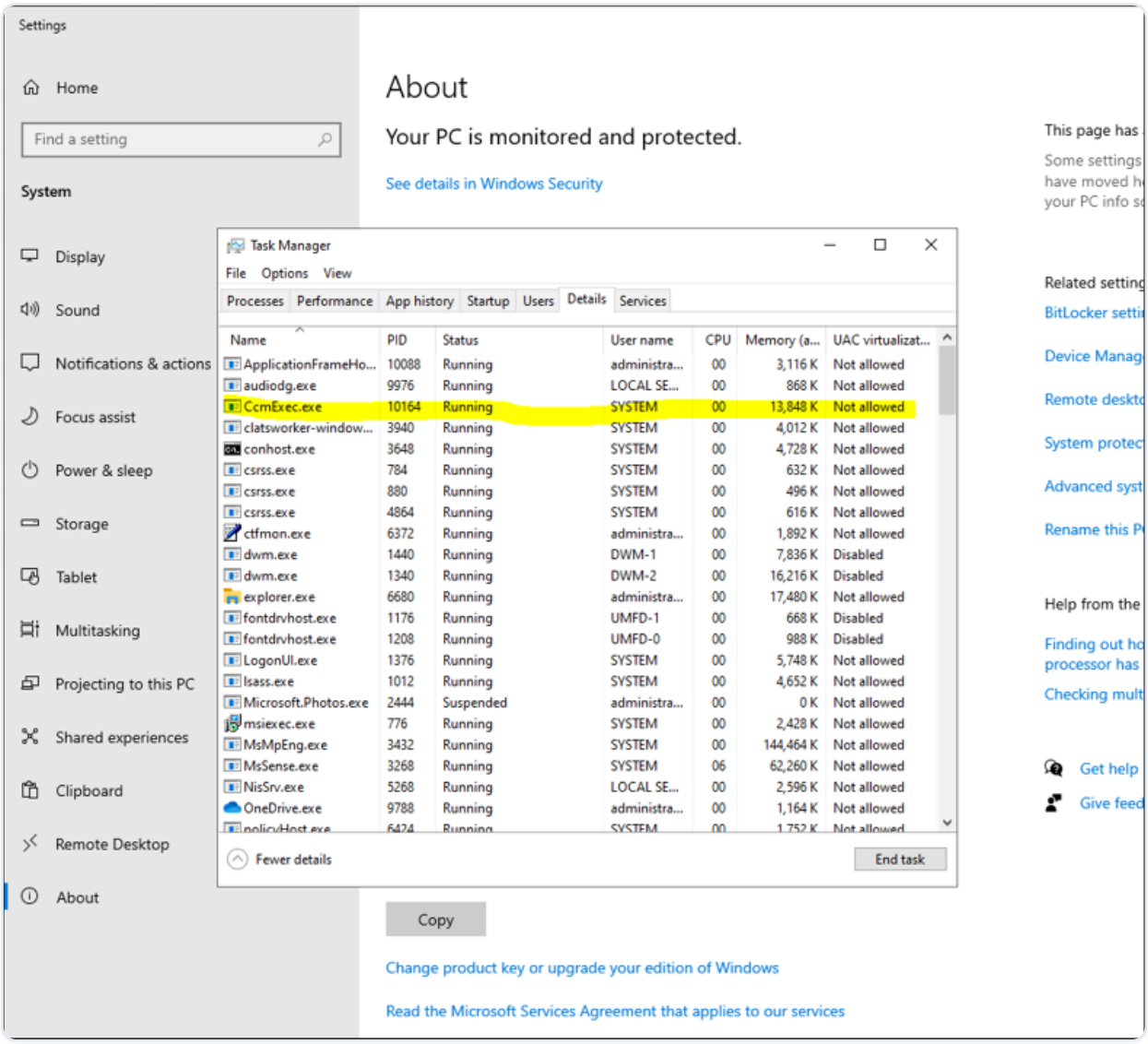
14. Siga as instruções do assistente. O **Assistente de Instalação do Cliente do Configuration Manager** foi concluído com êxito.



Para obter informações detalhadas, consulte Gerenciar coleções na documentação da Microsoft.

ETAPA 3: VERIFICAR AS MÁQUINAS

1. Na máquina cliente, verifique se o cliente está instalado, verificando se o processo `CCMExec` está em execução.



2. Verifique se o Cliente está em execução para as VMs no SCCM.

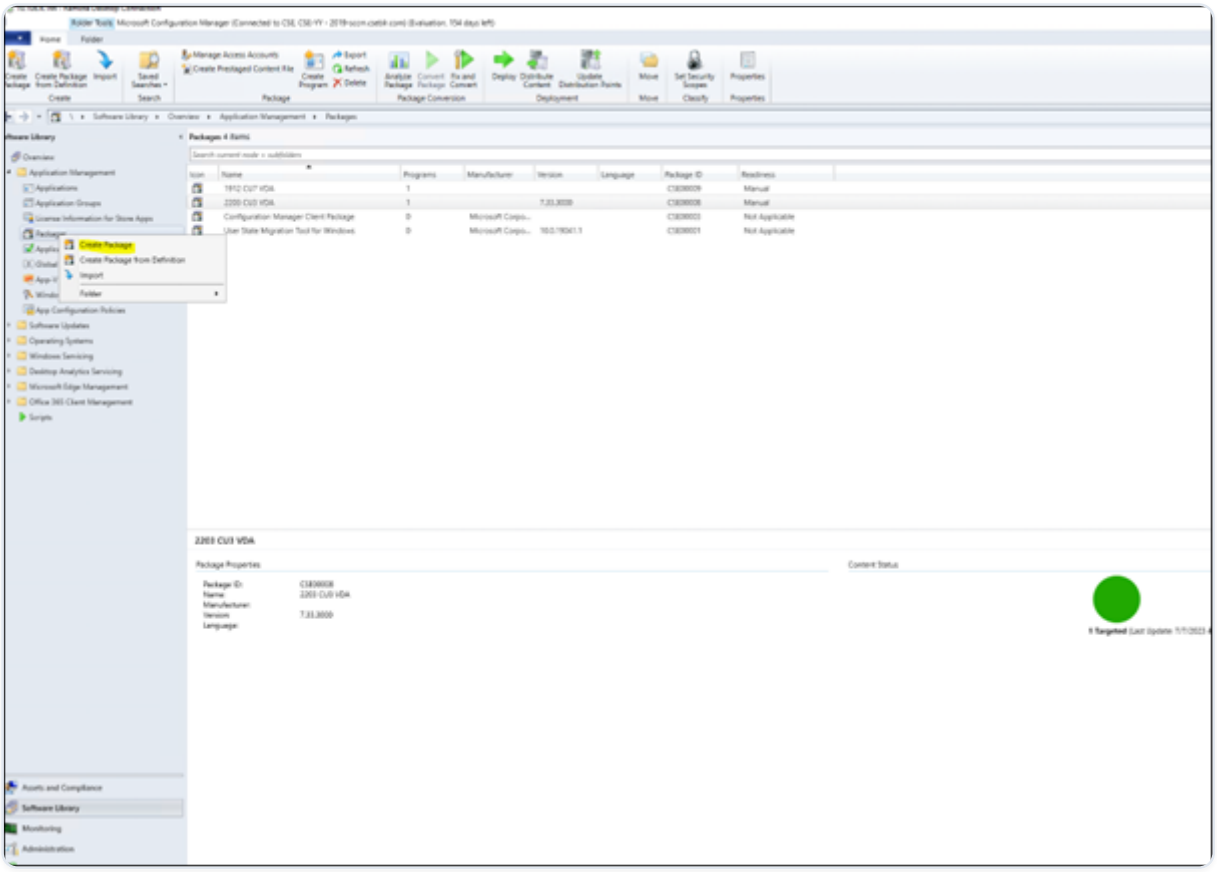
ETAPA 4: USAR O VDA PARA DISTRIBUIR CONTEÚDO

As etapas a seguir descrevem como você pode usar o VDA implantado para distribuir conteúdo nas máquinas virtuais associadas.

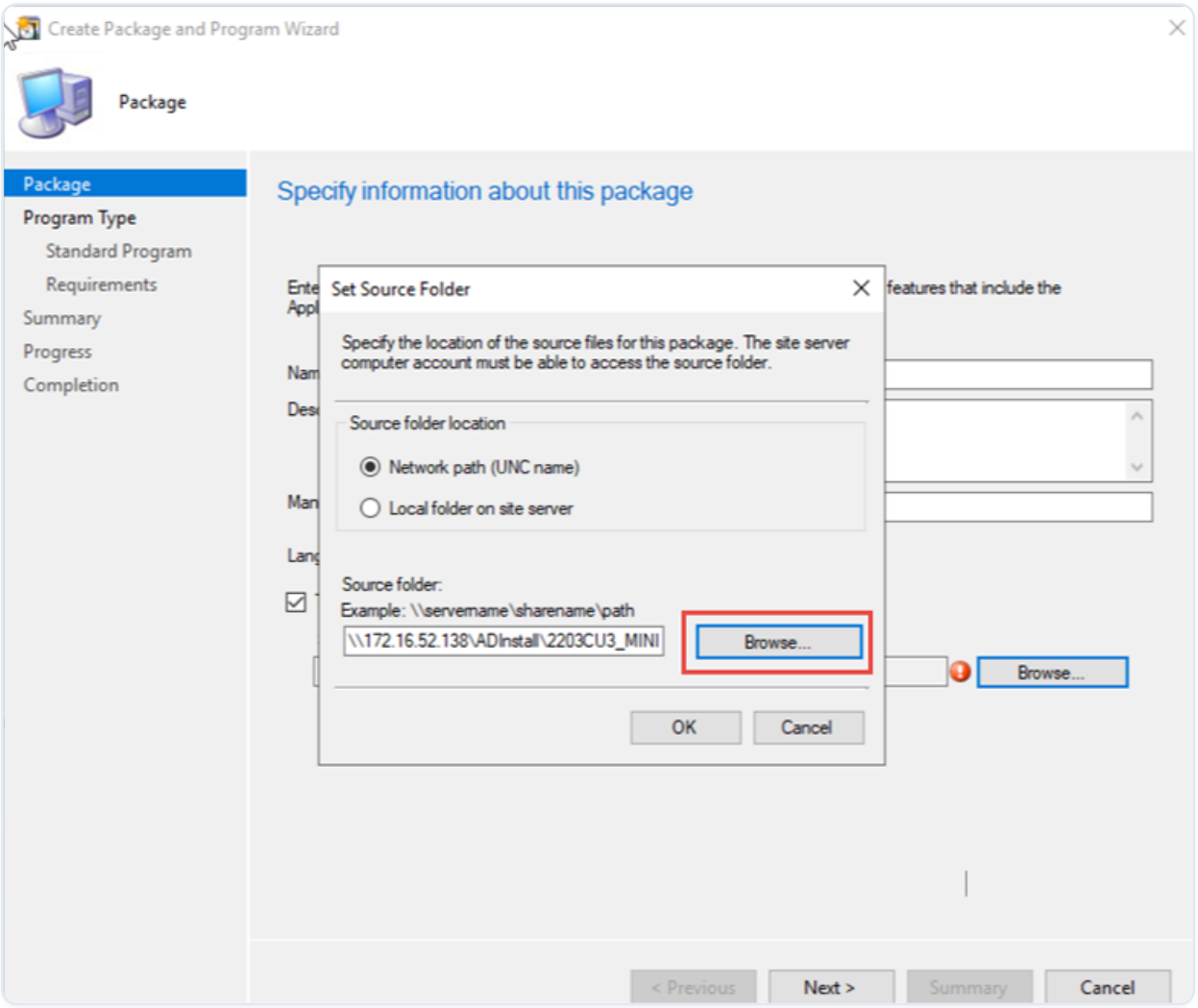
1. Criar um pacote
2. Distribuir conteúdo

Criar um pacote

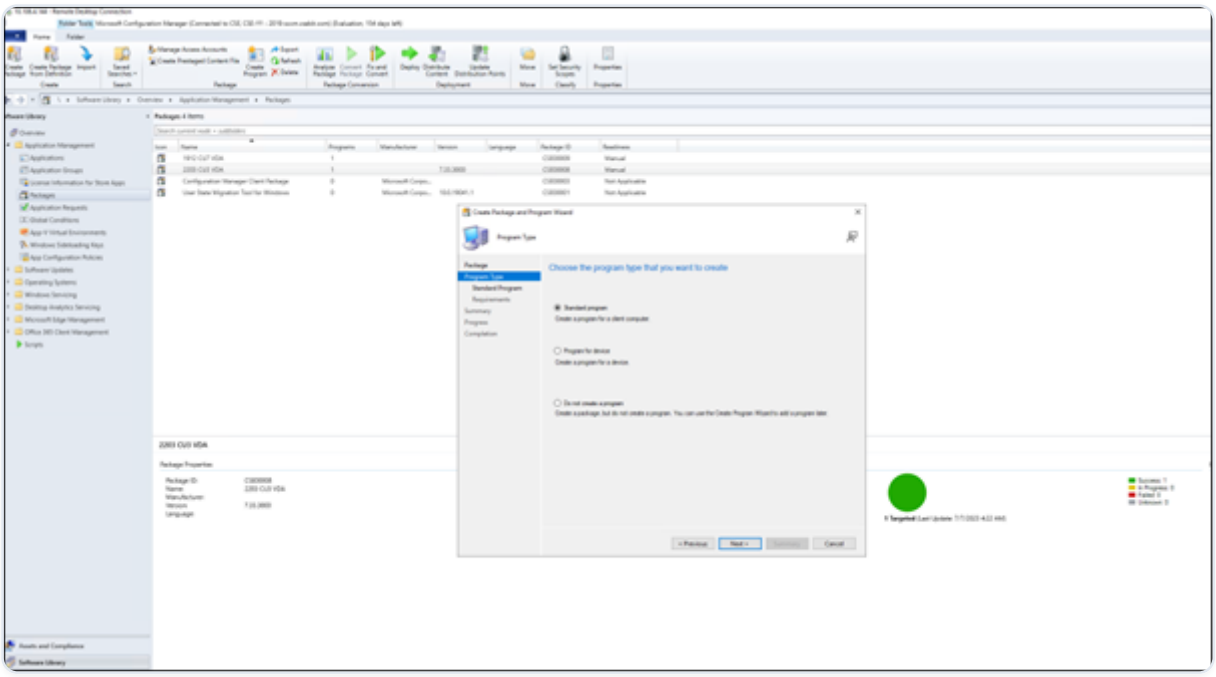
1. Para criar um pacote, clique com o botão direito do mouse no VDA desejado e clique em **Criar Pacote**.



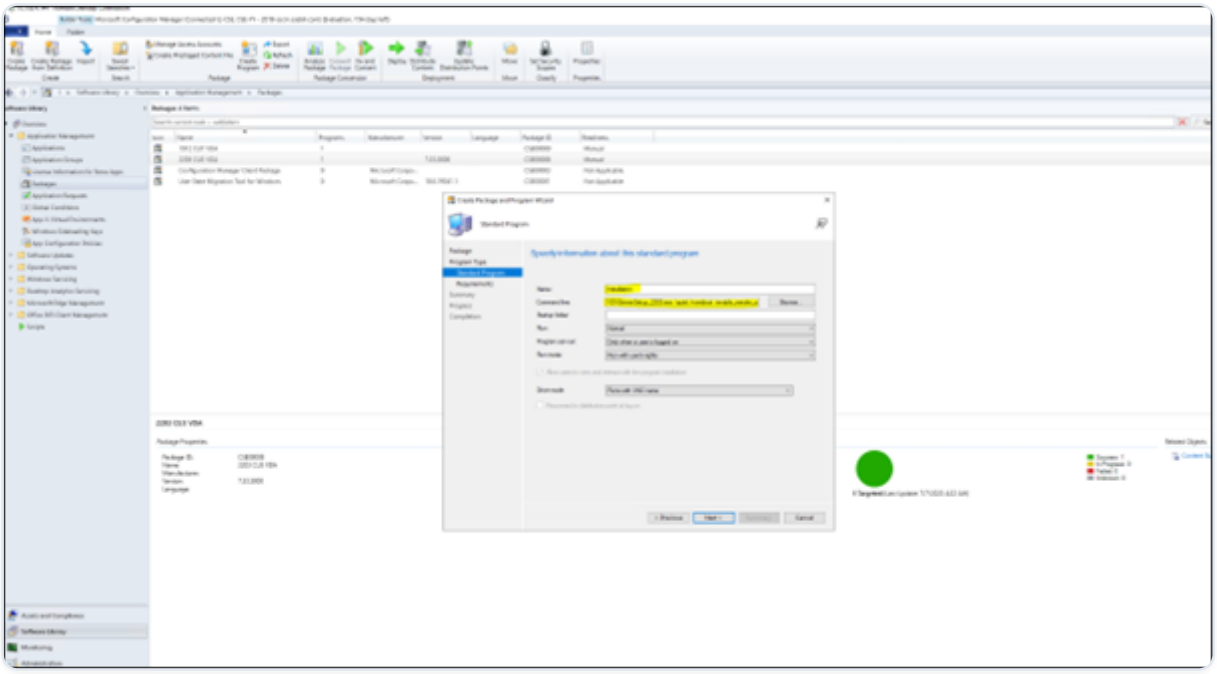
2. Especifique o local dos arquivos de origem para este pacote clicando em **Procurar**.



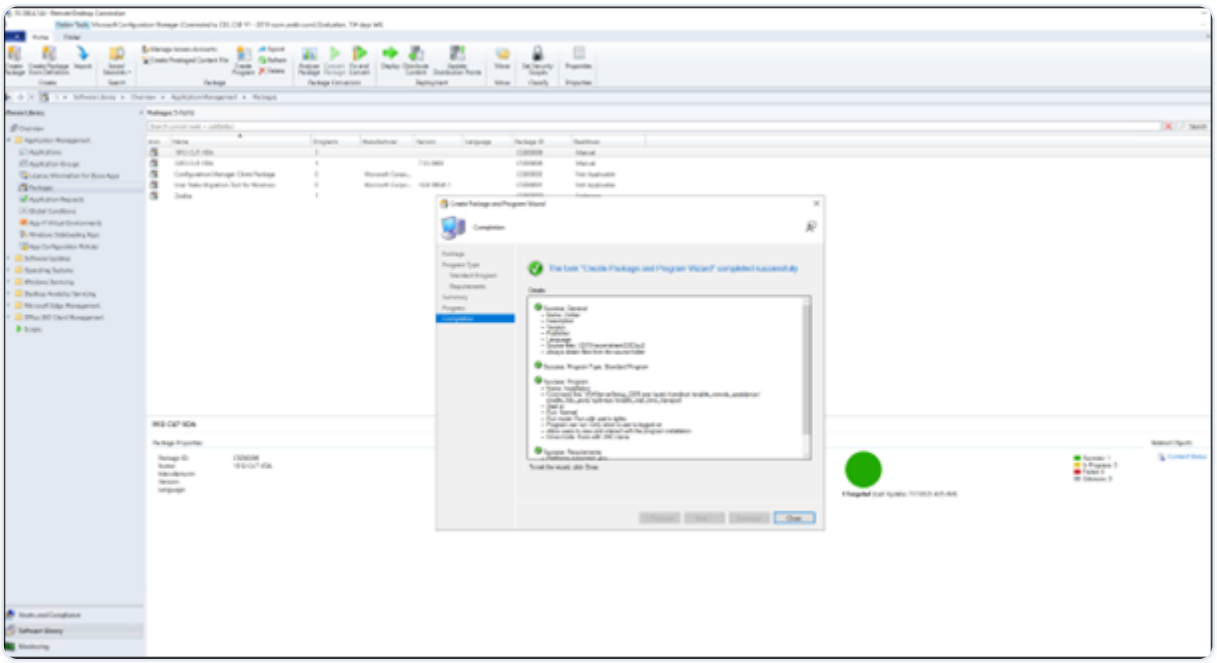
3. Selecione o tipo de pacote desejado.



4. Insira o **Nome** do pacote e a **Linha de comando**.



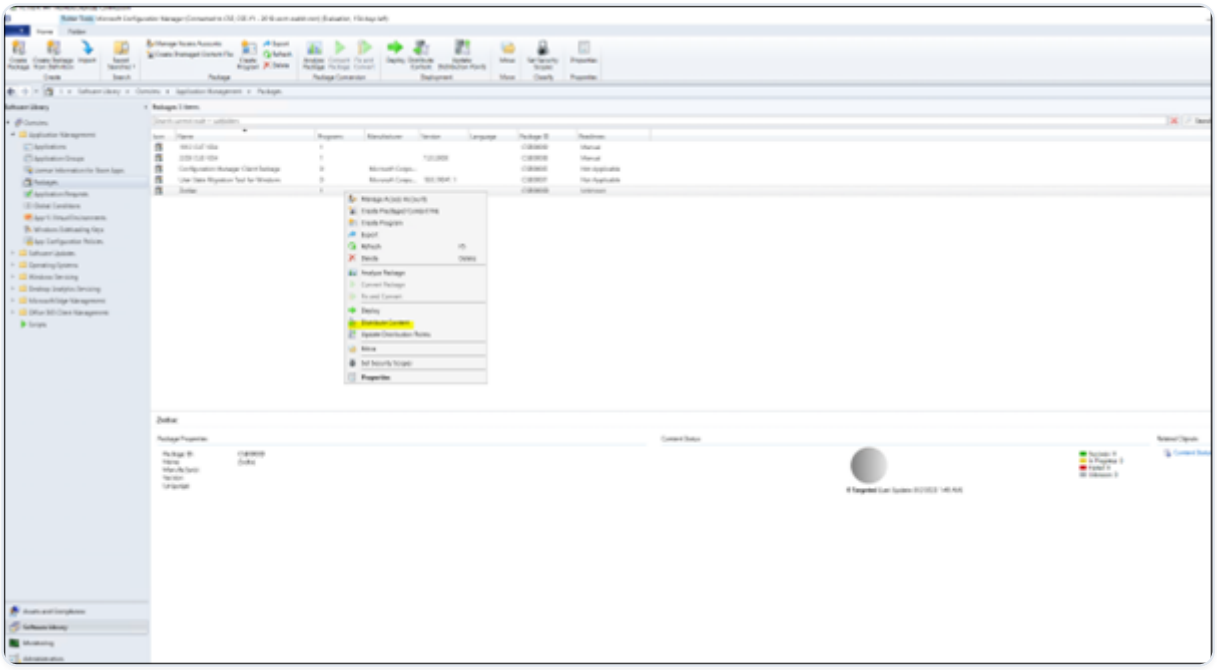
5. Clique em **Avançar**.



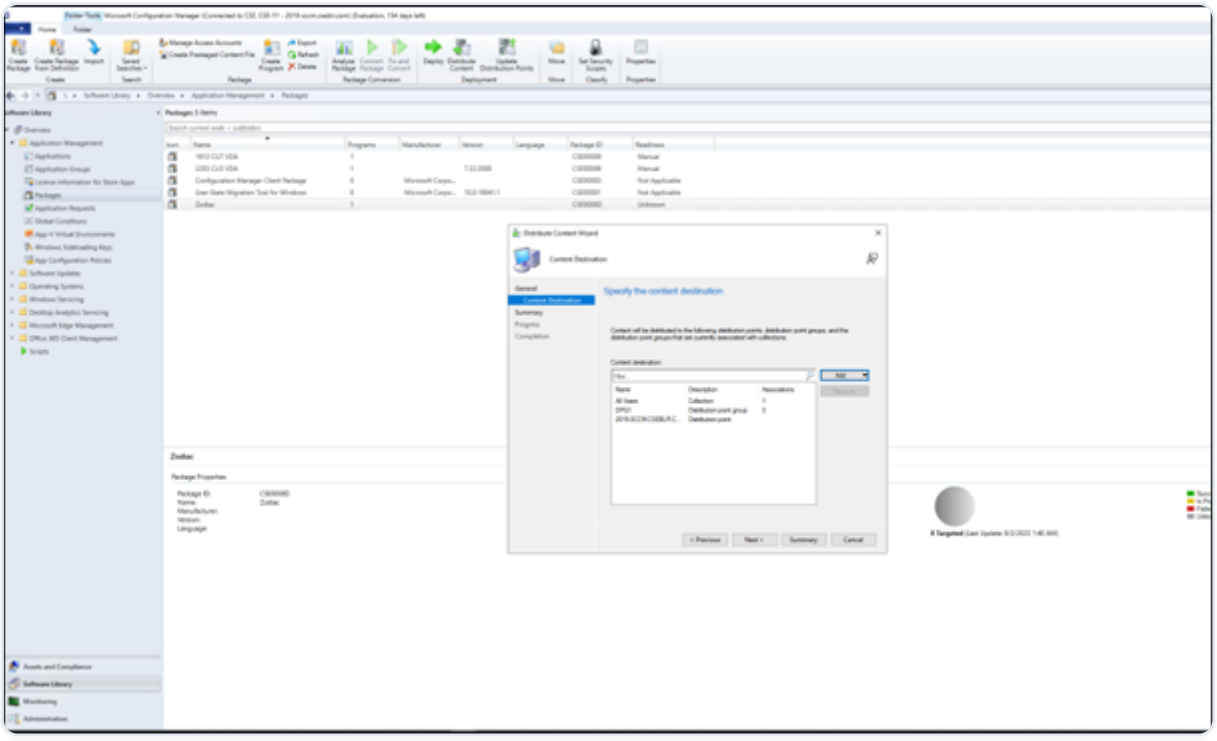
Para obter informações detalhadas, consulte Pacotes e programas no Configuration Manager na documentação da Microsoft.

Distribuir conteúdo

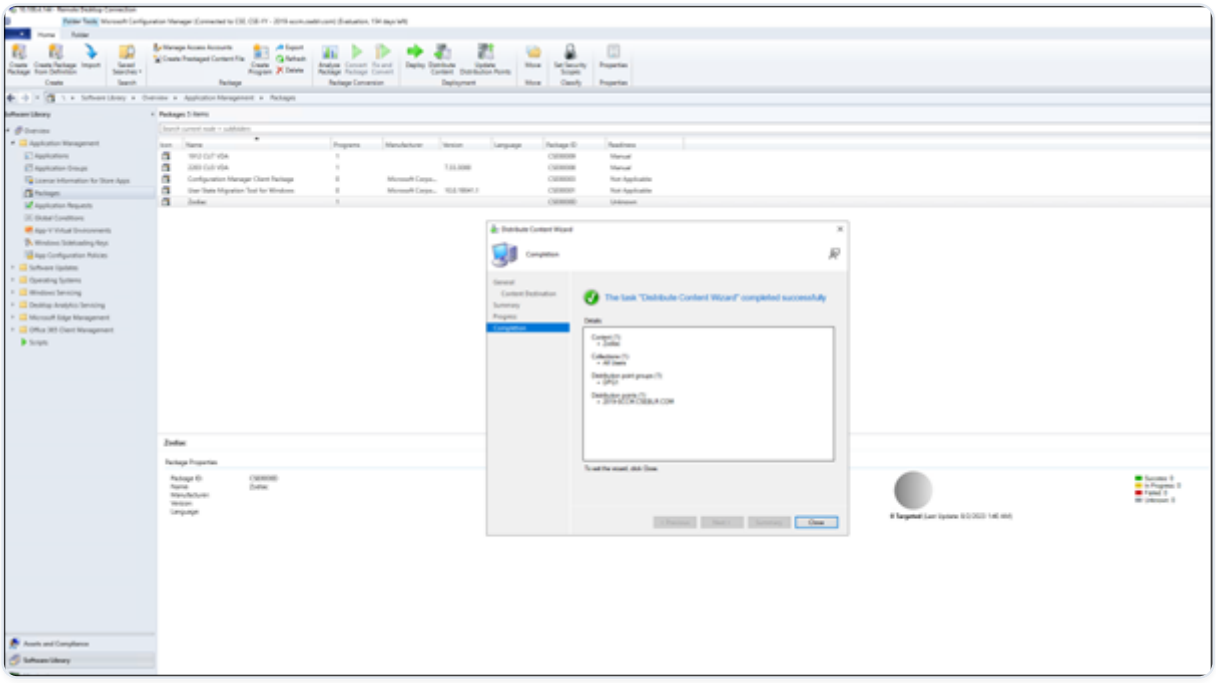
1. Clique com o botão direito do mouse no nome do pacote que você criou.
2. Selecione **Distribuir Conteúdo**.



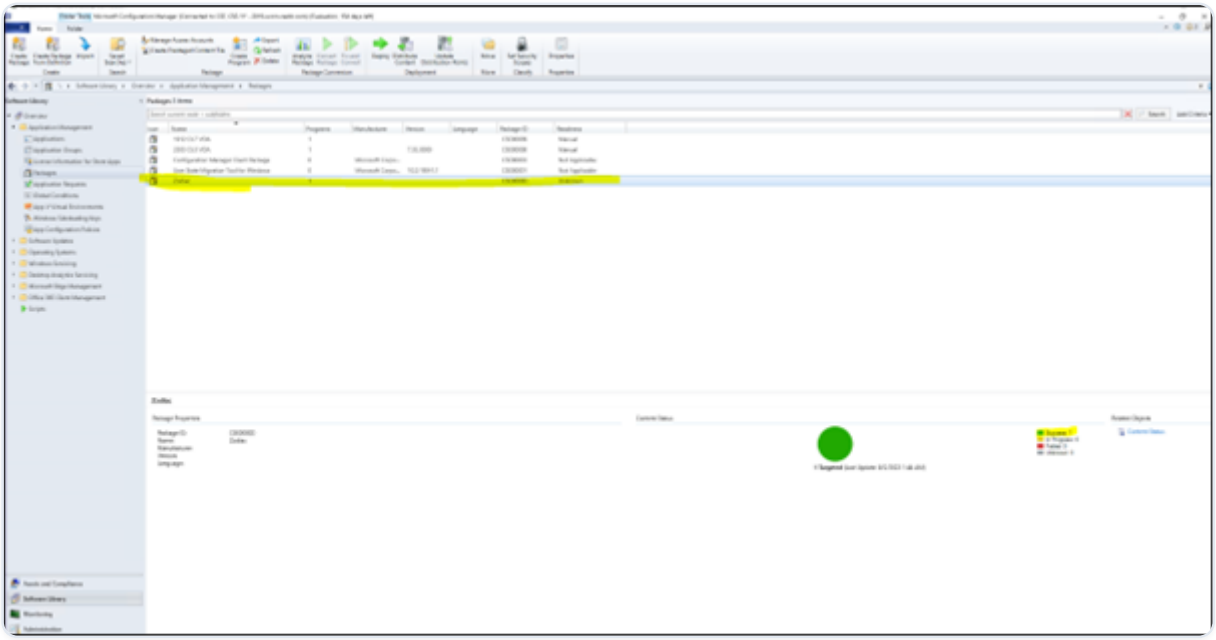
3. Na janela do **Assistente para Distribuir Conteúdo**, selecione o local dos arquivos de origem para o pacote que você criou. Neste exemplo, é `2019-SCCM`. Clique em **Avançar**.



4. Verifique se o Pacote (neste exemplo, `Zodiac`) está disponível para implantação.



A imagem a seguir ilustra que o pacote está disponível para implantação.

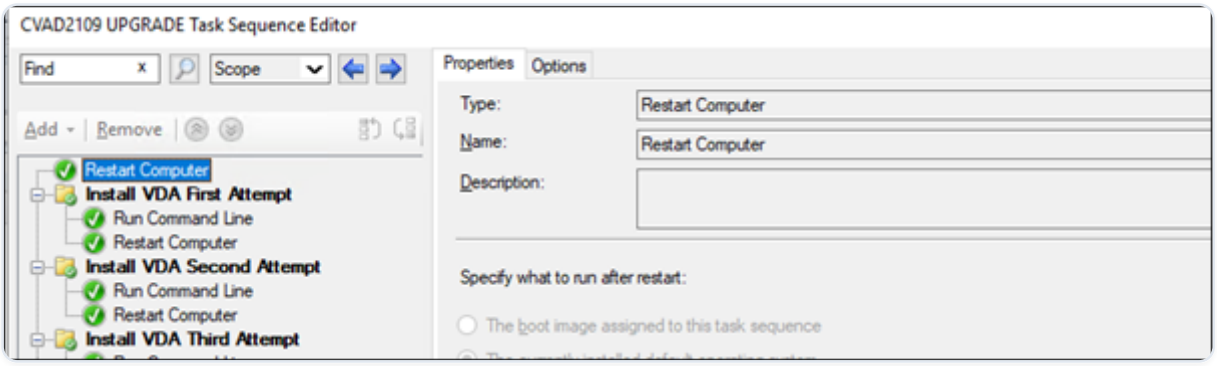


Para obter informações detalhadas, consulte Implantar e gerenciar conteúdo para o Configuration Manager na documentação da Microsoft.

Exemplo de sequência de instalação usando o SCCM

O exemplo a seguir mostra a sequência de instalação.

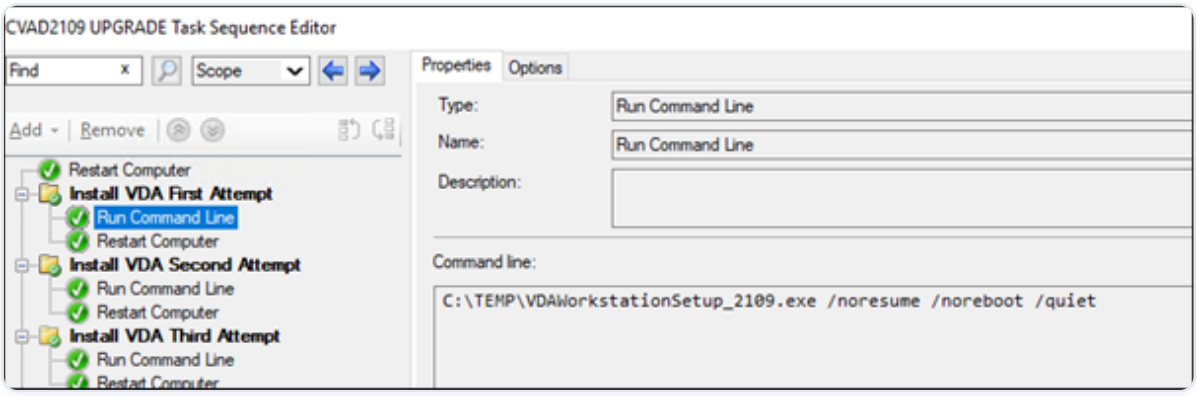
1. **Reiniciar Computador:** Prepare a máquina reiniciando-a.



2. **Instalar VDA Primeira Tentativa:** Inicie a instalação do VDA.

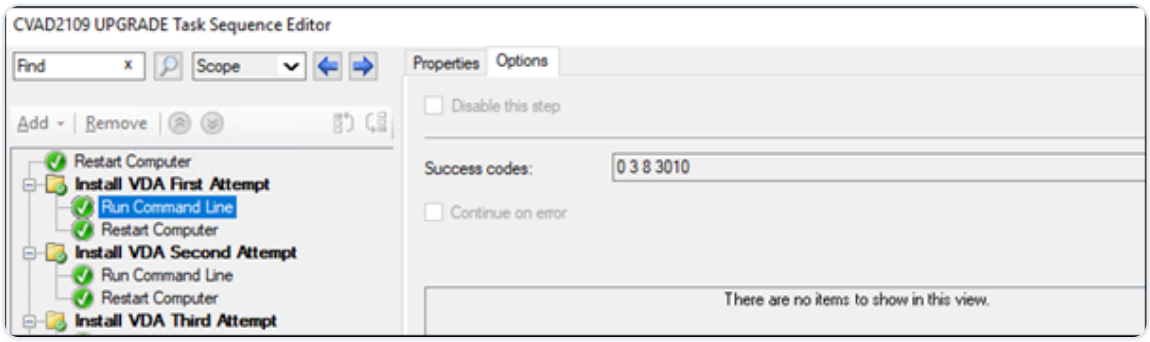
   a. Adicione as opções `/quiet`, `/noreboot` e `/noresume` às suas opções de linha de comando.

   b. Execute o instalador do VDA de sua escolha (imagem local ou um dos instaladores mínimos).

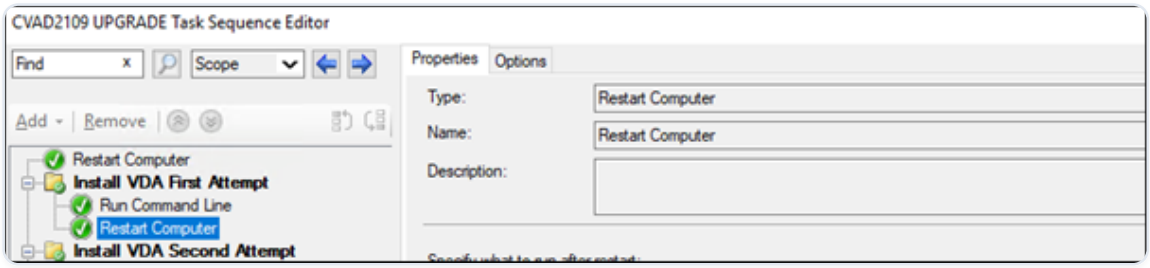


   c. O SCCM deve capturar o código de retorno.

      - Se o código de retorno for 0 ou 8, a instalação estará concluída e será necessário reiniciar.



      - Se o código de retorno for 3, reinicie a máquina e, em seguida, passe o controle para **Instalar VDA Segunda Tentativa**.



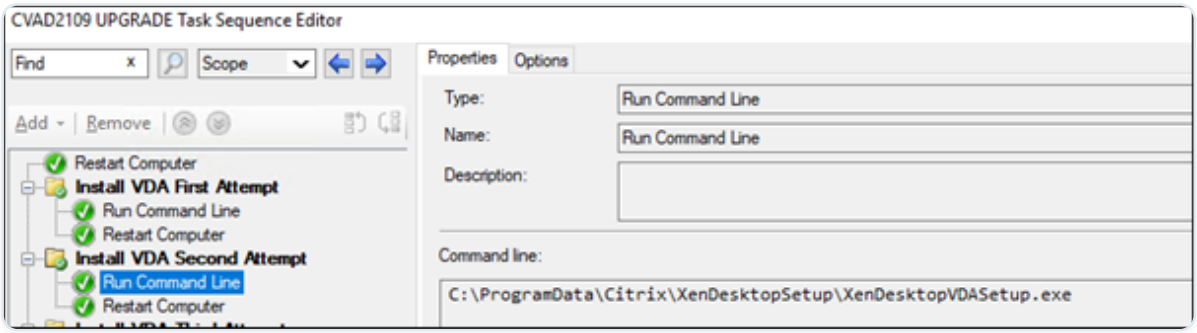
3. **Instalar VDA Segunda Tentativa:** Continuar a instalação do VDA.

   a. Após a **Instalação do VDA Primeira Tentativa**, se o arquivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` existir, a instalação não está completa e deve ser continuada após a conclusão da reinicialização.



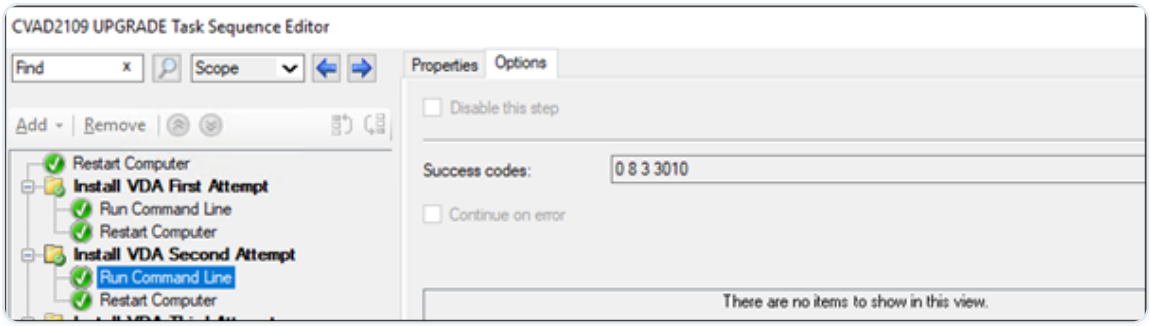
   b. **Instalar VDA Segunda Tentativa** se repete até que o arquivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` não exista ou um código de retorno diferente de 0 ou 8 seja retornado. Trate qualquer outro código de retorno como um erro, e INSTALAR VDA SEGUNDA TENTATIVA deve relatar um erro e parar.

   c. Retome a instalação do VDA executando o instalador VDA apropriado (`XenDesktopVdaSetup.exe` para a maioria dos casos, ou `XenDesktopRemotePCSetup.exe` se `VDAWorkstationCoreSetup_XXXX.exe` foi usado) do diretório do arquivo `%programdata%\ Citrix\XenDesktopSetup\` sem parâmetros de linha de comando. (O instalador VDA usa os parâmetros que salvou durante a primeira execução do instalador.)



   d. Observe o código de retorno do instalador VDA.

- 0 ou 8: Sucesso, instalação concluída, reinicialização necessária.



- 3: A instalação não está completa. Reinicie a máquina e repita INSTALAR VDA SEGUNDA TENTATIVA até que o arquivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` não exista ou até que um 0 ou 8 seja retornado. Trate qualquer outro código de retorno como um erro, e INSTALAR VDA SEGUNDA TENTATIVA deve relatar um erro e terminar.

Para mais informações sobre códigos de retorno, consulte Códigos de retorno de instalação do Citrix.

Exemplos de comandos de instalação do VDA

As opções de instalação disponíveis variam, dependendo do instalador utilizado. Consulte os seguintes artigos para obter detalhes sobre as opções de linha de comando.

- Instalar VDAs
- Instalar usando a linha de comando

COMANDOS DE INSTALAÇÃO PARA ACESSO REMOTO A PC

- O comando a seguir usa o instalador VDA principal de sessão única (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- O comando a seguir usa o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

COMANDO DE INSTALAÇÃO PARA VDI DEDICADO

- O comando a seguir usa o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`):

```
VDAWorkstationSetup.exe /quiet /components vda /controllers
“control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /
noreboot
```

Instalar VDAs usando Ansible

Visão geral

Este artigo descreve como implantar VDAs usando Ansible. Para mais informações, consulte a documentação do Ansible.

> **Observação:**
>
> Este artigo descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

Etapas principais para implantar VDA usando Ansible

1. Configurar o ambiente da máquina virtual.
2. Instalar o Ansible
3. Configuração do Kerberos
    a. Instalar o Kerberos
    b. Configurar o Kerberos
4. Configurar o Ansible

ETAPA 1: CONFIGURAR O AMBIENTE DA MÁQUINA VIRTUAL

Execute os seguintes comandos no servidor Windows.

1. Defina PS RemoteSigned. `Set-ExecutionPolicy RemoteSigned`
2. Defina o WinRM para usar não criptografado: `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

> **Observação:**

> Se ocorrer um erro nesta etapa, use o seguinte comando: `Enable-PSRemoting -Force`

3. Abra a porta 5985 do firewall. `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ETAPA 2: INSTALAR O ANSIBLE

Para instalar o Ansible com Ubuntu 20.4 ou posterior, execute os seguintes comandos:

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ETAPA 2I: INSTALAR O KERBEROS

Para instalar o Kerberos, execute o seguinte comando.

`sudo apt install python3-dev libkrb5-dev krb5-user`

ETAPA 2II: CONFIGURAR O KERBEROS

Para configurar o Kerberos, execute o seguinte comando:

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

Observação:

Use letras maiúsculas para o nome do realm do Kerberos.

```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        .toronto.edu = UTORONTO.CA
        .utoronto.ca = UTORONTO.CA
```

ETAPA 3: CONFIGURAR O ANSIBLE

Para configurar o host do Ansible, conclua as seguintes etapas:

1. Execute o seguinte comando:

   `Edit /etc/ansible/hosts`

2. Configure um arquivo `Install.yaml` do Delivery Controller

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

```
- name: Install multi-session VDA using network share path
  hosts: TSVDA

  tasks:

  - name: mount a cvad iso
    community.windows.win_disk_image:
      image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: present
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user: [redacted]
      ansible_become_password: [redacted]
    register: disk_image_out

  - name: copy iso file to c drive temp folder
    ansible.windows.win_copy:
      src: "{{disk_image_out.mount_paths[0]}}"
      dest: C:\Temp\
      remote_src: yes

  - name: unmount iso
    community.windows.win_disk_image:
      image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: absent
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user: [redacted]
      ansible_become_password: [redacted]
-- INSERT --                                                                    26,83         Top
```

```
- name: unmount iso
  community.windows.win_disk_image:
    image_path: \\[redacted]\Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
    state: absent
  become: true
  become_method: runas
  become_flags: logon_type=new_credentials logon_flags=netcredentials_only
  vars:
    ansible_become_user: [redacted]
    ansible_become_password: [redacted]

- name: stop windows upgrade service
  ansible.windows.win_service:
    name: wuauserv
    start_mode: disabled
    state: stopped

- name: Restart server before install
  ansible.windows.win_reboot:

- name: Install vda from exe
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    arguments: /quiet /verboselog /PORTNUMBER [redacted] /logpath 'C:\CitrixInstallationLogs\TSVDA' /components "VDA,PLUGINS"  /CONT
ROLLERS '[redacted]'  /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT /NOREBOOT /NORESUME
    expected_return_code: [0, 3,3010]
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
```

```
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
  win_reboot:
  when: install_vda.changed

- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find
```

```
- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find

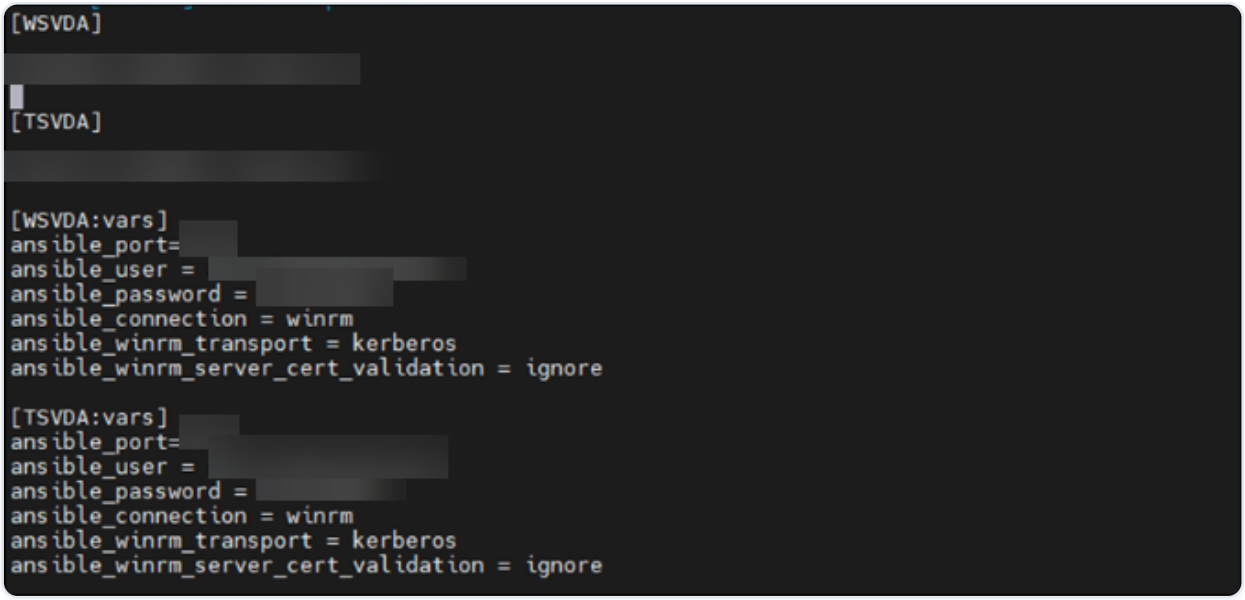
- name: Restart server after VDA install
  win_reboot:
  when: vda_install_find.matched == 0

- name: remove temp folder
  win_file:
    path: C:\Temp\
    state: absent
```

3. Execute o arquivo yaml com o seguinte comando: `sudo ansible-playbook install.yml -vvv` (Modo detalhado)

4. Você pode configurar vários hosts no arquivo de configuração com outras configurações adicionais.

   `Edit /etc/ansible/hosts`



Instalar VDAs usando Microsoft Intune

Visão geral

Este artigo descreve como implantar VDAs usando Microsoft Intune. Para obter mais informações, consulte a documentação da Microsoft.

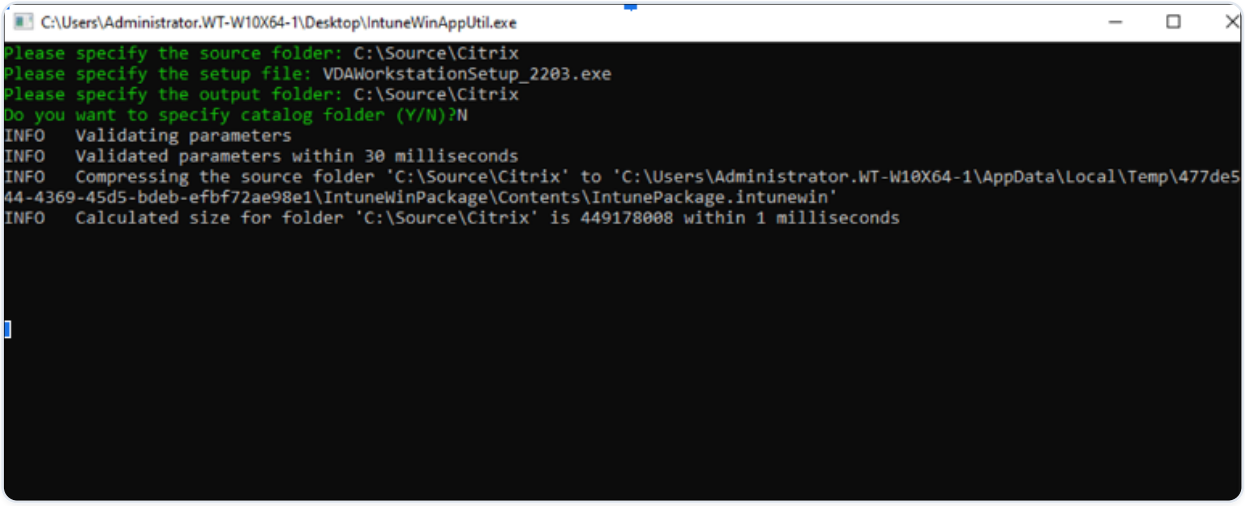
> **Observação:**
>
> O artigo a seguir descreve apenas recomendações baseadas em como a Citrix® testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não se responsabiliza por quaisquer atualizações ou ajustes necessários para que isso se adapte às necessidades do cliente.

Etapas principais para implantar VDA usando Microsoft Intune

1. Preparar a instalação para o Citrix VDA.
2. Configurar o Assinante do Programa de Desenvolvedores do Microsoft 365.
3. Adicionar e atribuir um aplicativo.
4. Instalar o aplicativo no dispositivo registrado.

ETAPA 1: PREPARAR A INSTALAÇÃO PARA O CITRIX VDA

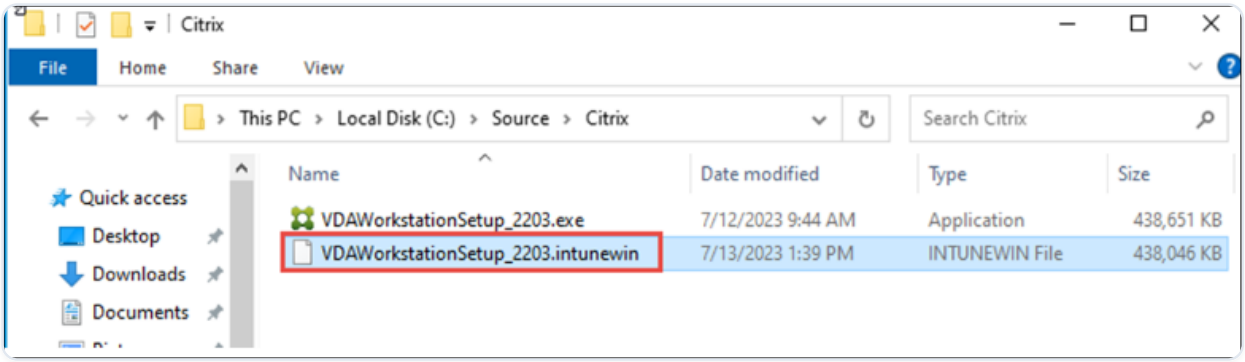
1. Baixe o IntuneWinAppUtil.exe atualizado do GitHub.
2. Execute o arquivo `IntuneWinAppUtil.exe` usando **Executar como administrador**.
3. Insira os seguintes dados:



   a. **Especifique a pasta de origem**: Insira a pasta que contém os arquivos de configuração do seu aplicativo. Por exemplo, C:\source\Citrix.
   b. **Especifique o arquivo de configuração**: Insira o nome do arquivo de configuração (como setup.exe ou setup.msi). Por exemplo, VDAWorkstationSetup_2203.exe.
   c. **Especifique a pasta de saída**: Insira o caminho da pasta de saída para gerar o arquivo .intunewin. Por exemplo, C:\source\Citrix.
   d. **Deseja especificar a pasta de catálogo (S/N)**: Digite N.

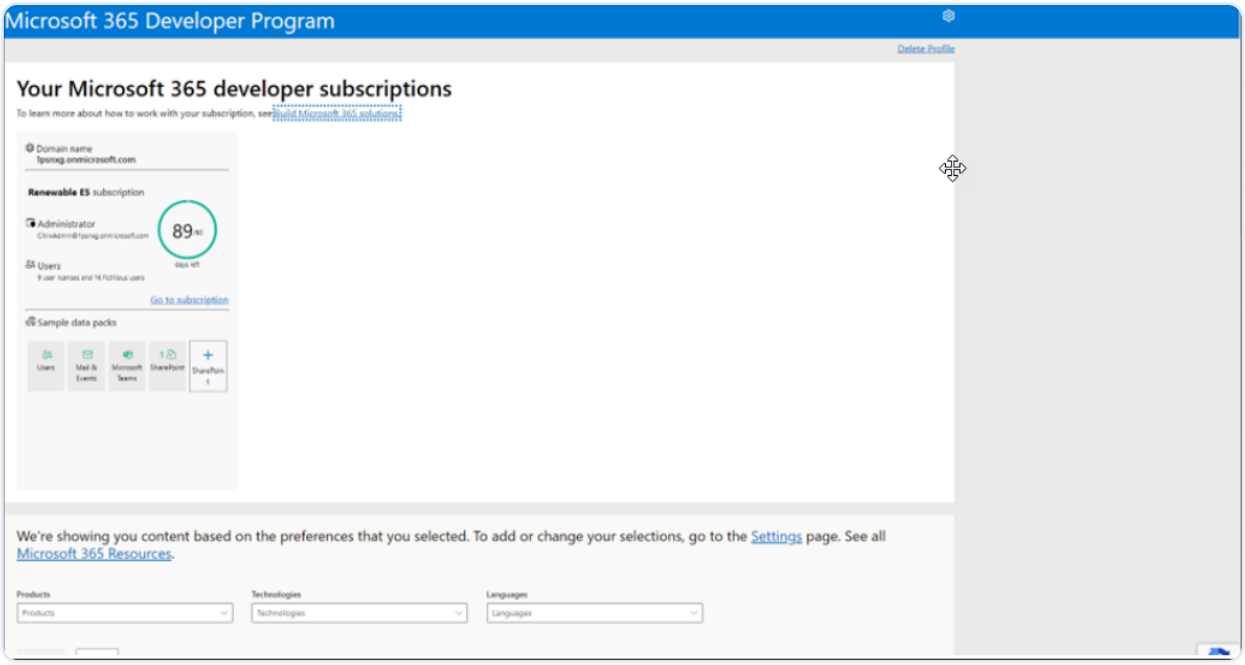
> **Observação:**
>
> Aguarde alguns minutos enquanto a **Win32 Content Prep Tool** está em execução. Assim que ele gerar o arquivo `.intunewin`, o status indicará 100% na parte inferior do prompt de comando.

4. Assim que o processo for concluído, vá para a pasta de saída (Neste exemplo, `C:\source\Citrix`) para obter o arquivo de implantação do Microsoft Intune.
5. Inscreva-se para uma avaliação gratuita do Microsoft Intune.

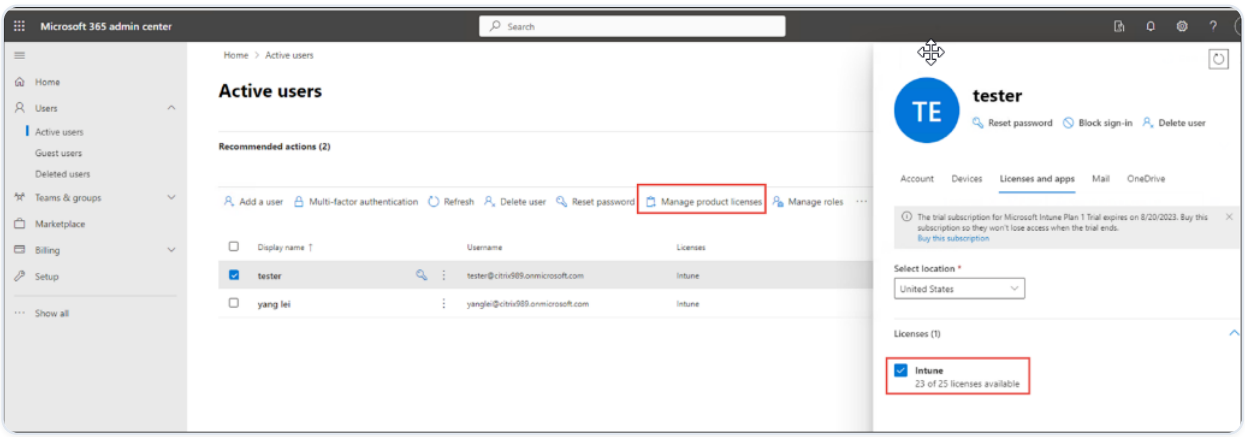


ETAPA 2: CONFIGURAR O ASSINANTE DO PROGRAMA DE DESENVOLVEDORES DO MICROSOFT 365

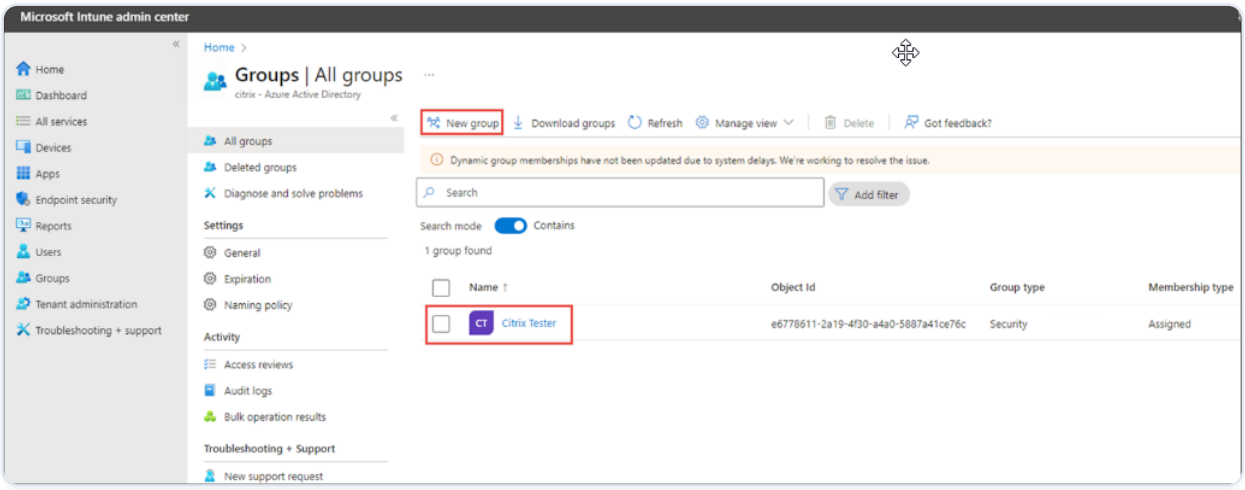
1. Crie o sandbox instantâneo para ativar sua assinatura. Para obter seu sandbox de desenvolvedor, vá para o seu painel do Programa de Desenvolvedores do Microsoft 365 e selecione **Adicionar uma nova assinatura**.



2. Crie um usuário no centro de administração do Microsoft 365 e atribua uma licença ao usuário.



3. Crie um grupo.



4. Depois que o grupo for criado, você deverá fornecer a autoridade MDM ao grupo. Configure o registro automático. Pode levar um minuto para ativar. Ou você pode adicionar manualmente a autoridade MDM ao grupo, seguindo as etapas abaixo:

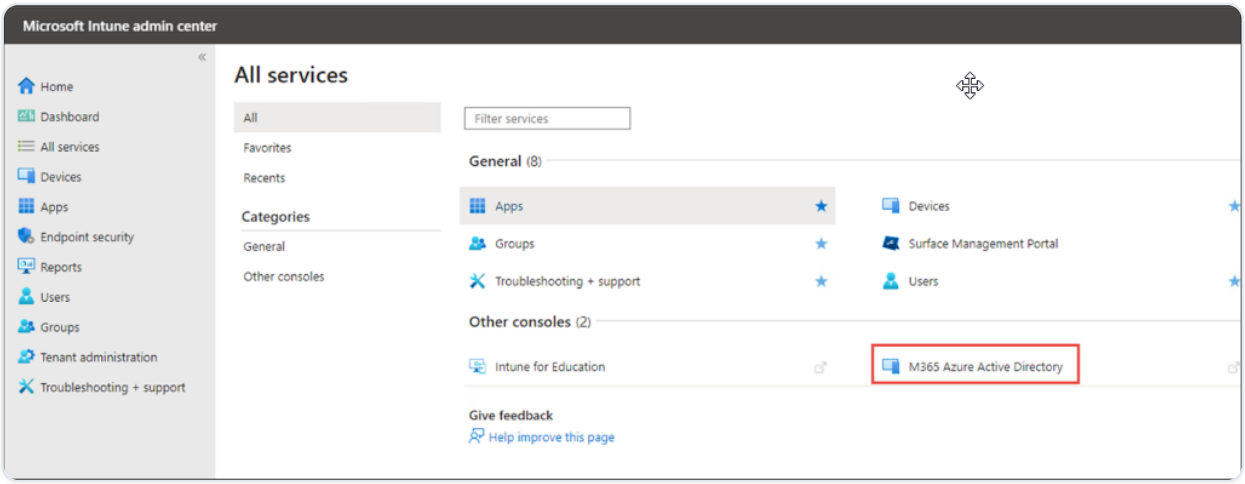
   a. Vá para **Todos os serviços > Microsoft Entra**.

   b. Vá para **settings > Mobility** e selecione **Microsoft Intune**.

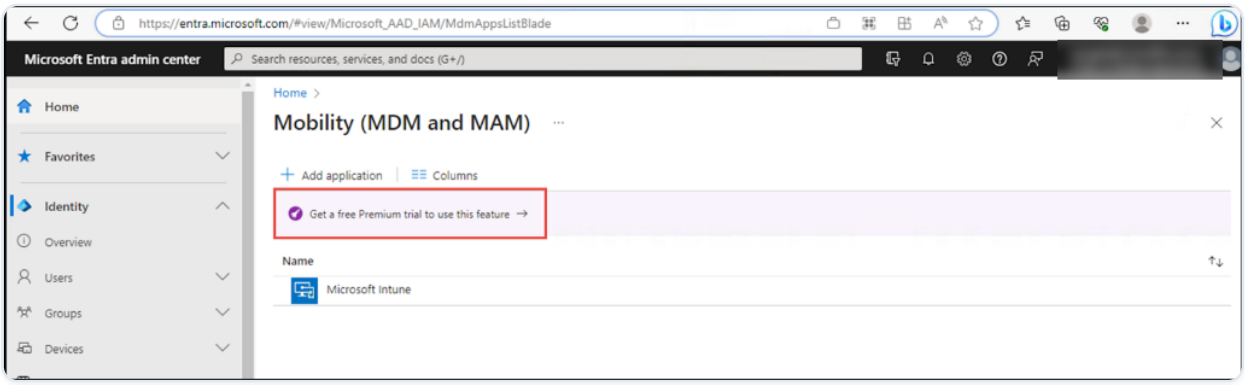
   c. Selecione o grupo que você acabou de criar. Isso abre uma página com o escopo de usuário MDM.

   d. Clique em **Salvar**.

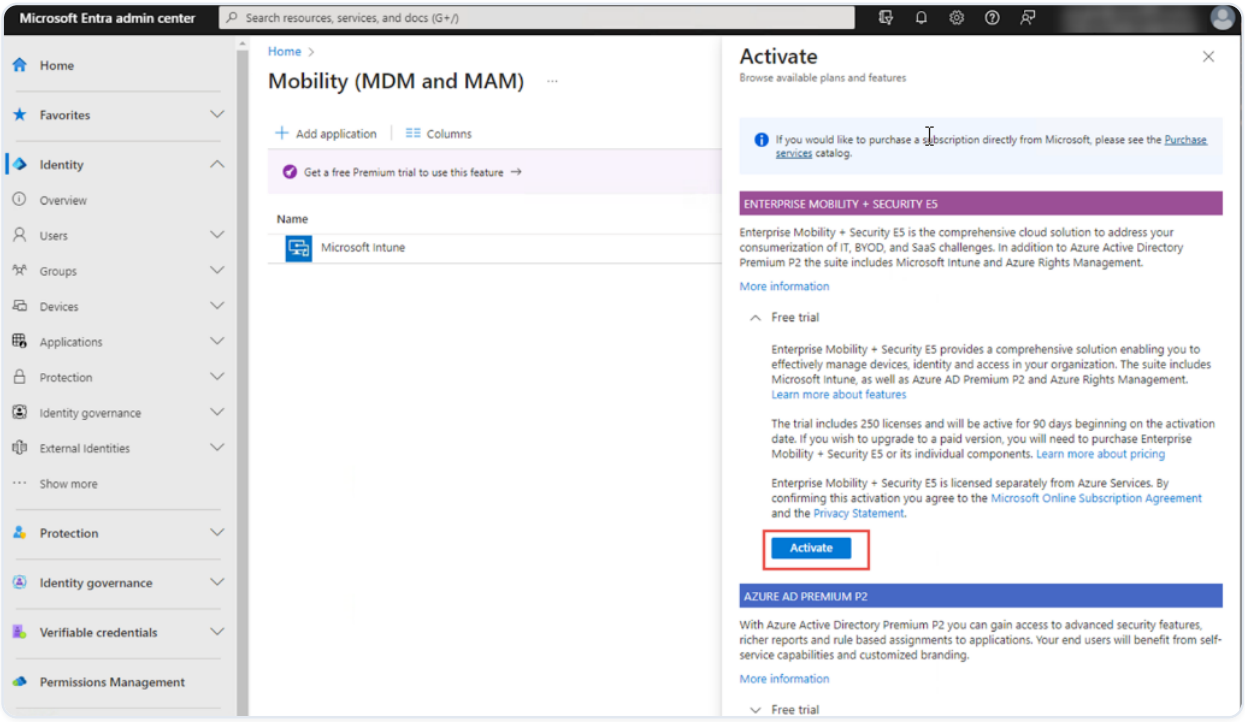
5. Na guia **All Services**, clique em **M365 Azure Active Directory**.



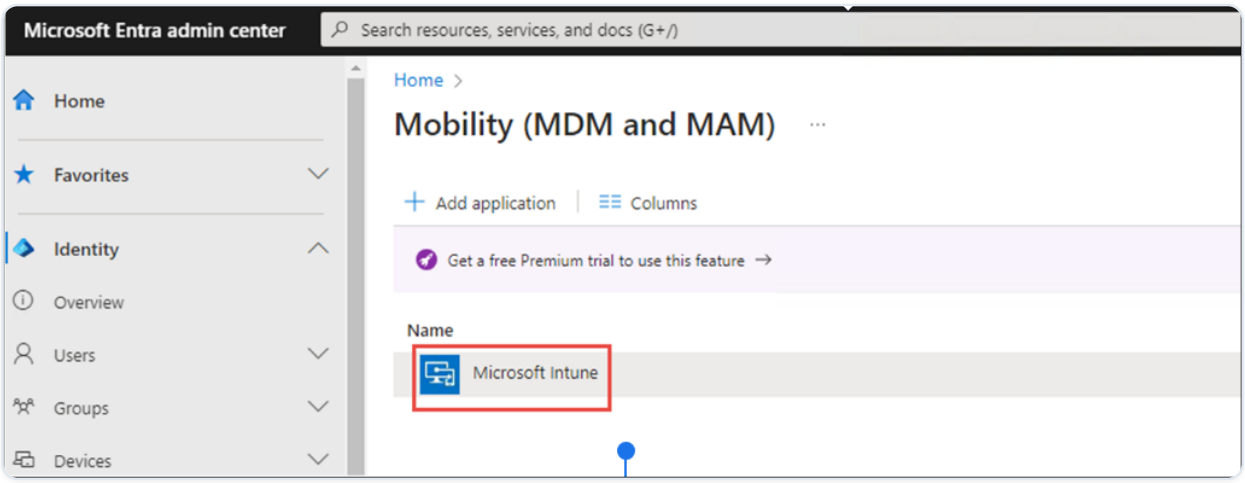
6. Clique em **Obter uma avaliação Premium gratuita para usar este recurso**.



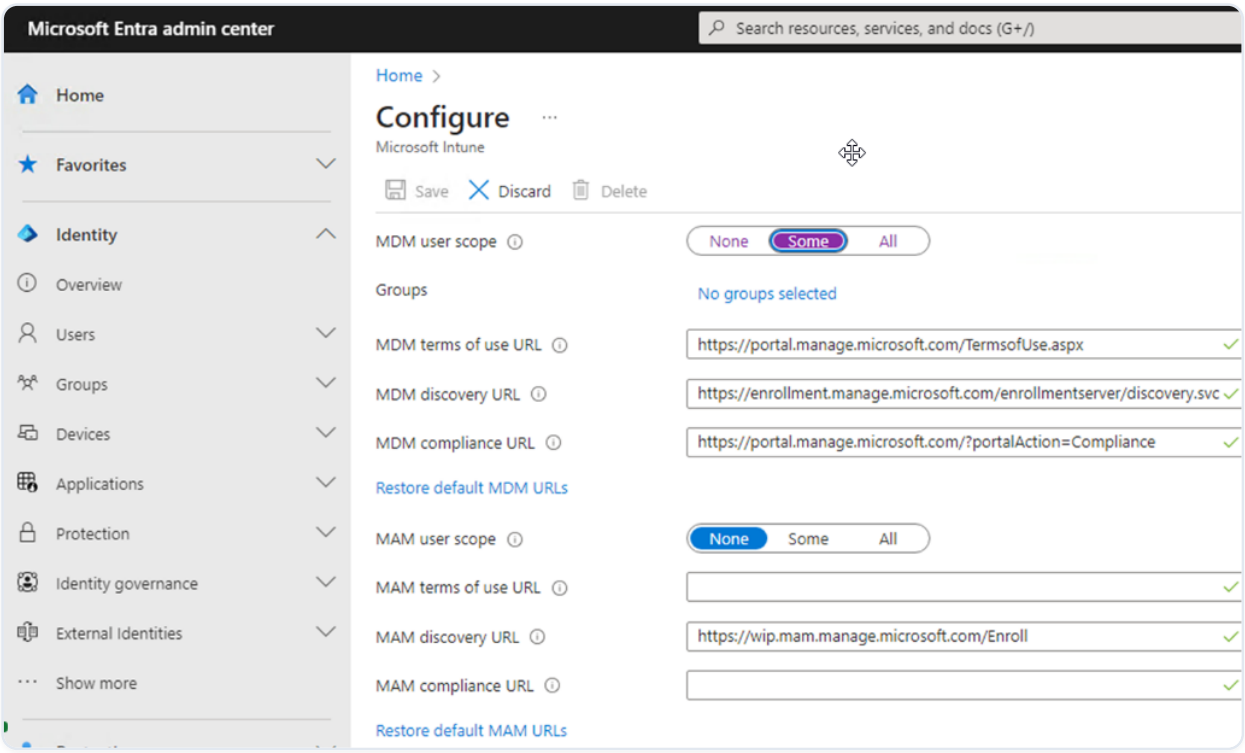
7. Clique em **Ativar**.



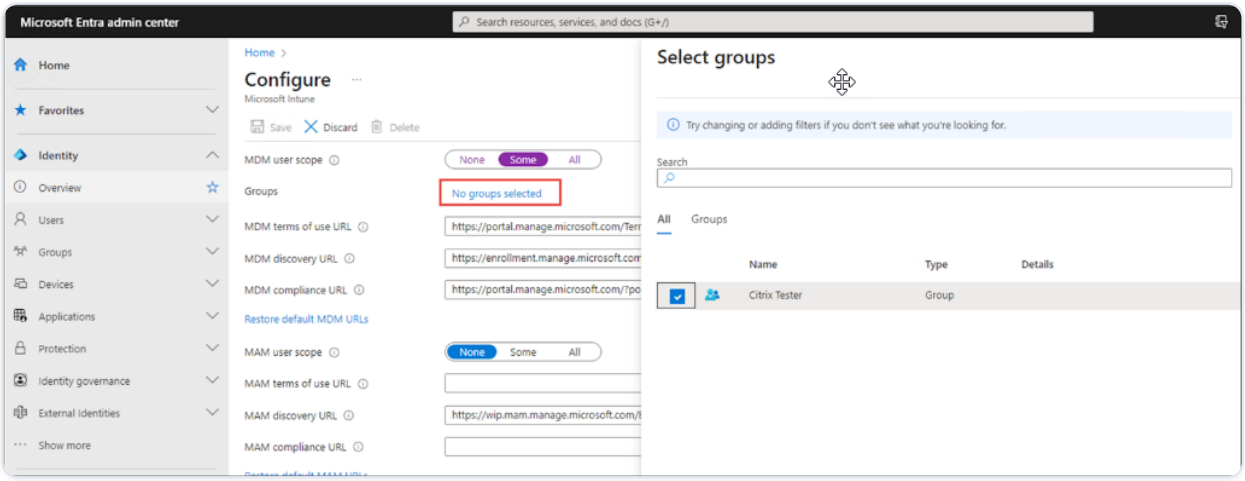
8. Agora, clique em **Microsoft Intune**.



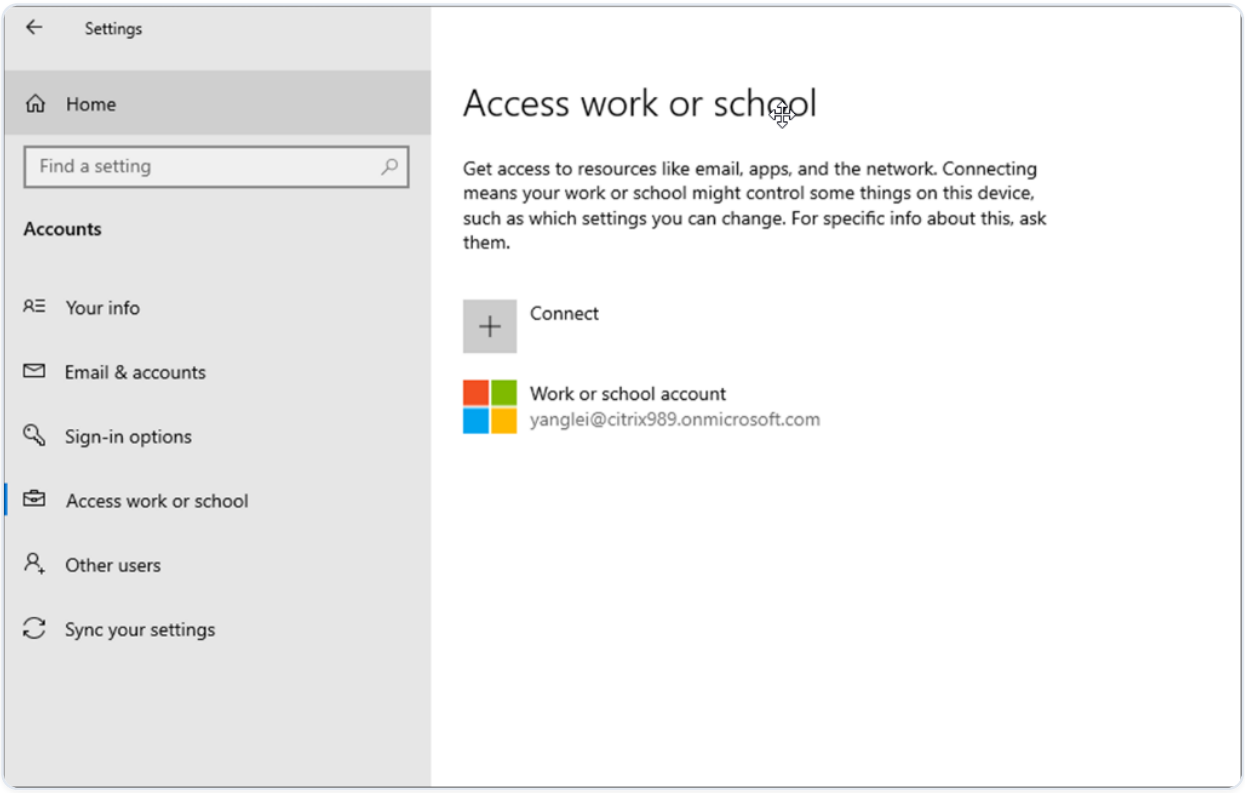
9. Na guia **Configure**, insira as configurações necessárias.



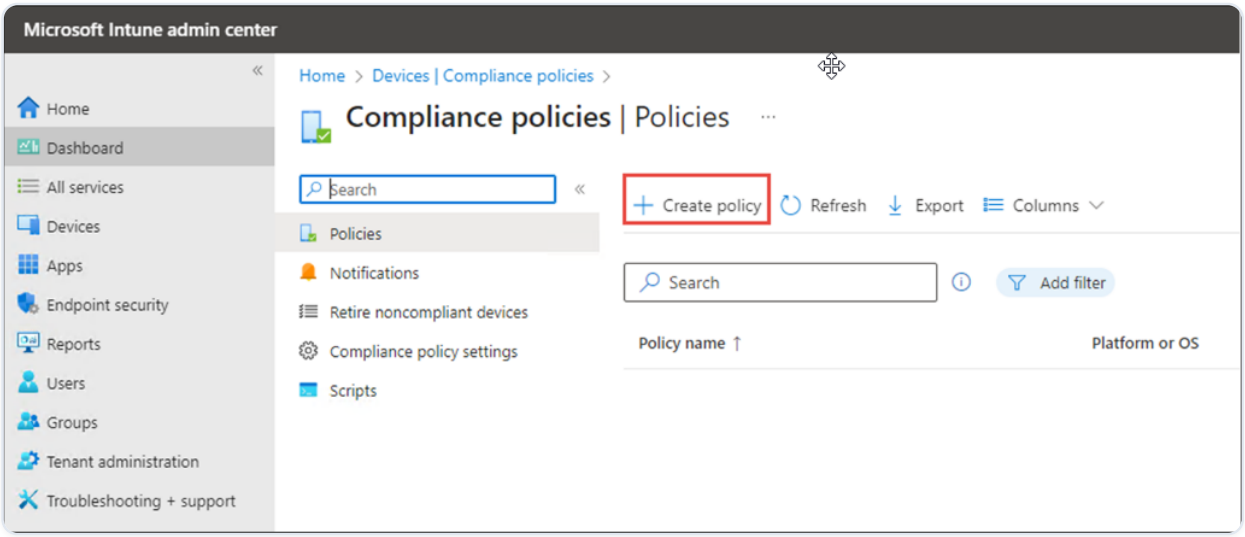
10. Para adicionar um grupo, clique em **Nenhum grupo selecionado**.



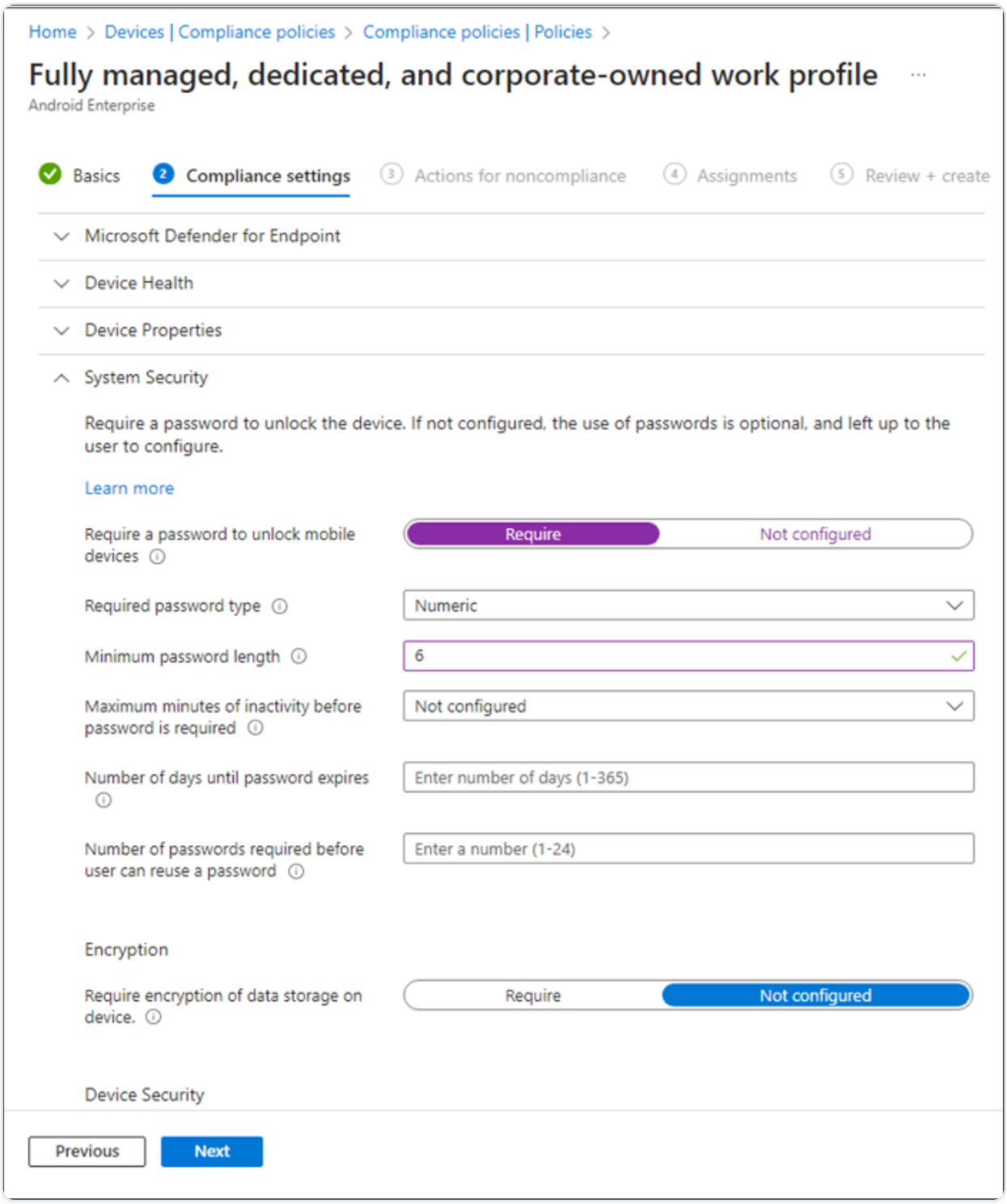
11. Registre seu dispositivo.



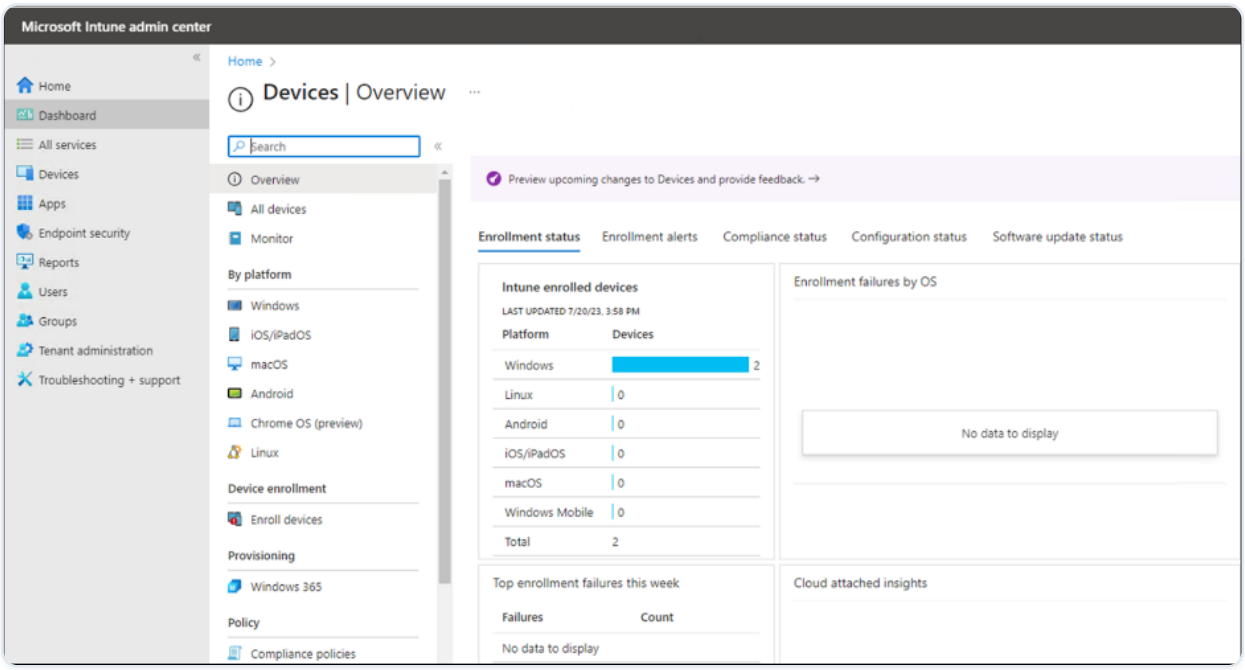
12. Crie uma política de conformidade de dispositivo para alterar a conformidade do seu Dispositivo recém-criado para `Compliant`.



13. Vá para a guia **Atribuições** para adicionar o grupo recém-criado.



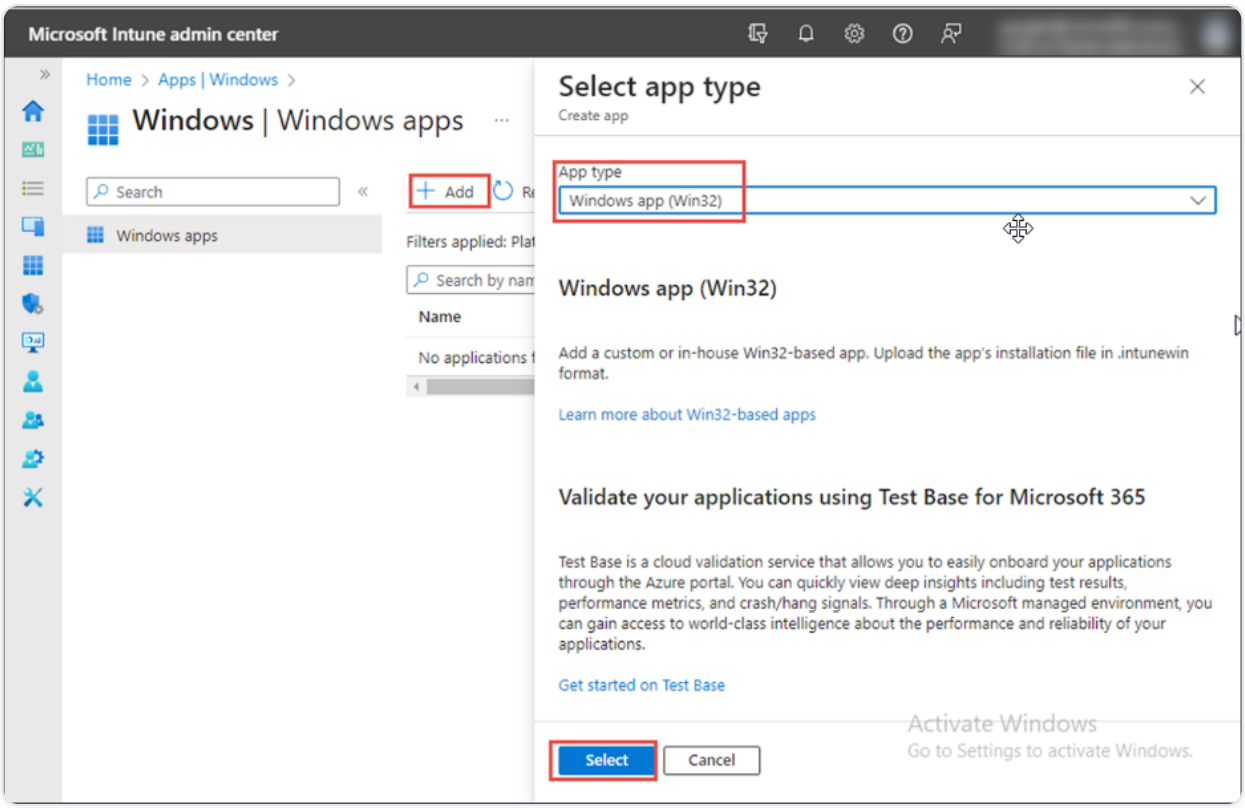
14. Confirme o registro do dispositivo.



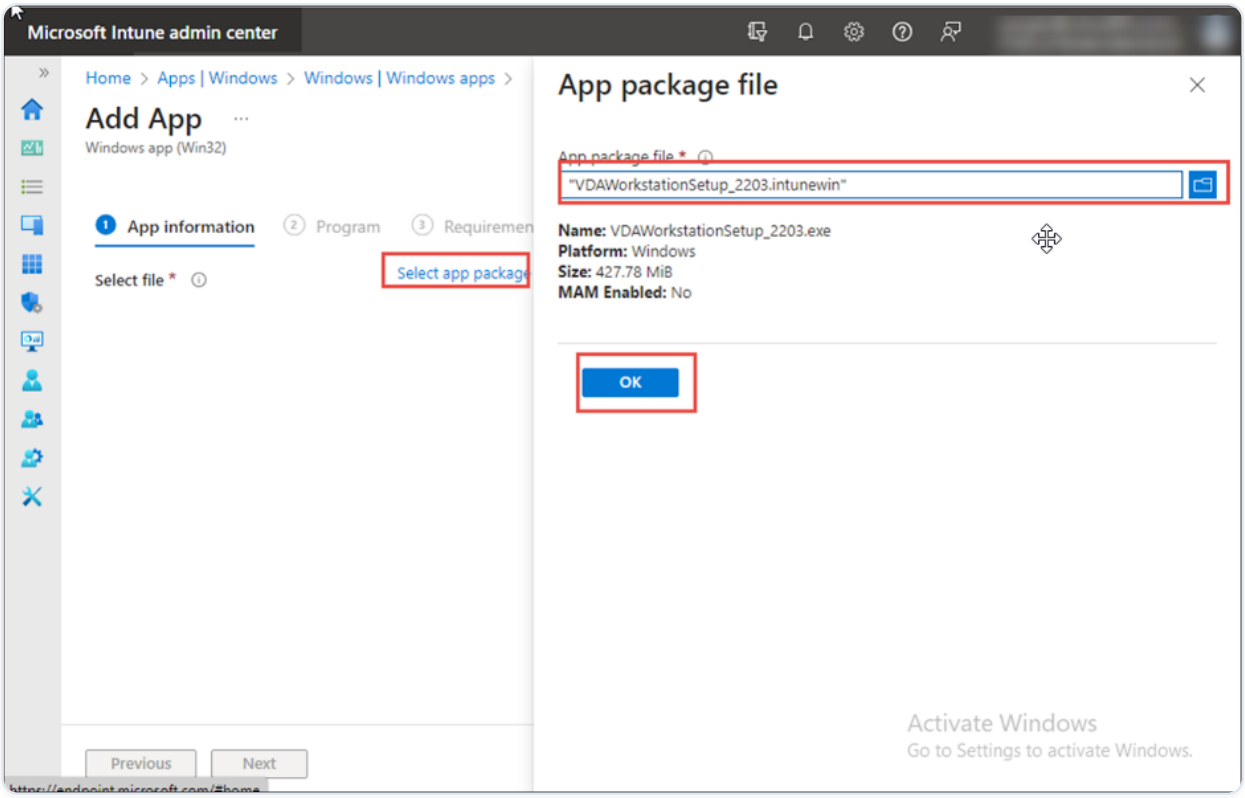
Para informações detalhadas, consulte programa de desenvolvedor do Microsoft 365.

ETAPA 3: ADICIONAR E ATRIBUIR UM APLICATIVO

1. Faça login no centro de administração do Microsoft Intune.
2. Selecione **Aplicativos > Todos os aplicativos > Adicionar** ou vá para **Aplicativos > Windows > Aplicativos do Windows**.



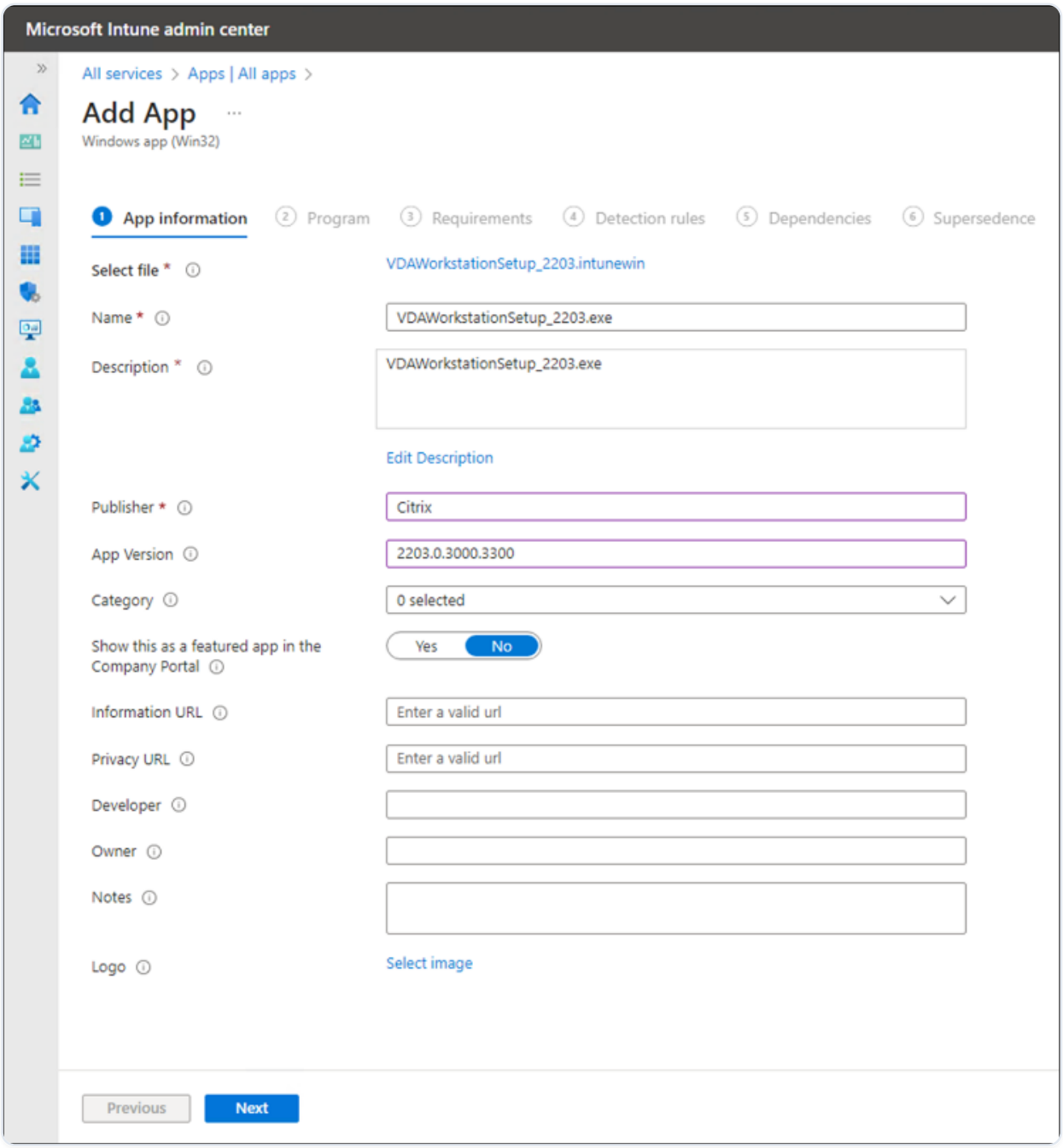
3. No painel **Selecionar tipo de aplicativo**, selecione **Outros tipos de aplicativo > Aplicativo Windows (Win32)** e clique em **Selecionar**.
4. No painel **Adicionar aplicativo**, clique em **Selecionar arquivo de pacote de aplicativo**. Clique em **procurar**.
5. Selecione o arquivo preparado com a extensão `.intunewin`. O arquivo preparado é criado durante a etapa Preparar instalação para o Citrix VDA. Uma página contendo informações detalhadas sobre o aplicativo é exibida.



Observação:

- Se você estiver usando uma máquina server-core, você deve usar o VDA workstation core.
- Se você estiver usando um SO de desktop Windows 10, você deve usar o VDA workstation.
- Se você estiver usando um SO de servidor (Por exemplo, Windows 2022), você deve usar a configuração do servidor VDA.
- Neste exemplo, estamos usando a versão 2203, mas isso é aplicável a todas as versões.

6. Clique em **OK** no painel **Arquivo de pacote do aplicativo**.
7. Na tela seguinte, na guia **Informações do Aplicativo**, insira o **Nome** do Aplicativo e a **Descrição** do Aplicativo Windows. Insira o nome do **Editor** como `Citrix`, e você pode especificar informações adicionais do aplicativo aqui. Clique em **Avançar**.



8. Na próxima tela, insira os seguintes valores:

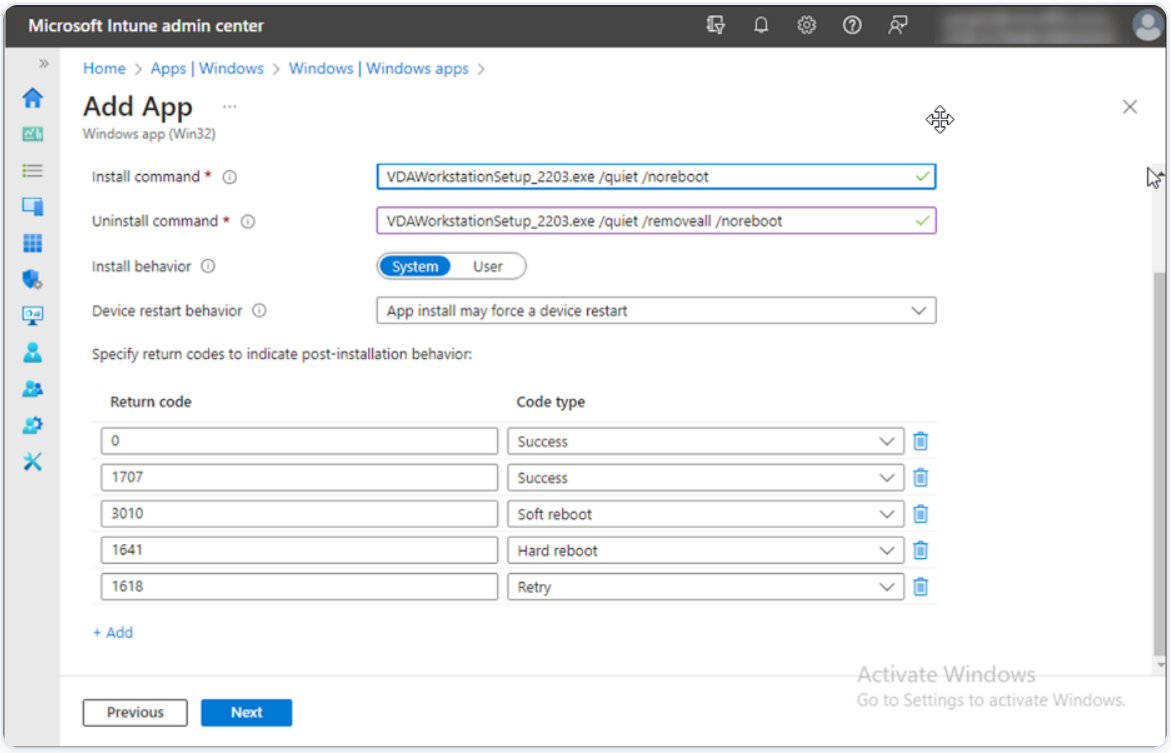
   - **Comando de instalação**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **Comando de desinstalação**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **Comportamento de instalação**:

- **Sistema**: Selecione esta opção para instalar o aplicativo em todos os dispositivos do grupo.
- **Usuário**: Selecione esta opção para instalar o aplicativo apenas em um dispositivo de usuário específico no grupo.

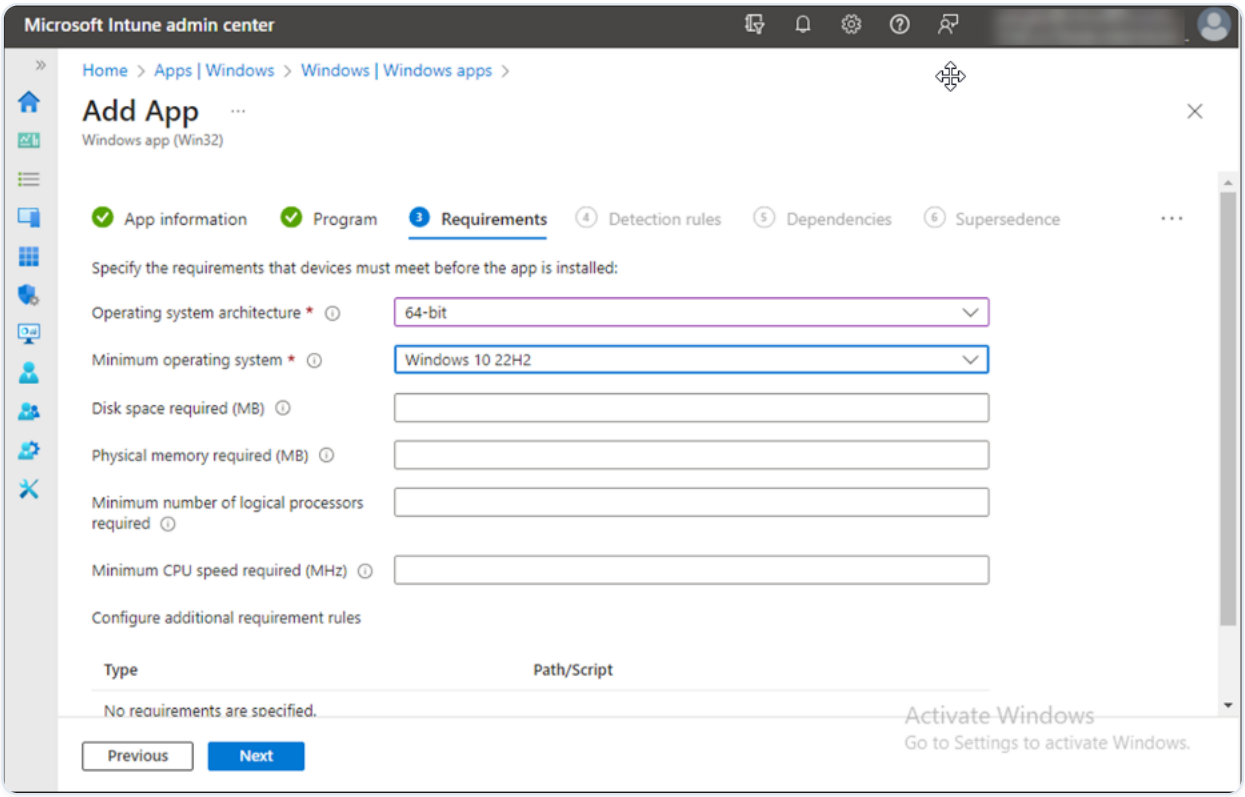
9. Clique em **Avançar**.

Observação:

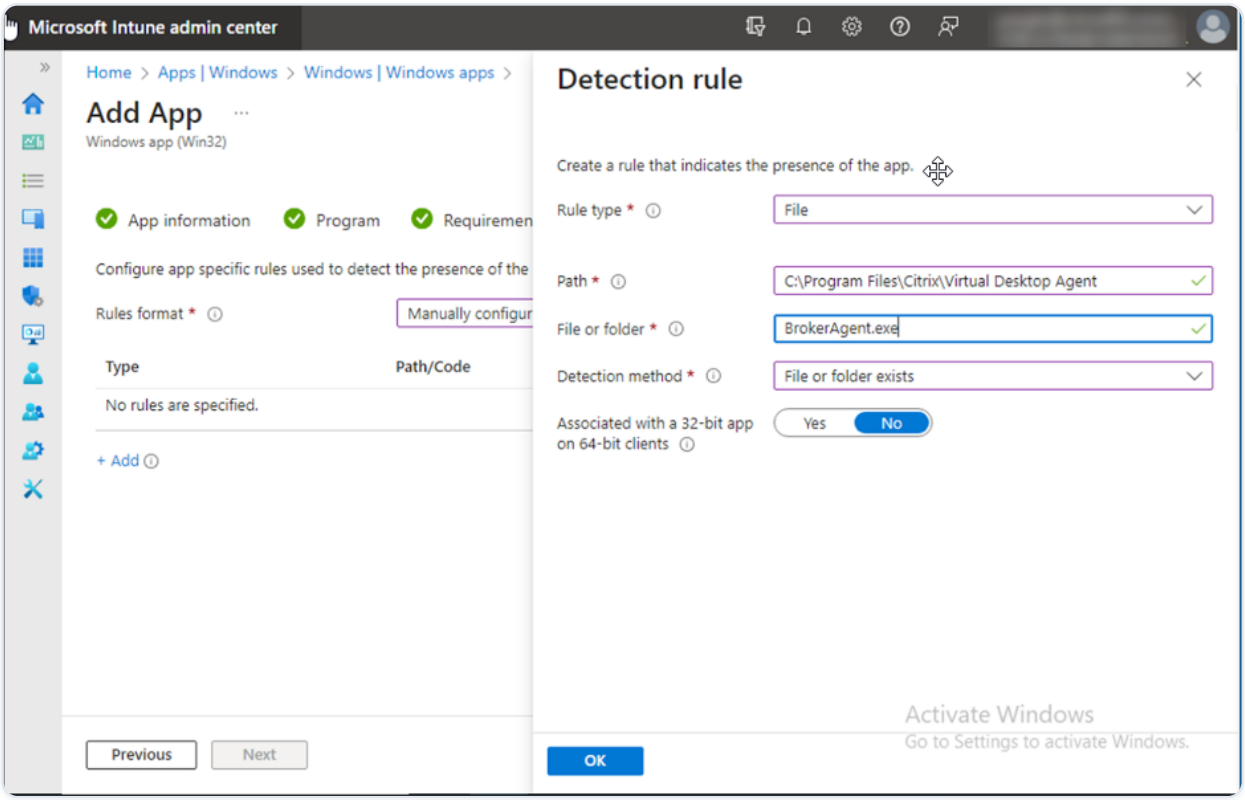
- Este exemplo usa a versão 2203, mas você pode usá-lo com qualquer versão.
- Adicionar `/noreboot` a um comando não significa que não haverá reinicializações durante a instalação ou implantação, mas apenas impõe reinicializações obrigatórias. Para obter mais informações sobre scripts, consulte Opções de linha de comando para instalar um VDA.
- Para **Comportamento de reinicialização do dispositivo**, selecione **O Intune forçará uma reinicialização obrigatória do dispositivo**.
- Na caixa de texto **Código de retorno**, insira `0`, `3` e `8` para sucesso pós-instalação. Para obter informações sobre outros códigos de retorno, consulte Códigos de retorno de instalação do Citrix.



10. Na tela seguinte, na guia **Requisitos**, insira os valores necessários. Clique em **Avançar**.

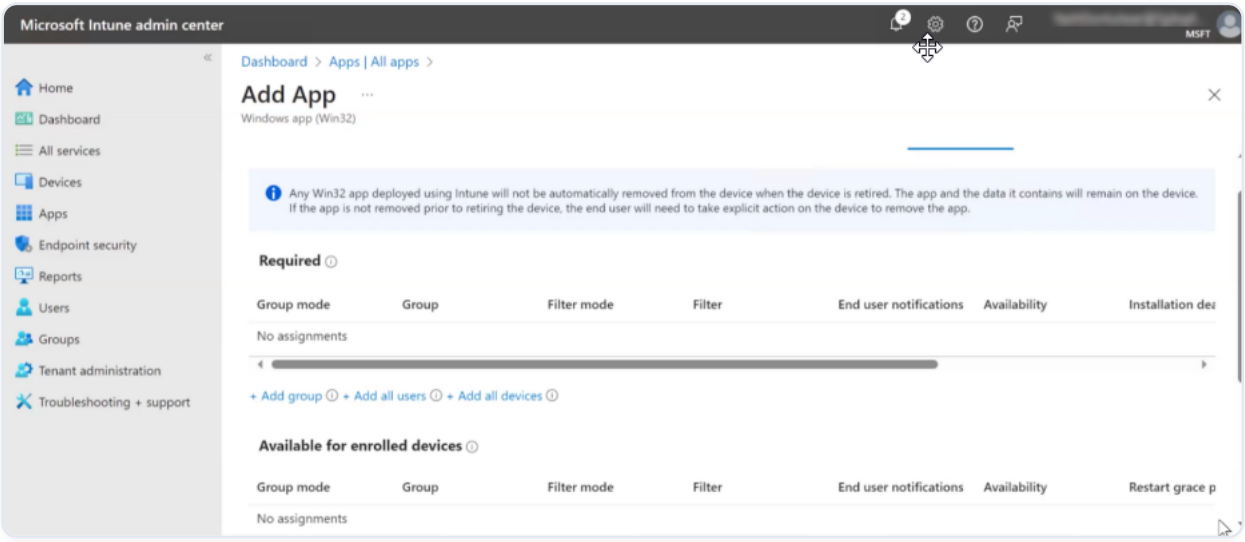


11. Na tela seguinte, na guia **Regra de detecção**, adicione **Regra de detecção** para adicionar o agente Broker. Clique em **OK**.

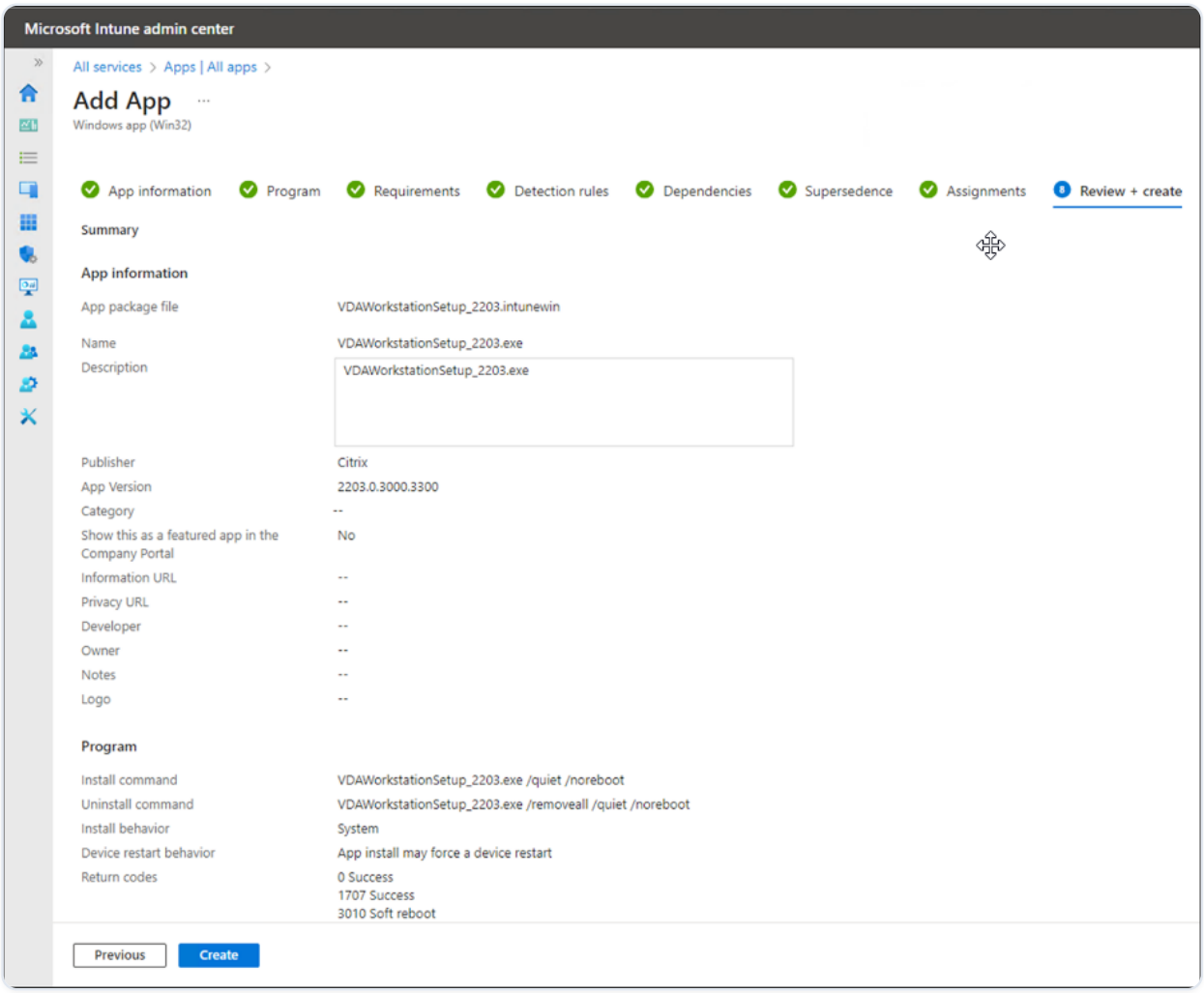


12. Na guia **Atribuições**, você pode adicionar os dispositivos no seguinte:

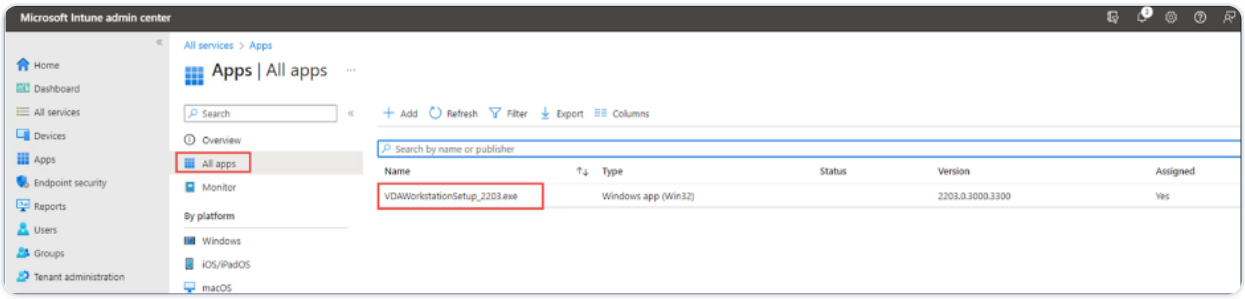
- **Obrigatório**: Os dispositivos para os quais as atualizações ocorrem automaticamente.
- **Disponível para dispositivos registrados**: Os dispositivos para os quais as atualizações ocorrem manualmente.



13. Revise os detalhes e clique em **Criar**.



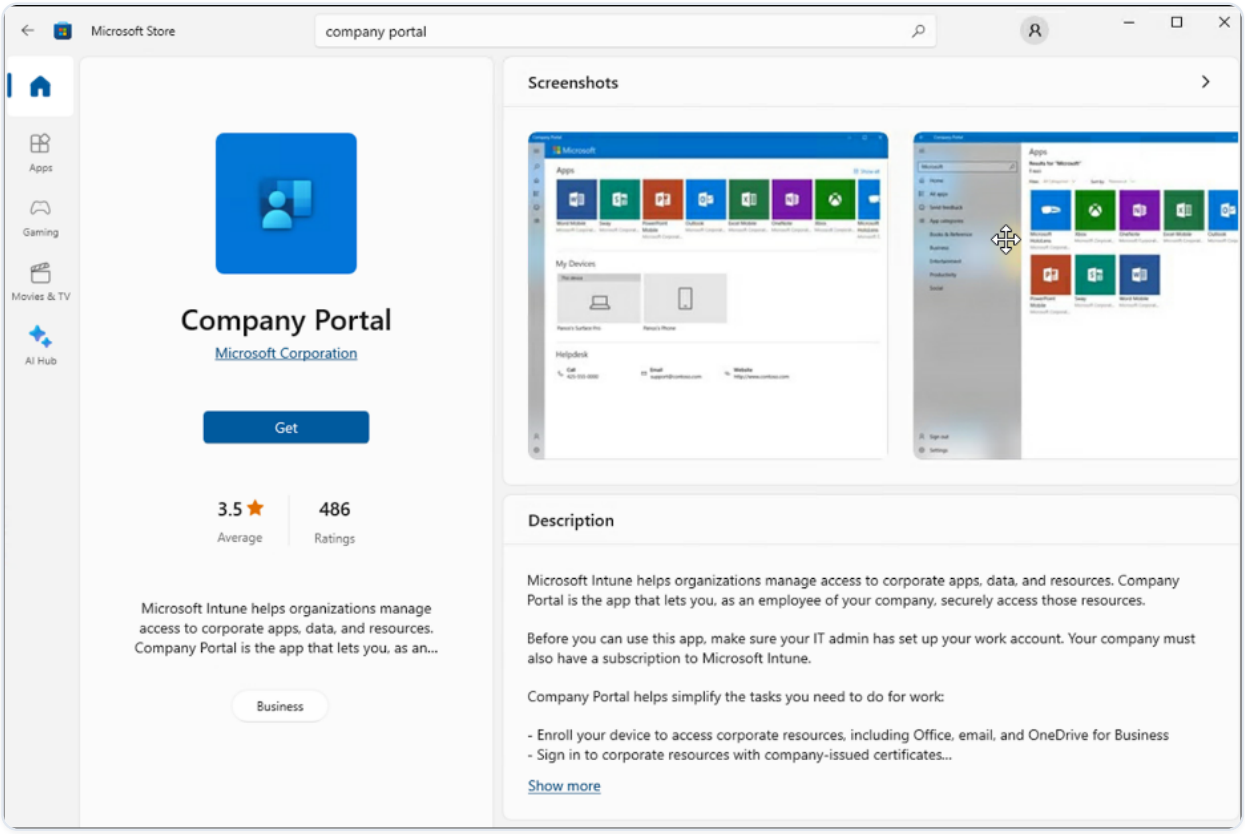
O aplicativo foi atribuído com sucesso.



Para obter informações detalhadas, consulte Adicionar e atribuir um aplicativo.

ETAPA 4: INSTALAR O APLICATIVO NO DISPOSITIVO REGISTRADO

1. Faça login no seu dispositivo Windows 10 Desktop registrado. O dispositivo deve estar registrado no Microsoft Intune. Além disso, você deve fazer login no dispositivo usando uma conta contida no grupo que você atribuiu ao aplicativo. Para obter mais informações, consulte a documentação da Microsoft.
2. No menu **Iniciar**, abra a **Microsoft Store**.
3. Procure o aplicativo **Portal da Empresa** e instale-o.



4. Execute o aplicativo **Portal da Empresa**.
5. Clique no aplicativo que você adicionou usando o Microsoft Intune. Se você não atribuiu nenhum aplicativo com sucesso ao usuário do Intune, a seguinte mensagem será exibida:

```
Your IT administrator did not make any apps available to you.
```

6. Clique em **Instalar**.

Criar um site

> **Observação:**
>
> Durante a criação do site, depois de adicionar uma licença para habilitar a Licença de Direitos Híbridos, os hosts de nuvem pública (como Microsoft Azure, Google Cloud Platform e Amazon Web Services) não aparecem na lista de tipos de conexão até que a criação do site seja concluída.

> Um site é o nome que você dá a uma implantação do Citrix Virtual Apps and Desktops™. Ele compreende os Delivery Controllers e outros componentes principais, Virtual Delivery Agents (VDAs), conexões com hosts, catálogos de máquinas e grupos de entrega. Você cria o site depois de instalar os componentes principais e antes de criar o primeiro catálogo de máquinas e grupo de entrega.

Se o seu Controller estiver instalado no Server Core, use os cmdlets do PowerShell no Citrix Virtual Apps and Desktops SDK para criar um site.

Ao criar um site, você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente Citrix (CEIP). O CEIP coleta estatísticas anônimas e informações de uso e as envia para a Citrix. O primeiro pacote de dados é enviado à Citrix aproximadamente sete dias após a criação do site. Você pode alterar sua inscrição a qualquer momento após a criação do site. Selecione **Configurações** no painel esquerdo do Web Studio e, em seguida, localize a configuração **Programa de Melhoria da Experiência do Cliente Citrix**. Para obter detalhes, consulte `<http://more.citrix.com/XD-CEIP>`.

O usuário que cria um site se torna um administrador completo. Para obter mais informações, consulte Administração delegada.

Revise este artigo antes de criar o site, para saber o que esperar.

Etapa 1. Abra o assistente de criação de site - Citrix Site Manager

Use a ferramenta Citrix Site Manager para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como site). A ferramenta é instalada automaticamente quando você instala um Delivery Controller.

Para executar esta ferramenta, abra o menu Iniciar da sua área de trabalho em um Delivery Controller e selecione **Citrix > Citrix Site Manager**. Consulte Instalar o Web Studio.

Etapa 2. Nome do site

Na página **Introdução**, digite um nome para o site.

Etapa 3. Bancos de dados

A página **Bancos de dados** contém seleções para configurar os bancos de dados do site, de monitoramento e de registro de configuração. Para obter detalhes sobre as opções e requisitos de configuração do banco de dados, consulte Bancos de dados.

> **Observação:**
>
> Se um SQL Server Always On Listener estiver configurado para criptografia TLS, você poderá ser solicitado a inserir credenciais com permissões de criação de banco de dados. As tentativas de criar o banco de dados ainda falharão mesmo se você inserir credenciais de administrador válidas. Verifique se o certificado do SQL Server inclui o nome DNS do listener nos Subject Alternative Names (SAN). Para obter mais informações, consulte `<https://docs.microsoft.com/pt-br/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>`.

> Se você optar por instalar o SQL Server Express para usar como banco de dados do site (o padrão), uma reinicialização ocorrerá após a instalação desse software. Essa reinicialização não ocorrerá se você optar por não instalar o software SQL Server Express para usar como banco de dados do site.

Se você não estiver usando o SQL Server Express padrão, certifique-se de que o software SQL Server esteja instalado nas máquinas antes de criar um site. Requisitos do sistema lista as versões compatíveis.

Se você quiser adicionar mais Delivery Controllers ao site e já tiver instalado o software Controller em outros servidores, poderá adicionar esses Controllers a partir desta página. Se você também planeja gerar scripts que configuram os bancos de dados, adicione os Controllers antes de gerar os scripts.

Etapa 4. Licenciamento

Na página **Licenciamento**, especifique o endereço do Servidor de Licenças e, em seguida, indique qual licença usar (instalar).

- Especifique o endereço do Servidor de Licenças no formato `name:[port]`. O *nome* deve ser um FQDN, NetBIOS ou endereço IP. FQDN é recomendado. Se você omitir o número da porta, o padrão é 27000. Clique em **Conectar**. Você não pode prosseguir para a próxima página até que uma conexão bem-sucedida seja feita com o Servidor de Licenças.
- Quando uma conexão é estabelecida, **Usar uma licença existente** é selecionado por padrão. A exibição lista os produtos compatíveis para os quais este produto pode ser configurado, com base nas licenças atualmente instaladas.
    - Se você quiser configurar este produto como um dos produtos listados (por exemplo, Citrix Virtual Apps Premium ou Citrix Virtual Desktops™ Premium), usando uma dessas licenças, selecione essa entrada.
    - Se você já alocou e baixou uma licença (usando a Ferramenta Citrix Manage Licenses) para usar com este produto, mas ainda não instalou a licença:
        - Clique em **Procurar arquivo de licença**.
        - No explorador de arquivos, localize e selecione a licença que você baixou. Os produtos associados agora aparecem na página **Licenciamento** do assistente de criação do site. Selecione a entrada que deseja usar.
    - Se o produto desejado não for exibido, ou se você não tiver licenças alocadas e baixadas, você pode alocar, baixar e instalar uma licença. Para fazer isso, o Servidor de Licenças deve ter acesso à internet. Você deve ter um Código de Acesso de Licença para o produto desejado. A Citrix envia esse código por e-mail para você.
        - Clique em **Alocar e baixar**.
        - Na caixa de diálogo **Alocar Licenças**, insira o Código de Acesso de Licença enviado pela Citrix. Clique em **Alocar licenças**.
        - Os produtos associados à nova licença aparecem na página **Licenciamento** do assistente de criação do site. Selecione a entrada que deseja usar.

    Alternativamente, selecione **Usar a avaliação gratuita de 30 dias** e instale as licenças mais tarde. Para obter detalhes, consulte a documentação de licenciamento.

Etapa 5. Resumo

A página **Resumo** lista as informações que você especificou. Use o botão **Voltar** se quiser alterar algo. Quando terminar, clique em **Concluir**.

Mais informações

Conexão do host, rede e armazenamento

Se você estiver usando VMs em um hipervisor ou outro serviço para entregar aplicativos e desktops, poderá, opcionalmente, criar a primeira conexão com esse host. Você também pode especificar recursos de armazenamento e rede para essa conexão. Após criar o site, você pode modificar essa conexão e recursos, e criar mais conexões. Para obter detalhes, consulte Conexões e recursos.

- Para obter informações especificadas na página **Conexão**, consulte Conexões e recursos.
    - Se você não estiver usando VMs em um hipervisor ou outro serviço (ou se usar o Web Studio para gerenciar desktops em PCs blade dedicados), selecione o tipo de conexão **Nenhum**.
    - Se você estiver configurando um site de Acesso Remoto para PC e planeja usar o recurso Wake on LAN, selecione o tipo **Microsoft System Center Virtual Machine Manager** ou **Wake on LAN de PC Remoto**. Para obter mais informações, consulte Wake on LAN.

  Além do tipo de conexão, especifique se você usará ferramentas Citrix (como Machine Creation Services™) ou outras ferramentas para criar VMs.
- Para obter informações especificadas nas páginas **Armazenamento** e **Rede**, consulte Armazenamento do host, Gerenciamento de armazenamento e Seleção de armazenamento.
- Se você tiver uma Licença de Direitos Híbridos e tiver adicionado conexões de host de nuvem pública (por exemplo, AWS), essas conexões serão listadas aqui. Para visualizar essas conexões de host de nuvem pública, atualize o Web Studio vários minutos após adicioná-las.

Acesso Remoto ao PC

Para obter informações sobre implantações de Acesso Remoto para PC, consulte Acesso Remoto para PC.

Se você usar o recurso Wake on LAN, conclua as etapas de configuração no Microsoft System Center Configuration Manager antes de criar o site. Para obter detalhes, consulte Configuration Manager e Wake on LAN de Acesso Remoto para PC.

Criar e gerenciar conexões e recursos

Importante:

A partir do Citrix Virtual Apps and Desktops™ 7 2006, se sua implantação atual usar alguma das seguintes tecnologias, você poderá atualizar sua implantação para a versão atual somente após remover os itens de Fim de Vida (EOL) que usam essas tecnologias.

- vDisks Pessoais (PvDs)
- AppDisks™
- Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic

Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

Observação:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Se você deseja usar conexões de host de nuvem pública em sua implantação, você precisa da Licença de Direitos Híbridos para concluir sua nova instalação ou atualização para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização pausa ou para, e uma mensagem explicativa aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Efeito da Licença de Direitos Híbridos na conexão de host

Existem três cenários em que a conexão de host com os hosts de nuvem pública é afetada com base no direito à Licença de Direitos Híbridos:

- Para criar uma nova conexão de host com os hosts de nuvem pública, você deve ter a Licença de Direitos Híbridos.
- Se você tem a Licença de Direitos Híbridos, mas a licença expirou, as conexões existentes com hosts de nuvem pública são marcadas como não autorizadas e entram em modo de manutenção. Quando as conexões de host existentes estão em modo de manutenção, você não pode fazer o seguinte:
  - Adicionar ou modificar conexões de host
  - Criar catálogo e atualizar imagem
  - Executar ações de energia
- Quando as conexões de host não autorizadas mudam para autorizadas, as conexões de hospedagem existentes são reativadas.

Introdução

Opcionalmente, você pode criar sua primeira conexão com os recursos de hospedagem ao criar um Site. Posteriormente, você pode alterar essa conexão e criar outras conexões. A configuração de uma conexão inclui a seleção do tipo de conexão entre os hipervisores suportados e o armazenamento e a rede que você seleciona dos recursos para essa conexão.

Administradores Somente Leitura podem visualizar detalhes de conexão e recursos. Você deve ser um Administrador Completo para executar tarefas de gerenciamento de conexão e recursos. Para obter detalhes, consulte Administração delegada.

Onde encontrar informações sobre tipos de conexão

Você pode usar as plataformas de virtualização suportadas para hospedar e gerenciar máquinas em seu ambiente Citrix Virtual Apps ou Citrix Virtual Desktops. O artigo Requisitos do sistema lista os tipos suportados.

Para obter detalhes, consulte as seguintes fontes de informação:

- **XenServer (anteriormente Citrix Hypervisor™):**
  - Ambientes de virtualização XenServer.
  - Documentação do XenServer®.
- **Nutanix Acropolis:**
  - Ambientes de virtualização Nutanix.

  - Documentação do Nutanix.

- **VMware:**
  - Ambientes de virtualização VMware.
  - Documentação do produto VMware.
- **Microsoft Hyper-V:**
  - Artigo (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/msscvmm.html) sobre ambientes de virtualização do Microsoft System Center Virtual Machine Manager.
  - Documentação da Microsoft.
- **Conexões de host de nuvem pública (AWS, Google Cloud, Microsoft Azure, soluções de nuvem e parceiros Nutanix e soluções de nuvem e parceiros VMware):** Para obter informações relacionadas a hosts de nuvem pública, consulte Configurar tipo de recurso.

> **Observação:**
>
> As fontes de informação direcionam você para a documentação do Citrix DaaS™. Se você está familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local apresenta várias diferenças. No Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio. As atualizações são lançadas para o serviço aproximadamente a cada quatro semanas. Assim, você pode descobrir que certos recursos disponíveis com o serviço não estão disponíveis na versão local.

Armazenamento do host

Um produto de armazenamento é suportado quando gerenciado por um hipervisor suportado. O Suporte Citrix auxilia esses fornecedores de produtos de armazenamento na solução e resolução de problemas, e documenta esses problemas no centro de conhecimento, conforme necessário.

Ao provisionar máquinas, os dados são classificados por tipo:

- Dados do sistema operacional (SO), que incluem imagens mestre.
- Dados temporários. Esses dados incluem todos os dados não persistentes gravados em máquinas provisionadas por MCS, arquivos de paginação do Windows, dados de perfil de

usuário e quaisquer dados sincronizados com o ShareFile. Esses dados são descartados cada vez que uma máquina é reiniciada.

Fornecer armazenamento separado para cada tipo de dado pode reduzir a carga e melhorar o desempenho em cada dispositivo de armazenamento, aproveitando ao máximo os recursos disponíveis do host. 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 clusterizados do Windows Server 2012 (com ou sem armazenamento anexado), ou um appliance de um fornecedor de armazenamento. O armazenamento central também pode fornecer suas próprias otimizações, como caminhos de controle de armazenamento do hipervisor e acesso direto através de plug-ins de parceiros.

Armazenar dados temporários localmente evita a necessidade de atravessar a rede para acessar o armazenamento compartilhado. Também reduz a carga no dispositivo de armazenamento compartilhado. O armazenamento compartilhado pode ser mais caro, então armazenar dados localmente pode reduzir despesas. Esses benefícios devem ser ponderados em relação à disponibilidade de armazenamento suficiente nos servidores hipervisores.

Ao criar uma conexão, você escolhe um de dois métodos de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local para o hipervisor.

Ao usar armazenamento local em um ou mais hosts XenServer para armazenamento temporário de dados, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter®, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

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 do SO.

Ao selecionar este método, você pode escolher se deseja usar armazenamento local (em servidores no mesmo pool de hipervisores) para dados temporários da máquina. Este método não requer persistência ou tanta resiliência quanto os dados no armazenamento compartilhado, conhecido como *cache de dados temporários*. O disco local ajuda a reduzir o tráfego para o

armazenamento principal do SO. Este disco é limpo após cada reinício da máquina. O disco é acessado através de um cache de memória write-through. Se você usar armazenamento local para dados temporários, o VDA provisionado estará vinculado a um host de hipervisor específico. Se esse host falhar, a VM não poderá iniciar.

Exceção: O Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários em armazenamento local ao usar Volumes de Armazenamento Clusterizados (CSV).

Crie uma conexão para armazenar dados temporários localmente e, em seguida, habilite e configure valores não padrão para o tamanho do disco de cache e o tamanho da memória de cada VM. Os valores padrão são adaptados ao tipo de conexão e são suficientes para a maioria dos casos. Para obter detalhes, consulte Criar catálogos de máquinas.

O hipervisor também pode fornecer tecnologias de otimização por meio do cache de leitura das imagens de disco localmente. Por exemplo, o XenServer oferece o IntelliCache™, que reduz o tráfego de rede para o armazenamento central.

Armazenamento local ao hipervisor

O método de armazenamento local ao hipervisor armazena dados localmente no hipervisor. Com este método, as imagens mestre e outros dados do SO são transferidos para os hipervisores no Site. Este processo ocorre para a criação inicial da máquina e futuras atualizações de imagem. Este processo resulta em tráfego significativo na rede de gerenciamento. As transferências de imagem também consomem muito tempo, e as imagens ficam disponíveis para cada host em um momento diferente.

Criar uma conexão e recursos

Opcionalmente, você pode criar a primeira conexão ao criar o Site. O assistente de criação do Site contém as páginas relacionadas à conexão descritas nas seções a seguir.

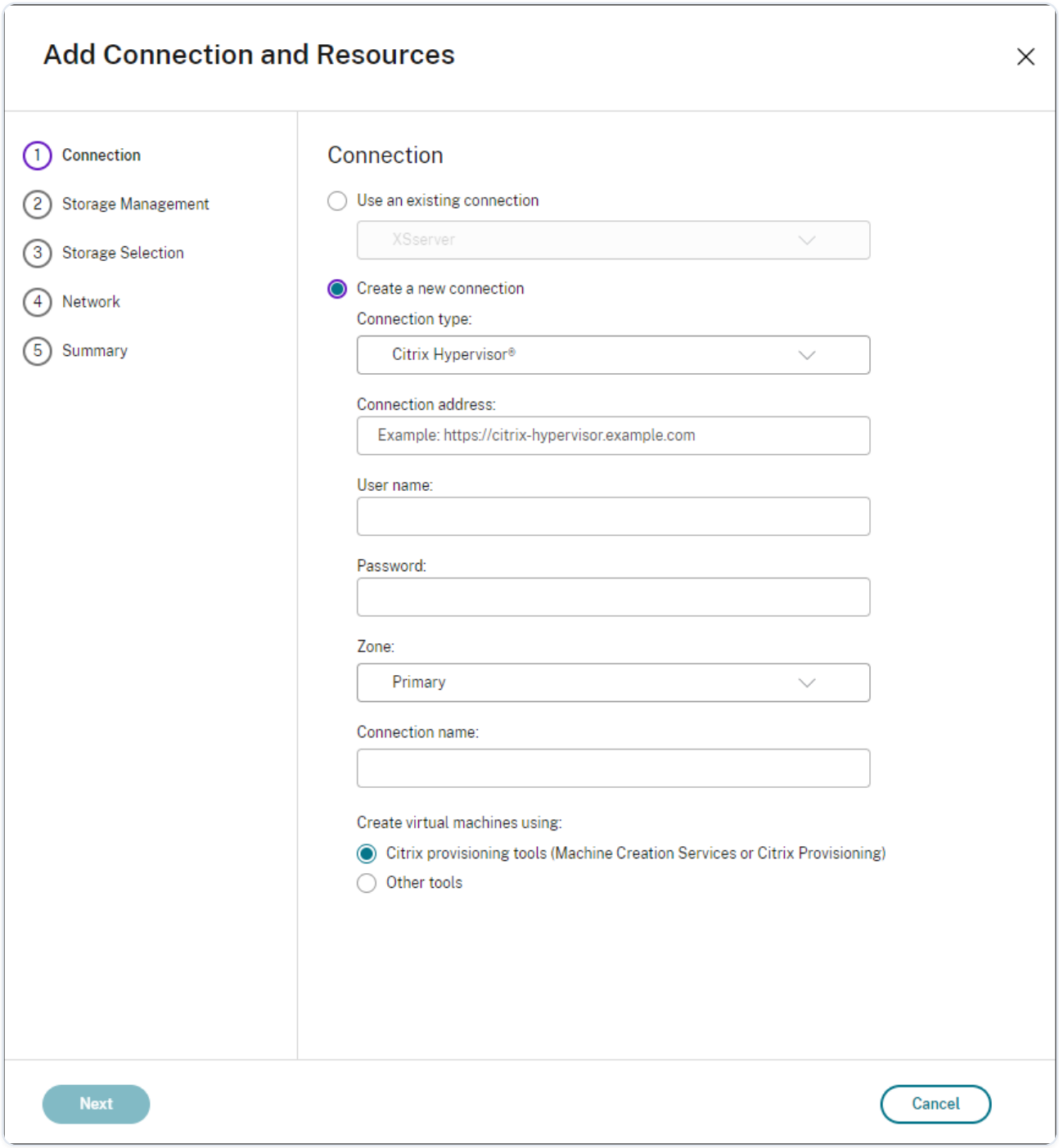
Se você estiver criando uma conexão depois de criar o Site, comece com a etapa 1.

> **Importante:**
>
> Os recursos do host (armazenamento e rede) devem estar disponíveis antes de você criar uma conexão.

1. Faça login no Web Studio.

2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione **Adicionar Conexões e Recursos** na barra de ações.
4. O assistente o guiará pelas seguintes páginas (o conteúdo específico da página depende do tipo de conexão selecionado). Após concluir cada página, clique em **Avançar** até chegar à página **Resumo**.

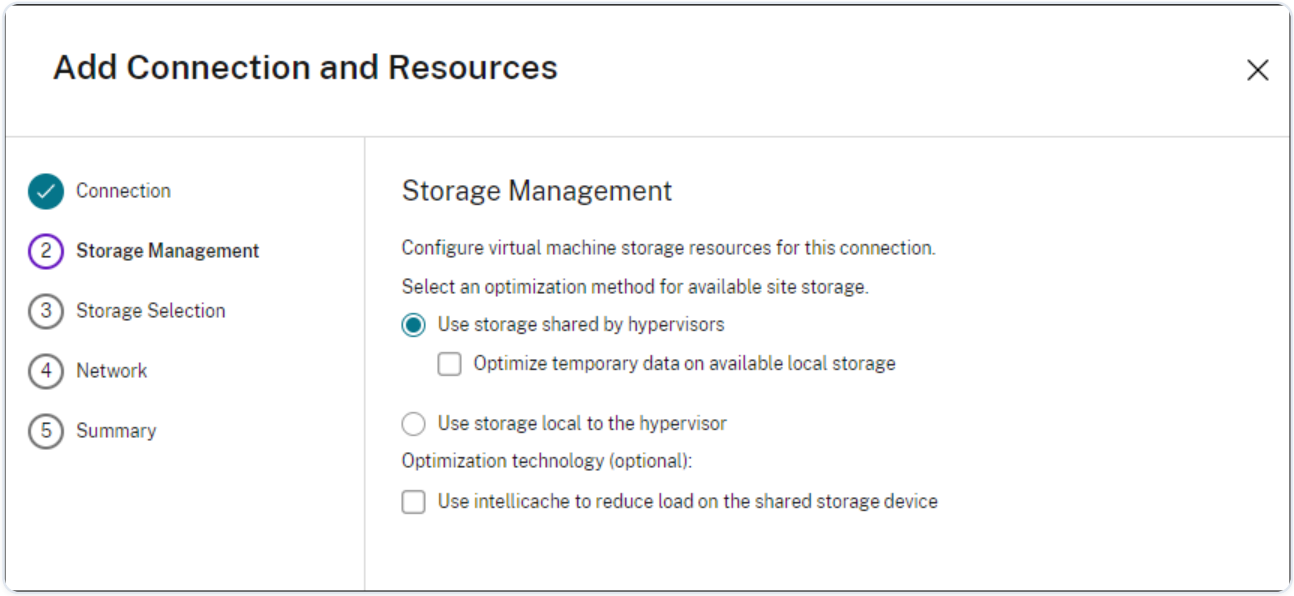
Conexão



Na página **Conexão**:

- Para criar uma conexão, selecione **Criar uma nova Conexão**. Para criar uma conexão com base na mesma configuração de host de uma conexão existente, selecione **Usar uma Conexão existente** e, em seguida, escolha a conexão relevante.
- Selecione o hipervisor que você está usando no campo **Tipo de conexão**. As conexões de host de nuvem pública são listadas na lista suspensa somente se você usar a Licença de Direitos Híbridos. Alternativamente, você pode usar o comando PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true para obter o seguinte:
  - Lista de todos os plugins de hipervisor suportados pela Citrix, incluindo plugins de terceiros.
  - Disponibilidade do plugin do hipervisor. Se o status de disponibilidade for **false**, a possível razão pode ser que o plug-in do hipervisor não esteja instalado corretamente ou você não tenha direito à Licença de Direitos Híbridos.
- Os campos de endereço de conexão e credenciais diferem, dependendo do tipo de conexão selecionado. Insira as informações solicitadas.
- Insira um nome de conexão. Este nome aparece no Web Studio.
- Escolha a ferramenta que você usa para criar máquinas virtuais: ferramentas do Web Studio (como Machine Creation Services™ ou Citrix Provisioning) ou outras ferramentas.

Gerenciamento de armazenamento



Para obter informações sobre tipos e métodos de gerenciamento de armazenamento, consulte Armazenamento do host.

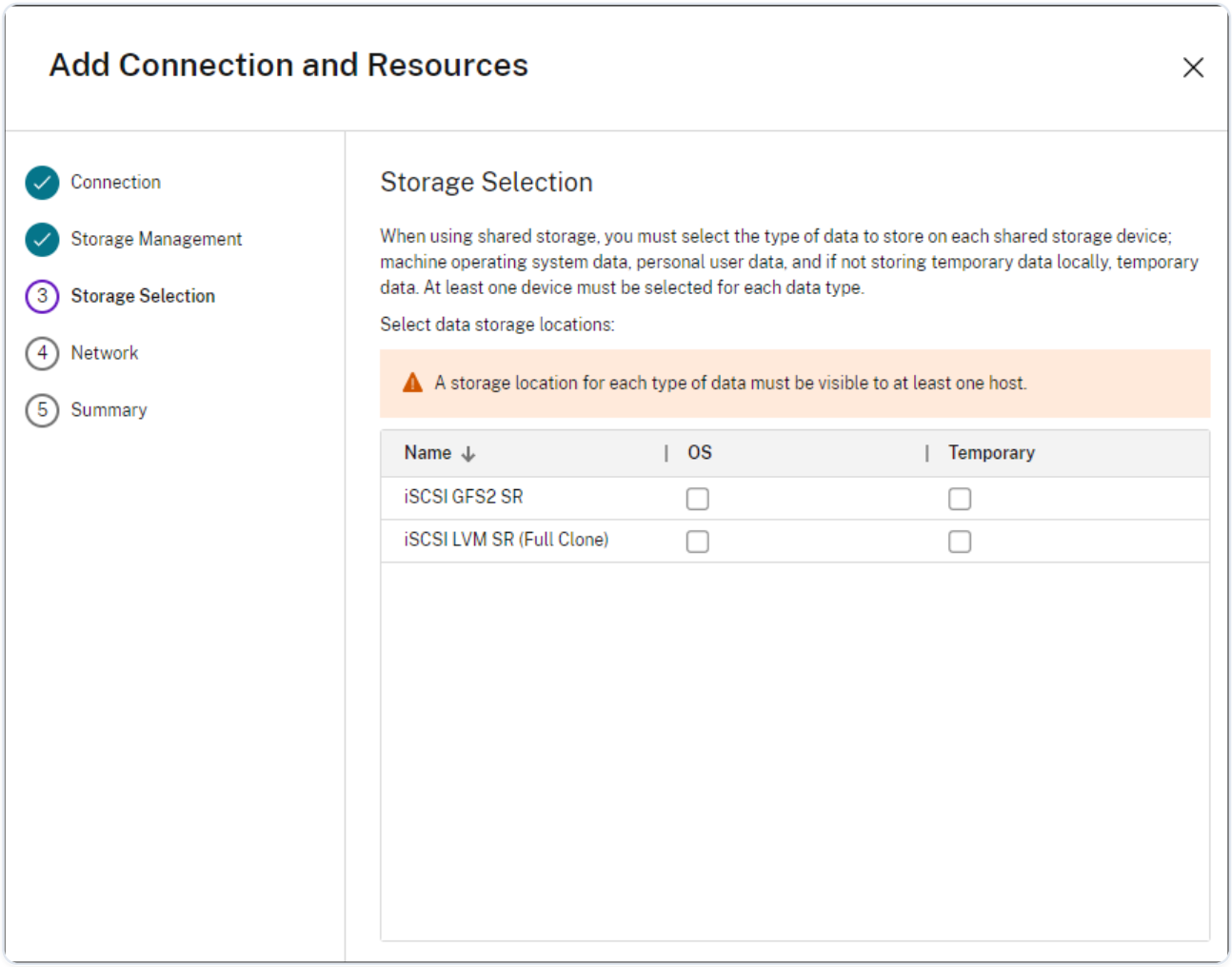
Se você estiver configurando uma conexão com um host Hyper-V ou VMware, navegue até e selecione um nome de cluster. Outros tipos de conexão não solicitam um nome de cluster.

Selecione um método de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local ao hipervisor.

- Se você escolher armazenamento compartilhado por hipervisores, indique se deseja manter dados temporários no armazenamento local disponível. (Você pode especificar tamanhos de armazenamento temporário não padrão nos catálogos de máquinas que usam esta conexão.) **Exceção:** Ao usar Volumes de Armazenamento Clusterizados (CSV), o Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários no armazenamento local. A configuração desse gerenciamento de armazenamento no Web Studio falha.

Se você usa armazenamento compartilhado em um pool XenServer, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Usar IntelliCache para conexões XenServer.

Seleção de armazenamento



Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento do host.

Selecione pelo menos um dispositivo de armazenamento de host para cada tipo de dado disponível. O método de gerenciamento de armazenamento selecionado na página anterior afeta quais tipos de dados estão disponíveis para seleção nesta página. Selecione pelo menos um dispositivo de armazenamento para cada tipo de dado suportado antes de prosseguir para a próxima página do assistente.

A parte inferior da página **Seleção de Armazenamento** contém mais opções de configuração se você escolheu armazenamento compartilhado por hipervisores e ativou **Otimizar dados temporários no armazenamento local disponível** na página anterior. Você pode selecionar quais dispositivos de armazenamento local usar para dados temporários.

O número de dispositivos de armazenamento atualmente selecionados é exibido (no gráfico anterior, "1 dispositivo de armazenamento selecionado"). Ao passar o mouse sobre essa entrada, os nomes dos dispositivos selecionados aparecem.

1. Clique em **Selecionar** para alterar os dispositivos de armazenamento a serem usados.
2. Na caixa de diálogo **Selecionar Armazenamento**, selecione ou desmarque as caixas de seleção do dispositivo de armazenamento e, em seguida, clique em **OK**.

Rede

Na página **Rede**, insira um nome para os recursos. Este nome aparece no Web Studio para identificar a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs usam.

Resumo

Na página **Summary**, revise suas seleções. Quando terminar, clique em **Finish**.

Lembre-se: Armazenar dados temporários localmente permite configurar valores não padrão para o armazenamento de dados temporários ao criar o Catálogo de Máquinas que contém máquinas usando essa conexão. Consulte Criar Catálogos de Máquinas.

Editar configurações de conexão

Não use este procedimento para renomear uma conexão ou para criar uma conexão. Essas conexões são operações diferentes. Altere o endereço somente se a máquina host atual tiver um

novo endereço. Inserir um endereço para uma máquina diferente quebra os Catálogos de Máquinas da conexão.

Você não pode alterar as configurações de **GPU** para uma conexão, porque os Catálogos de Máquinas que acessam esse recurso devem usar uma imagem mestre apropriada e específica para GPU. Crie uma conexão.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
4. Siga as orientações para as configurações disponíveis ao editar uma conexão.
5. Quando terminar, 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.

Página **Connection Properties**:

- Para alterar o endereço e as credenciais da conexão, selecione **Edit settings...** e insira as novas informações.
- Para especificar os servidores de alta disponibilidade para uma conexão XenServer, selecione **Editar servidores...** e selecione os servidores. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o XenServer caso o mestre do pool falhe.

> **Observação:**
>
> 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.

Página **Advanced**:

- Para um tipo de conexão Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN, que é usado com o Acesso Remoto a PC, insira as informações de **ConfMgr Wake Proxy**, pacotes mágicos e transmissão de pacotes.
- 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 iniciem

ao mesmo tempo. Cada tipo de conexão tem valores padrão específicos que são apropriados para a maioria dos casos e não devem ser alterados.

- A configuração **Simultaneous actions (all types)** especifica dois valores: um número absoluto máximo que pode ocorrer simultaneamente nesta conexão e uma porcentagem máxima de todas as máquinas que usam esta conexão. Você deve especificar valores absolutos e percentuais. O limite real aplicado é o menor dos valores.

  Por exemplo, em uma implantação com 34 máquinas, se **Ações simultâneas (todos os tipos)** for definido como um valor absoluto de 10 e um valor percentual de 10, o limite real aplicado é 3 (ou seja, 10% de 34 arredondado para o número inteiro mais próximo, que é menor que o valor absoluto de 10 máquinas).
- O **Número máximo de novas ações por minuto** é um número absoluto. Não há valor percentual.
- Insira informações no campo **Opções de conexão** somente sob a orientação de um representante do Suporte Citrix ou instruções explícitas da documentação.

Página **Locatários Compartilhados**:

Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura desta 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** para o aplicativo associado a esta conexão. Com essas informações, você pode autenticar no Azure. Recomendamos que você altere as chaves regularmente para garantir a segurança.
- Especifique locatários e assinaturas compartilhados. Você pode adicionar até oito locatários compartilhados. Para cada locatário, você pode adicionar até oito assinaturas.
- Clique em **Salvar** e **Aplicar** quando terminar.

Insira informações no campo **Opções de conexão** 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 **Hospedagem**.
2. Selecione os recursos de destino na conexão e, em seguida, selecione **Editar Rede** na barra de ações.

3. Selecione uma ou mais redes para as máquinas virtuais usarem.
4. Clique em **Salvar** para salvar suas alterações e sair.

Ativar ou desativar o modo de manutenção para uma conexão

Ativar o modo de manutenção para uma conexão impede que qualquer nova ação de energia afete qualquer máquina armazenada na conexão. Os usuários não podem se conectar a uma máquina quando ela está no modo de manutenção. Se os usuários já estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão. Para ativar o modo de manutenção, selecione **Ativar Modo de Manutenção** na barra de ações. Para desativar o modo de manutenção, selecione **Desativar Modo de Manutenção**.

Você também pode ativar ou desativar o modo de manutenção para máquinas individuais. Além disso, você pode ativar ou desativar o modo de manutenção para máquinas em Catálogos de Máquinas ou Grupos de Entrega.

Excluir uma conexão

A exclusão de uma conexão pode resultar na exclusão de um grande número de máquinas e na perda de dados. Certifique-se de que os dados do usuário nas máquinas afetadas estejam com backup ou não sejam mais necessários.

Antes de excluir uma conexão, certifique-se de que:

- Todos os usuários fizeram logoff das máquinas armazenadas na conexão.
- Nenhuma sessão de usuário desconectada está em execução.
- O modo de manutenção está ativado para máquinas agrupadas e dedicadas.
- Todas as máquinas nos Catálogos de Máquinas usados pela conexão são desligadas.

Um Catálogo de Máquinas se torna inutilizável quando você exclui uma conexão que é referenciada por esse catálogo. Se esta conexão for referenciada por um catálogo, você tem a opção de excluir o catálogo. Antes de excluir um catálogo, certifique-se de que ele não seja usado por outras conexões.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.

3. Selecione a conexão e então selecione **Excluir Conexão** na barra de ações.
4. Se esta conexão tiver máquinas armazenadas nela, será perguntado se as máquinas devem ser excluídas. Se elas forem excluídas, especifique o que deve ser feito com as contas de computador do Active Directory associadas.

Renomear ou testar uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Renomear Conexão** ou **Testar Conexão** na barra de ações.

Exibir detalhes da máquina em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Exibir Máquinas** na barra de ações.

O painel superior lista as máquinas acessadas pela conexão. Selecione uma máquina para ver seus detalhes no painel inferior. Os detalhes da sessão também são fornecidos para sessões abertas.

Use o recurso de pesquisa para encontrar máquinas rapidamente. Selecione uma pesquisa salva na lista na parte superior da janela ou crie uma pesquisa. Você pode pesquisar digitando todo ou parte do nome da máquina, ou pode construir uma expressão para usar em uma pesquisa avançada. Para construir uma expressão, clique em **Desdobrar** e, em seguida, selecione nas listas de propriedades e operadores.

Gerenciar máquinas em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione uma conexão e, em seguida, selecione **Exibir Máquinas** no painel **Ação**.
4. Selecione uma das seguintes opções na barra de ações. Algumas ações não estão disponíveis, dependendo do estado da máquina e do tipo de host da conexão.

AÇÃO	DESCRIÇÃO
Iniciar	Inicia a máquina se ela estiver desligada ou suspensa.
Suspender	Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
Desligar	Solicita ao sistema operacional que seja desligado.
Forçar desligamento	Desliga a máquina à força e atualiza a lista de máquinas.
Reiniciar	Solicita ao sistema operacional que seja desligado e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a área de trabalho permanecerá em seu estado atual.
Habilitar modo de manutenção	Interrompe temporariamente as conexões com uma máquina. Os usuários não podem se conectar a uma máquina neste estado. Se os usuários estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff. (Você também pode ativar ou desativar o modo de manutenção para todas as máquinas acessadas por meio de uma conexão, conforme descrito acima.)
Remover do Grupo de Entrega	Remover uma máquina de um Grupo de Entrega não a exclui do Catálogo de Máquinas que o Grupo de Entrega usa. Você só pode remover uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver removendo a máquina.
Excluir	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

AÇÃO	DESCRIÇÃO
	todos os dados do usuário estejam com backup ou não sejam mais necessários. Você só pode excluir uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver excluindo a máquina.

Para ações que envolvem o desligamento da máquina, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar dados de sistema operacional e temporários para VMs que usam uma conexão. Você também pode especificar quais servidores usar para o armazenamento de cada tipo de dado.

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione a conexão e, em seguida, selecione **Editar Armazenamento** na barra de ações.
4. No painel esquerdo, selecione o tipo de dados: sistema operacional ou temporário.
5. Marque ou desmarque as caixas de seleção para um ou mais dispositivos de armazenamento para o tipo de dados selecionado.
6. Clique em **OK**.

Cada dispositivo de armazenamento na lista inclui seu nome e status de armazenamento. Os valores de status de armazenamento válidos são:

- **Em uso:** O armazenamento está sendo usado para criar máquinas.
- **Substituído:** O armazenamento está sendo usado apenas para máquinas existentes. Nenhuma máquina nova é adicionada neste armazenamento.
- **Não em uso:** O armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo que está atualmente **Em uso**, seu status muda para **Substituído**. As máquinas existentes continuarão a usar esse dispositivo de

armazenamento (e podem gravar dados nele), portanto, é possível que esse local fique cheio mesmo depois de parar de ser usado para criar máquinas.

Excluir, renomear ou testar recursos

1. Faça login no Web Studio.
2. Selecione **Hospedagem** no painel esquerdo.
3. Selecione o recurso e, em seguida, selecione a entrada apropriada na barra de ações: **Excluir Recursos**, **Renomear Recursos** ou **Testar Recursos**.

Detectar recursos órfãos do Azure

Recursos órfãos são recursos não utilizados presentes no sistema e podem levar a despesas desnecessárias.

Este recurso permite detectar os recursos órfãos do Azure nos hosts do seu site Citrix Virtual Apps and Desktops.

Siga as etapas no Web Studio:

1. Em **Gerenciar**, selecione **Hospedagem** no painel esquerdo.
2. Selecione uma conexão e, em seguida, selecione **Detectar Recursos Órfãos** na barra de ações. A caixa de diálogo **Detectar Recursos Órfãos** exibe o relatório de recursos órfãos.
3. Para visualizar o relatório de recursos órfãos, selecione **Visualizar Relatório**.

Alternativamente, você pode detectar recursos órfãos do Azure usando o PowerShell. Para obter mais informações, consulte Recuperar uma lista de recursos órfãos.

Para entender as razões por trás dos recursos órfãos e aprender como prosseguir, consulte Gerenciar recursos órfãos do Azure de forma eficiente com o Citrix.

Temporizadores de conexão

Você pode usar as configurações de política para configurar três temporizadores de conexão:

- **Temporizador máximo de conexão:** Determina a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop virtual. Use as configurações de política **Temporizador de conexão de sessão** e **Intervalo do temporizador de conexão de sessão**.
- **Temporizador de inatividade da conexão:** Determina por quanto tempo uma conexão ininterrupta de dispositivo de usuário com um desktop virtual é mantida se não houver entrada

do usuário. Use as configurações de política **Temporizador de inatividade da sessão** e **Intervalo do temporizador de inatividade da sessão**.

- **Temporizador de desconexão:** Determina por quanto tempo um desktop virtual desconectado e bloqueado pode permanecer bloqueado antes que a sessão seja encerrada. Use as configurações de política **Temporizador de sessão desconectada** e **Intervalo do temporizador de sessão desconectada**.

Ao atualizar qualquer uma dessas configurações, certifique-se de que elas sejam consistentes em toda a sua implantação.

Consulte a documentação de configurações de política para obter mais informações.

Recuperar uma lista de recursos órfãos

Você pode obter uma lista de recursos órfãos que são criados pelo MCS, mas não são mais rastreados pelo MCS. Isso é atualmente aplicável a ambientes Azure. Para obter a lista, você pode usar comandos PowerShell. Você pode filtrar usando conexões.

> **Observação:**
>
> - O comando PowerShell é rejeitado se qualquer provisionamento ou atualização de imagem estiver 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 o valor true a esse recurso, o recurso será ignorado ao detectar recursos órfãos.

Limitações

- Somente um administrador integrado com função de administrador completo ou administrador de nuvem 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.

Para exibir a lista de recursos órfãos:

1. Abra uma janela do **PowerShell**.

2. Execute os seguintes comandos:

    a. Obtenha o uid da conexão. O uid da conexão é o valor do atributo HypervisorConnectionUid.

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. Obtenha a lista de recursos órfãos.

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

Para exibir a lista de recursos órfãos de um ID de assinatura:

1. Abra uma janela do **PowerShell**.
2. Execute os seguintes comandos:

    a. Encontre o uid da conexão usando o ID da assinatura. O uid da conexão é o valor do atributo HypervisorConnectionUid.

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. Obter a lista de recursos órfãos:

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

> **Observação:**
>
> Verifique os recursos cuidadosamente antes de excluí-los.

Próximos passos

Para obter informações sobre a conexão com tipos de host específicos, consulte:

- Conexão com AWS
- Conexão com XenServer

- Conexão com ambientes de nuvem do Google
- Conexão com Microsoft Azure
- Conexão com Microsoft System Center Virtual Machine Manager
- Conexão com Nutanix
- Conexão com soluções de nuvem e parceiros Nutanix
- Conexão com VMware
- Conexão com soluções de nuvem e parceiros VMware

Se você estiver no processo de implantação inicial, crie um catálogo de máquinas.

Conexão com a AWS

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem AWS.

> **Observação:**

> Antes de criar uma conexão com a AWS, você precisa primeiro concluir a configuração da sua conta AWS como um local de recurso. Consulte Ambientes de nuvem AWS.

Criar uma conexão

Ao criar uma conexão a partir do Web Studio:

- Você deve fornecer os valores da chave de API e da chave secreta. Você pode exportar o arquivo de chave contendo esses valores da AWS e depois importá-los. Você também deve fornecer a região, zona de disponibilidade, nome da VPC, endereços de sub-rede, nome de domínio, nomes de grupos de segurança e credenciais.
- 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. Certifique-se de que você está usando arquivos de credenciais do AWS Identity Access Management (IAM).

> **Observação:**

> 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 firewall e certifique-se de que o seguinte endereço pode ser contatado: `https://*.amazonaws.com`.

Valores padrão de conexão de host

Ao criar conexões de host em ambientes de nuvem AWS, os seguintes valores padrão são exibidos:

OPÇÃO	ABSOLUTO	PORCENTAGEM
Ações simultâneas (todos os tipos)	125	100
Máximo de novas ações por minuto	125	

O MCS suporta 100 operações de provisionamento simultâneas máximas por padrão.

URL do endpoint de serviço

URL do endpoint de serviço da zona padrão

Ao usar o MCS, uma nova conexão AWS é adicionada com uma chave de API e um segredo de API. Com essas informações, juntamente com a conta autenticada, o MCS consulta a AWS para as zonas suportadas usando a chamada de API AWS DescribeRegions EC2. A consulta é feita usando uma URL de endpoint de serviço EC2 genérica `https://ec2.amazonaws.com/`. Use o MCS para selecionar a zona para a conexão na lista de zonas suportadas. A URL de endpoint de serviço AWS preferencial é selecionada automaticamente para a zona. No entanto, depois de criar a URL do endpoint de serviço, você não pode mais definir ou modificar a URL.

Definir permissões do IAM

Use as informações nesta seção para definir permissões IAM para Citrix Virtual Apps and Desktops na AWS. O serviço IAM da Amazon permite contas com vários usuários, que podem ser ainda mais organizados em grupos. Esses usuários podem possuir diferentes permissões para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões IAM, consulte a referência de política JSON do IAM.

Para aplicar a política de permissões do IAM a um novo grupo de usuários:

1. Faça login no console de gerenciamento da AWS e selecione o **serviço IAM** na lista suspensa.
2. Selecione **Criar um Novo Grupo de Usuários**.
3. Digite um nome para o novo grupo de usuários e selecione **Continuar**.
4. Na página **Permissões**, escolha **Política Personalizada**. Selecione **Selecionar**.
5. Digite um nome para a **política de Permissões**.
6. Na seção **Documento de Política**, insira as permissões relevantes.

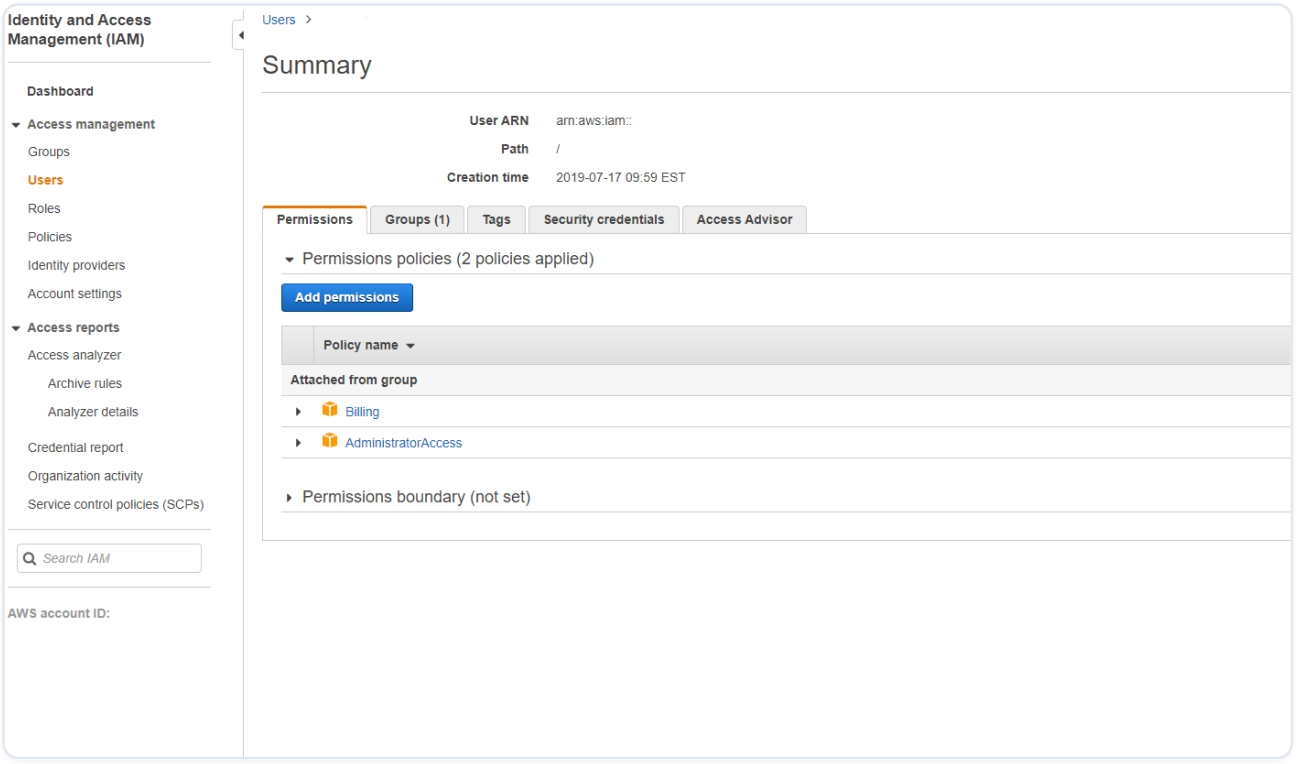
Após inserir as informações da política, selecione **Continuar** para completar o grupo de usuários. Os usuários do grupo recebem permissões para executar apenas as ações necessárias para o Citrix Virtual Apps and Desktops.

> **Importante:**
>
> Use o texto da política fornecido no exemplo anterior para listar as ações que o Citrix Virtual Apps and Desktops usa para executar ações dentro de uma conta AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar restrições adicionais aos recursos.

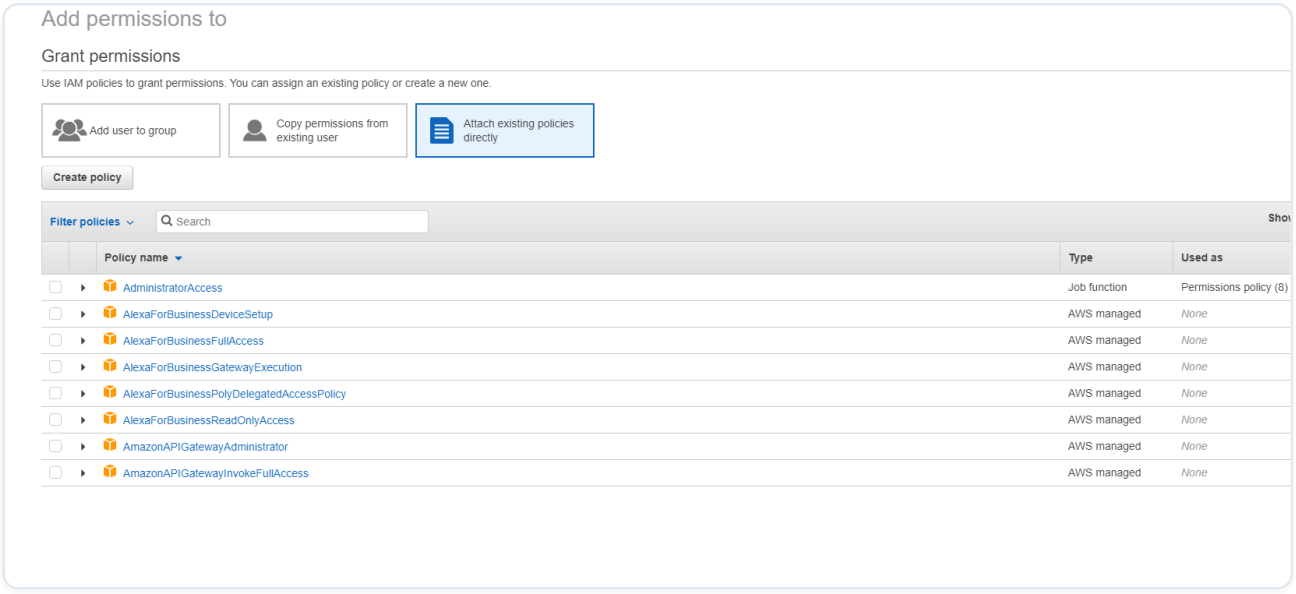
Definir permissões IAM

Defina as permissões na seção **IAM** do Console de Gerenciamento da AWS:

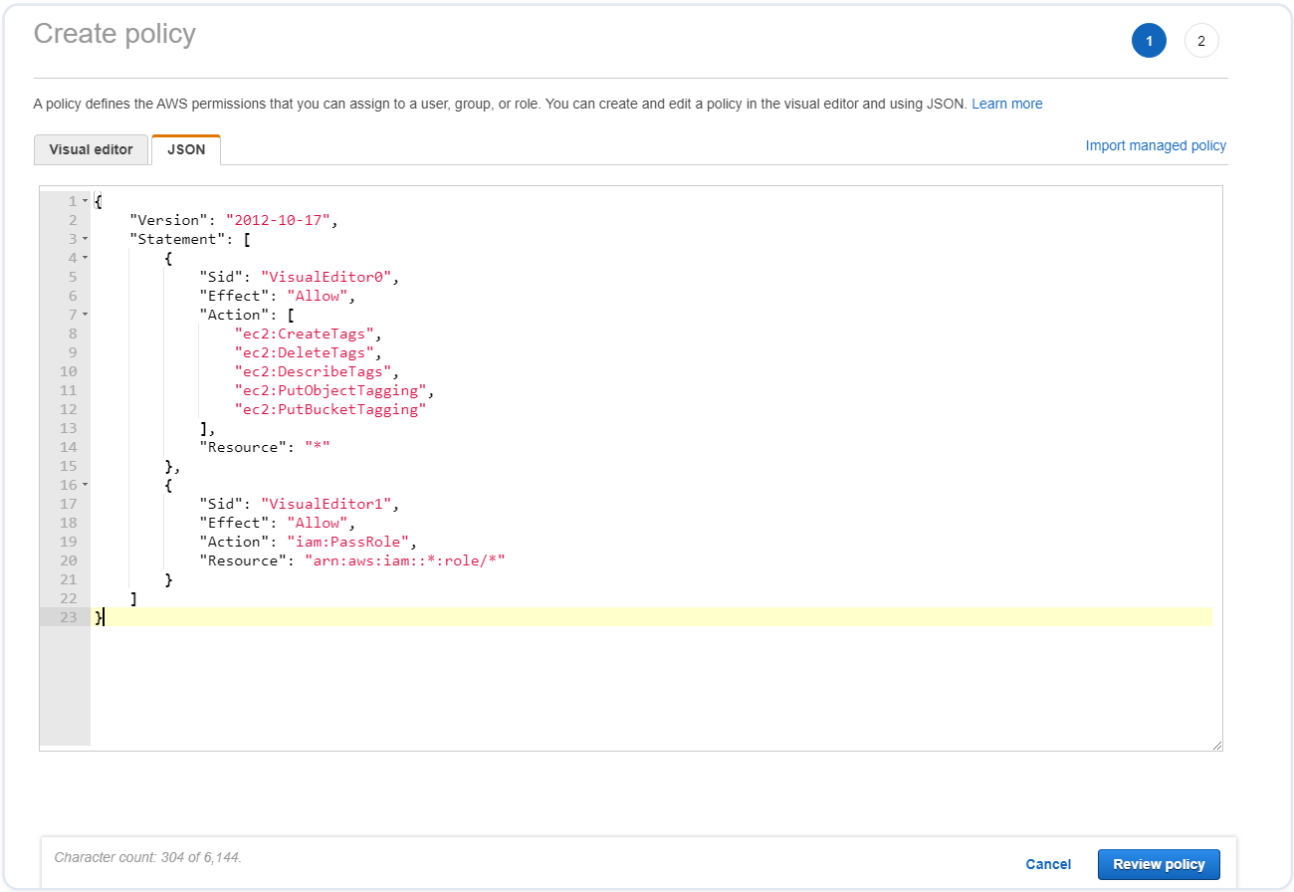
1. No painel **Resumo**, selecione a guia **Permissões**.
2. Selecione **Adicionar permissões.**



Na tela **Adicionar Permissões a**, conceda permissões:



Use o seguinte como exemplo na guia **JSON**:



Dica:

O exemplo JSON mencionado pode não incluir todas as permissões para o seu ambiente. Consulte Como Definir Permissões de Gerenciamento de Acesso de Identidade Executando Citrix Virtual Apps and Desktops no AWS para mais informações.

Permissões AWS necessárias

Esta seção contém a lista completa de permissões do AWS.

Observação:

A permissão *iam:PassRole* é necessária apenas para **role_based_auth**.

Criando uma conexão de host

Uma nova conexão de host é adicionada usando as informações do AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Gerenciamento de energia de VMs

As instâncias de máquina são 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",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Criar, atualizar ou excluir VMs

Um catálogo de máquinas é criado, atualizado ou excluído com VMs provisionadas como instâncias AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2: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:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Observação:

A seção EC2 relacionada a grupos de segurança é necessária apenas se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.

UPLOAD E DOWNLOAD DIRETO DE DISCO

O upload direto de disco elimina o requisito de volume worker para provisionamento de catálogo de máquinas e, em vez disso, usa APIs públicas fornecidas pela AWS. Essa funcionalidade reduz o custo associado a contas de armazenamento extras e a complexidade de manter as operações de volume worker.

Observação:

O suporte para volume worker está obsoleto.

As seguintes permissões devem ser adicionadas à política:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

Importante:

- Você pode adicionar uma VM a catálogos de máquinas existentes sem qualquer operação de volume worker, como AMI de volume worker e VM de volume worker.
- Se você excluir um catálogo existente que usava volume worker anteriormente, todos os artefatos, incluindo os relacionados ao volume worker, serão excluídos.

Criptografia EBS de volumes criados

O EBS pode criptografar automaticamente volumes recém-criados se a AMI for criptografada, ou se o EBS estiver configurado para criptografar todos os novos volumes. No entanto, para implementar a funcionalidade, as seguintes permissões devem ser incluídas na política do IAM.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }
```

```
    ]

}
```

Observação:

As permissões podem ser limitadas a chaves específicas, incluindo um bloco de Recurso e Condição a critério do usuário. Por exemplo, **Permissões KMS com Condição**:

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

A seguinte declaração de política de chave é a política de chave padrão completa para chaves KMS que é necessária para permitir que a conta use políticas do IAM para delegar permissão para todas as ações (kms:*) na chave KMS.

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

Para mais informações, consulte documentação oficial do AWS Key Management Service.

Autenticação baseada em função do IAM

As seguintes permissões são adicionadas para suportar a autenticação baseada em função.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

Política de permissões mínimas do IAM

O JSON a seguir pode ser usado para todos os recursos atualmente suportados. Você pode criar conexões de host, criar, atualizar ou excluir VMs e fazer gerenciamento de energia usando esta política. A política pode ser aplicada aos usuários conforme explicado nas seções Definir permissões IAM ou você também pode usar autenticação baseada em função usando a chave de segurança e a chave secreta **role_based_auth**.

Importante:

Para usar **role_based_auth**, primeiro configure a função IAM desejada em todos os Delivery Controllers em nosso site. Usando o Web 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 então usa 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:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
```

```
    ]
}
```

Observação:

- A seção EC2 relacionada a SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.
- A seção KMS é necessária apenas ao usar a criptografia de volume EBS.
- A seção de permissão iam:PassRole é necessária apenas para **role_based_auth**.
- Permissões específicas em nível de recurso podem ser adicionadas em vez de acesso total, com base em seus requisitos e ambiente. Consulte os documentos da AWS Demystifying EC2 Resource-Level Permissions e Access management for AWS resources para obter mais detalhes.

Validar permissões na conexão do host

Você pode validar as permissões em uma conexão de host para realizar tarefas relacionadas à criação e gerenciamento de catálogos de máquinas MCS. Essa implementação ajuda você a descobrir as permissões ausentes necessárias para diferentes cenários, como criação, exclusão e atualização de VMs, gerenciamento de energia de VMs e criptografia EBS, com antecedência, para que você possa evitar ser bloqueado em momentos críticos.

Você pode validar as permissões em uma conexão de host usando o comando PowerShell `Test-HypHypervisorConnection`. O resultado do comando é capturado como uma lista, onde cada item da lista é dividido em três seções.

- Categoria: A ação ou tarefa que um usuário pode realizar para criar e gerenciar um catálogo de máquinas MCS.
- Ação Corretiva: A etapa que um administrador deve realizar para resolver uma discrepância de permissões ausentes dos usuários.
- Permissão ausente: A lista de permissões ausentes para uma categoria.

Para validar as permissões, faça o seguinte:

1. Crie uma conexão de host com a AWS.
2. Abra uma janela do PowerShell no host do Delivery Controller™.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Execute o seguinte comando para verificar se você tem as permissões necessárias para consultar suas permissões.

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
```

5. Depois de adicionar as permissões ausentes necessárias para consultar suas permissões, execute o seguinte comando para verificar se você tem permissões nas seguintes categorias:
   - Criar Atualizar excluir
   - Gerenciamento de Energia
   - Criptografia EBS

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:
\Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
"" -CustomProperties ""
```

Para mais informações sobre como adicionar permissões, consulte Definir permissões IAM.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do AWS, consulte Criar um catálogo AWS

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com XenServer®

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de virtualização XenServer.

> **Observação:**

> Antes de criar uma conexão com o XenServer, você precisa primeiro concluir a configuração da sua conta XenServer como um local de recurso. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/install-prepare/xenserver.html).

Criar uma conexão com o XenServer

Ao criar uma conexão com o XenServer (anteriormente Citrix Hypervisor™), você deve fornecer as credenciais para um usuário VM Power Admin ou de nível superior.

A Citrix recomenda usar HTTPS para proteger as comunicações com o XenServer. Para usar HTTPS, você deve substituir o certificado SSL padrão instalado no XenServer.

Você pode configurar alta disponibilidade se ela estiver habilitada no servidor XenServer. Para versões do Citrix Virtual Apps and Desktops anteriores à 2507 LTSR, você não pode instalar um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor.

Você pode selecionar um tipo e grupo de GPU, ou pass-through, se o XenServer suportar vGPU. A exibição indica se a seleção possui recursos de GPU dedicados.

Ao usar armazenamento local em um ou mais hosts XenServer para armazenamento temporário de dados, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter®, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

Você pode usar o Citrix Provisioning (anteriormente Provisioning Services) e o Machine Creation Services™ (MCS) para provisionar:

- BIOS herdado para VMs de SO de Desktop ou Servidor suportadas.
- UEFI para VMs de SO de Desktop ou Servidor suportadas, incluindo Secure Boot.

> **Nota:**
>
> Permissões de operador de pool ou superiores são necessárias ao configurar o MCS.

Usar IntelliCache™ para conexões XenServer

Usando o IntelliCache, as implantações de VDI hospedadas são mais econômicas porque você pode usar uma combinação de armazenamento compartilhado e armazenamento local. Isso melhora o desempenho e reduz o tráfego de rede. O armazenamento local armazena em cache a

imagem mestre do armazenamento compartilhado, o que reduz o número de leituras no armazenamento compartilhado. Para desktops compartilhados, as gravações nos discos de diferenciação são gravadas no armazenamento local no host e não no armazenamento compartilhado.

- O armazenamento compartilhado deve ser NFS ao usar o IntelliCache.
- A Citrix recomenda que você use um dispositivo de armazenamento local de alto desempenho para garantir a transferência de dados mais rápida possível.

Para usar o IntelliCache, você deve habilitá-lo neste produto e no XenServer.

- Ao instalar o XenServer, selecione **Habilitar provisionamento dinâmico (Armazenamento otimizado para Desktops Virtuais)**. A Citrix não oferece suporte a pools mistos de servidores que têm o IntelliCache habilitado e servidores que não o têm. Para obter mais informações, consulte a documentação do XenServer.
- No Citrix Virtual Apps and Desktops™, o IntelliCache está desabilitado por padrão. Você pode alterar a configuração apenas ao criar uma conexão XenServer; você não pode desabilitar o IntelliCache posteriormente. Ao adicionar uma conexão XenServer:
  - Selecione **Compartilhado** como o tipo de armazenamento.
  - Selecione a caixa de seleção **Usar IntelliCache**.

Permissões necessárias do XenServer

As permissões do XenServer são baseadas em função (RBAC). O recurso Controle de Acesso Baseado em Função (RBAC) no XenServer permite atribuir usuários, funções e permissões para controlar quem tem acesso ao seu XenServer e quais ações eles podem executar. O sistema RBAC do XenServer mapeia um usuário (ou um grupo de usuários) para funções definidas (um conjunto nomeado de permissões). As funções têm permissões XenServer associadas para executar certas operações.

Para obter mais informações, consulte Controle de acesso baseado em função.

A hierarquia de funções, em ordem crescente de permissões, é: Somente Leitura → Operador de VM → Administrador de VM → Administrador de Energia de VM → Operador de Pool → Administrador de Pool.

A seção a seguir resume a função mínima necessária para cada tarefa de provisionamento.

Criando uma conexão de host

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Adicionar uma conexão de host usando as informações obtidas do XenServer	Somente leitura
Visualizar usuários e suas funções atribuídas	Somente leitura

Gerenciamento de energia de VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Ligar ou desligar as VMs	Operador de VM

Criar, atualizar ou excluir VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Adicionar ou remover VMs de agendamentos de snapshots existentes	Administrador de energia de VM
Adicionar, modificar, excluir agendamentos de snapshots	Operador de Pool
Publicar imagem mestre	Operador de Pool (Requer bloqueio de porta de switch)
Criar um catálogo de máquinas	Operador de Pool: Requer bloqueio de porta de switch
Adicionar ou remover VMs (VMs não habilitadas para GPU)	Administrador de VM
Adicionar ou remover VMs (VMs habilitadas para GPU)	Operador de Pool
Adicionar, remover ou configurar disco virtual ou dispositivos de CD	Administrador de VM
Gerenciar Tags	Operador de VM

Para obter mais informações sobre funções e permissões RBAC, consulte funções e permissões RBAC.

Para obter informações sobre o bloqueio de porta de switch, consulte Usar bloqueio de porta de switch.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do XenServer, consulte Criar um catálogo do XenServer

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com ambientes de nuvem do Google

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

> **Nota:**
>
> Antes de criar uma conexão com ambientes de nuvem do Google, você precisa primeiro concluir a configuração da sua conta do Google Cloud como um local de recurso. Consulte Ambientes do Google Cloud.

Adicionar uma conexão

Siga as orientações em Criar uma conexão e recursos. A descrição a seguir o orienta na configuração de uma conexão de hospedagem:

1. Em **Gerenciar > Configuração**, selecione **Hospedagem** no painel esquerdo.
2. Selecione **Adicionar Conexão e Recursos** na barra de ações.
3. Na página **Conexão**, selecione **Criar uma nova Conexão** e **ferramentas de provisionamento Citrix™**, e então selecione **Avançar**.
    - **Tipo de conexão**. Selecione **Google Cloud** no menu.
    - **Nome da conexão**. Digite um nome para a conexão.
4. Na página **Região**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Avançar**.

5. Na página **Rede**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Avançar**. O nome do recurso ajuda a identificar a combinação de região e rede. Redes virtuais com o sufixo *(Compartilhado)* anexado ao seu nome representam VPCs compartilhadas. Se você configurar uma função IAM no nível da sub-rede para uma VPC compartilhada, apenas sub-redes específicas da VPC compartilhada aparecerão na lista de sub-redes.

   > **Nota:**
   >
   > - O nome do recurso pode conter 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

6. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir** para sair da janela **Adicionar Conexão e Recursos**.

Após 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 sob a conexão. Para fazer isso, selecione o recurso sob a conexão e, em seguida, selecione a opção aplicável na barra de ações.

URLs de endpoint de serviço

Você deve ter acesso às seguintes URLs:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Projetos do Google Cloud

Existem basicamente dois tipos de projetos do Google Cloud:

- Projeto de provisionamento: Neste caso, a conta de administrador atual é proprietária das máquinas provisionadas no projeto. Este projeto também é conhecido como projeto local.
- Projeto VPC Compartilhada: Projeto no qual as máquinas criadas no projeto de provisionamento usam a VPC do projeto VPC Compartilhada. A conta de administrador usada para o projeto de provisionamento tem permissões limitadas neste projeto, especificamente, apenas permissões para usar a VPC.

Criar um ambiente seguro para o tráfego gerenciado do GCP

Você pode permitir o acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aprimora a segurança para manipular dados confidenciais. Para conseguir isso, você pode fazer uma das seguintes opções:

- Inclua as seguintes regras de entrada dos controles de serviço da VPC para a Conta de Serviço do Cloud Build. Se você seguir esta etapa, não siga as etapas abaixo para criar um ambiente seguro para o tráfego gerenciado do GCP.

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

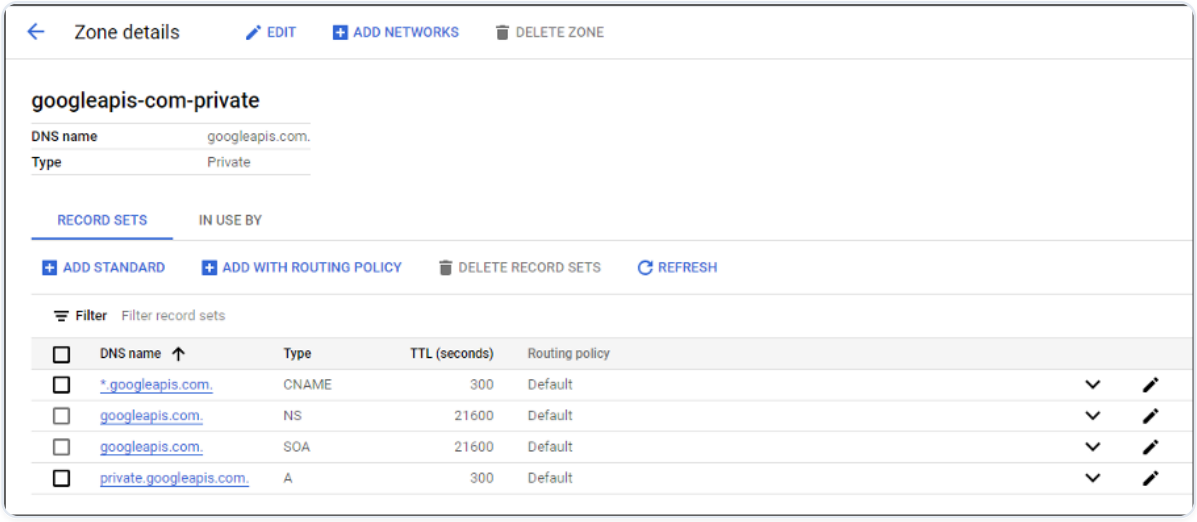
Service name: All services
```

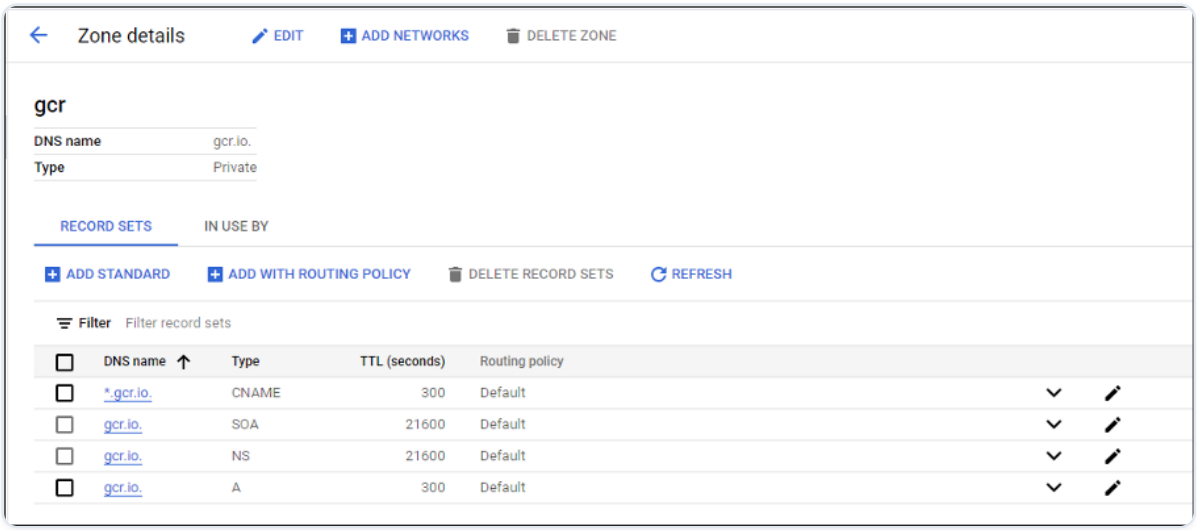
- Se você estiver usando um pool de trabalhadores privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter informações sobre o pool de trabalhadores privado, consulte Visão geral dos pools privados.

Requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP

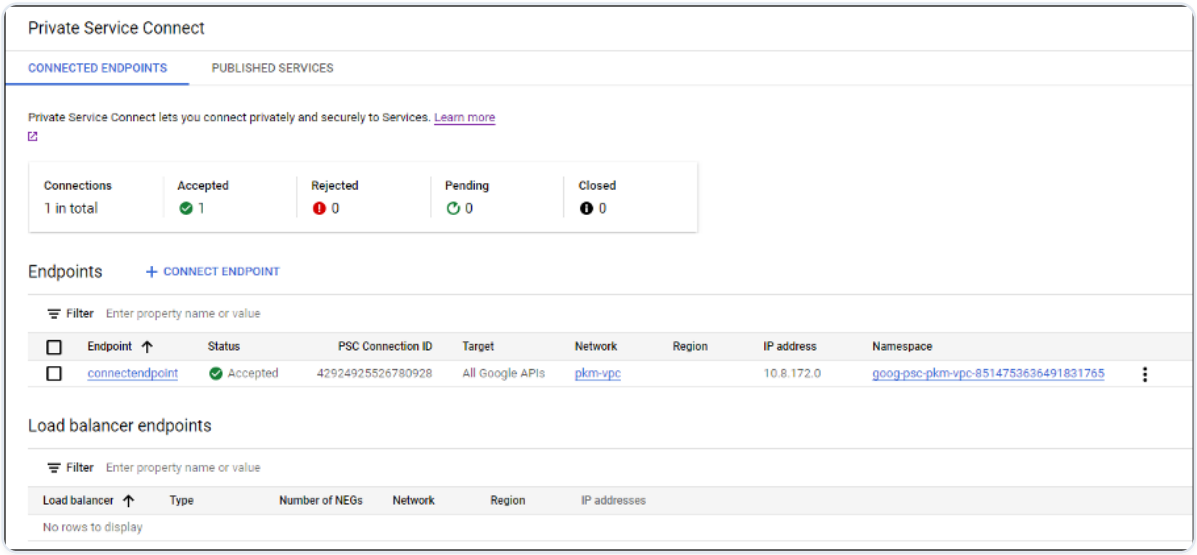
Os requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP são:

- Certifique-se de que a conexão de hospedagem esteja no modo de manutenção ao atualizar as propriedades personalizadas.
- Para usar pools de trabalhadores privados, as seguintes alterações são necessárias:
  - Para a Conta de Serviço do Citrix Cloud™, adicione as seguintes funções IAM:
    - Conta de Serviço do Cloud Build
    - Administrador de Instância de Computação
    - Usuário da Conta de Serviço
    - Criador de Token da Conta de Serviço
    - Proprietário do WorkerPool do Cloud Build
  - Crie a Conta de Serviço do Citrix Cloud no mesmo projeto que você usa para criar uma conexão de hospedagem.
  - Configure zonas DNS para `private.googleapis.com` e `gcr.io` conforme descrito em Configuração de DNS.

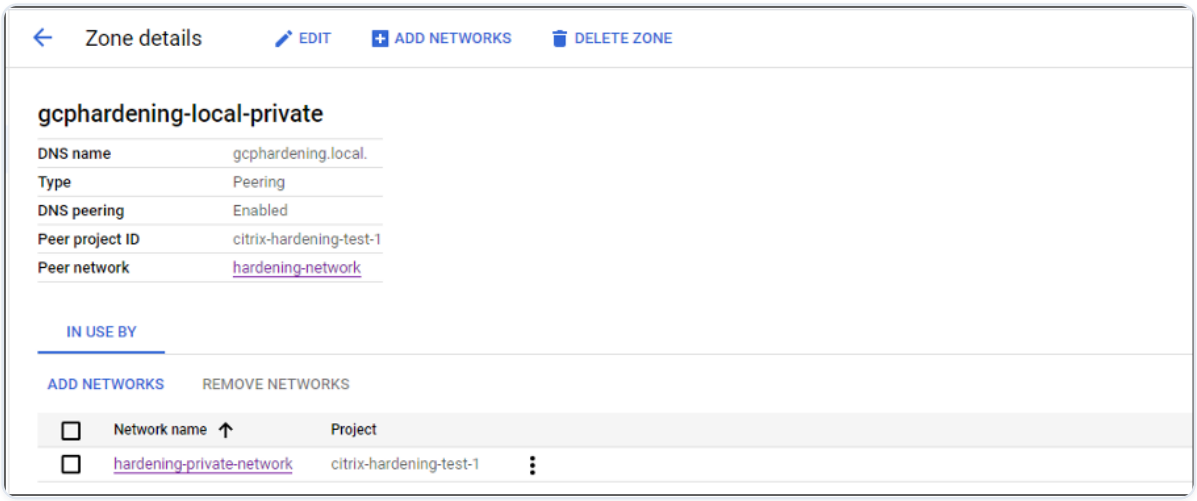




- Configure a Tradução de Endereços de Rede (NAT) privada ou use a conexão de serviço privada. Para obter mais informações, consulte Acessar APIs do Google por meio de endpoints.



- Se estiver usando uma VPC emparelhada, crie um emparelhamento de zona do Cloud DNS para a VPC emparelhada. Para obter mais informações, consulte Criar uma zona de emparelhamento.



- Nos controles de serviço da VPC, configure regras de Egress para que as APIs e VMs possam se comunicar com a internet. As regras de Ingress são opcionais. Por exemplo:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

Habilitar o pool de trabalhadores privado

Para habilitar o pool de trabalhadores privado, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell no host do Delivery Controller ou use o SDK do PowerShell Remoto. Para obter mais informações sobre o SDK do PowerShell Remoto, consulte SDKs e APIs.
2. Execute os seguintes comandos:
   a. `Add-PSSnapin citrix*`

b. `cd XDHyp:\Connections\`

c. `dir`

3. Copie o `CustomProperties` da conexão para um bloco de notas.
4. Anexe a configuração de propriedade `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`. 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="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo: `$customProperty = '<CustomProperties…</CustomProperties>'`.
6. Execute `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Execute `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Execute `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Execute o seguinte para atualizar uma conexão de host existente:

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

Permissões GCP necessárias

Esta seção contém a lista completa de permissões GCP. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

> **Nota:**

> O GCP está introduzindo alterações no comportamento padrão e no uso de contas de serviço do Cloud Build Services após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build ativada antes de April 29, 2024 não são afetados por esta alteração. No entanto, se você quiser ter o comportamento existente do Cloud Build Service após April 29, poderá criar ou aplicar a política da organização para desativar a imposição da restrição antes de ativar a API. Se você definir a nova política da organização, ainda poderá seguir as permissões existentes nesta seção e os itens que estão marcados como **Antes da Alteração da Conta de Serviço do Cloud Build**. Caso contrário, siga as permissões existentes e os itens que estão marcados como **Após a Alteração da Conta de Serviço do Cloud Build**.

Criando uma conexão de host

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

  ```
  compute.instanceTemplates.list

  compute.instances.list

  compute.networks.list

  compute.projects.get

  compute.regions.list

  compute.subnetworks.list

  compute.zones.list

  resourcemanager.projects.get
  ```

  As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Administrador de Computação
  - Usuário do Cloud Datastore

- Permissões adicionais necessárias para Shared VPC para a Conta de Serviço do Citrix Cloud no projeto Shared VPC:

  ```
  compute.networks.list

  compute.subnetworks.list

  resourcemanager.projects.get
  ```

  As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Usuário da Rede de Computação

Gerenciamento de energia de VMs

Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento no caso de catálogos somente com gerenciamento de energia:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list
```

```
resourcemanager.projects.get

compute.zoneOperations.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

Criar, atualizar ou excluir VMs

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly
```

```
compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset
```

```
compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels
```

```
compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

```

```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Citrix Cloud no projeto de VPC Compartilhada para criar uma unidade de hospedagem usando VPC e sub-rede do projeto de VPC Compartilhada:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário do Cloud Datastore

Permissões mínimas necessárias ao baixar o disco de instruções de preparação para o MCS:

- (Antes da alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Build no projeto de provisionamento.

- (Após a alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get
```

```
compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Conta de Serviço do Cloud Build (Após a alteração da Conta de Serviço do Cloud Build, é a Conta de Serviço do Cloud Compute)
  - Administrador de Instância de Computação
  - Usuário da Conta de Serviço

- Permissões mínimas necessárias para a Conta de Serviço do Cloud Compute no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

  ```
  resourcemanager.projects.get

  storage.objects.create

  storage.objects.get

  storage.objects.list
  ```

  As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Usuário da Rede de Computação
  - Usuário da Conta de Armazenamento
  - Usuário do Cloud Datastore

  Permissões adicionais necessárias para VPC Compartilhada ao baixar o disco de instruções de preparação para o MCS:

  - (Antes da alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Build no projeto de provisionamento.
  - (Após a alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

  ```
  compute.firewalls.list

  compute.networks.list

  compute.subnetworks.list

  compute.subnetworks.use
  ```

```
resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário da Conta de Armazenamento
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para o Cloud Key Management Service (KMS) para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Visualizador de KMS de Computação

Permissões gerais

A seguir estão as permissões para a conta de serviço do Citrix Cloud no projeto de provisionamento para todos os recursos suportados no MCS. Essas permissões fornecem a melhor compatibilidade daqui para frente:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get
```

```
compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list
```

```
compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig
```

```
compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list
```

```
resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas da Google Cloud Platform (GCP), consulte Criar um catálogo do Google Cloud Platform

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com HPE Moonshot

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do HPE Moonshot.

> **Observação:**
>
> Antes de criar uma conexão com o HPE Moonshot, você precisa primeiro concluir a configuração da sua conta HPE. Consulte Ambientes de virtualização HPE Moonshot.

Criar uma conexão

Você pode criar uma conexão com o HPE Moonshot usando:

- Web Studio
- Comandos PowerShell

Criar uma conexão usando o Web Studio

1. Na página **Adicionar Conexão e Recursos**, selecione **HPE Moonshot** como o tipo de conexão.
2. Insira o endereço de conexão do seu Moonshot iLO Chassis Manager. Você pode usar um endereço IP, nome de host ou FQDN para o endereço.
3. Insira suas credenciais administrativas do chassi e um nome de conexão amigável.

A configuração da conexão para quando uma das seguintes situações ocorre:

- O Citrix Virtual Apps and Desktops™ recebe um certificado público assinado por CA com erros: Uma mensagem de erro aparece. Siga as instruções na tela para corrigir o problema. Caso contrário, você não poderá prosseguir com a criação da conexão.
- O Citrix Virtual Apps and Desktops recebe um certificado privado assinado por CA. Uma página de aviso aparece. Compare a impressão digital recebida com a do servidor para a validade do certificado. Se for válido, selecione **Confiar no certificado** e clique em **OK** para prosseguir com a criação da conexão. O Citrix Virtual Apps and Desktops confiará então no certificado e armazenará a impressão digital para validação futura.

Criar uma conexão usando comandos PowerShell

Ao criar uma conexão usando o comando PowerShell, forneça as seguintes informações:

- IP: Endereço IP do 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
```

> **Observação:**
>
> O parâmetro `sslthumbprint` é necessário apenas para certificados privados assinados por CA.

Validação de certificado e impressão digital

Para criar uma conexão bem-sucedida com **HPE Moonshot**, o certificado não deve ter erros e o thumbprint deve ter um valor correto. A seguir estão os casos de uso relacionados à validação de certificado e thumbprint:

- O certificado assinado por CA pública tem erros. A conexão não é criada com sucesso. Consulte os detalhes do erro e resolva o problema.

- Certificado assinado por CA pública sem erros. A conexão é criada com sucesso, e o valor `SslThumbprints` é **Null**.
- Certificado assinado por CA privada sem erros e um valor `sslthumbprint`. A conexão é criada com sucesso com um valor `SslThumbprints` correto.
- Certificado assinado por CA privada com um valor de thumbprint incorreto. A conexão não é criada com sucesso.
- Certificado assinado por CA privada sem erros. A conexão é criada com sucesso. O `SSlThumbprints` é **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 o Web Studio
- Atualizar valor de thumbprint usando comando PowerShell

Corrigir problemas de certificado

O Citrix Virtual Apps and Desktops bloqueia uma conexão HPE Moonshot quando surgem problemas de certificado, impedindo que você entregue e gerencie cargas de trabalho em nós HPE Moonshot associados. Você verá um ícone de erro ao lado da conexão na lista **Conexões de host**. Consulte a tabela a seguir para problemas e soluções específicas.

PROBLEMA	SOLUÇÃO
Ocorre um erro de certificado no certificado assinado por CA pública	Clique na conexão e selecione a guia **Solução de problemas**. Visualize os detalhes do erro e resolva o problema.
O certificado recebido é assinado por CA privada ou expirou.	Edite a conexão do host para atualizar a impressão digital do certificado. Etapas detalhadas:
	1. Selecione a conexão e clique em **Editar Conexão**.

PROBLEMA	SOLUÇÃO	
	2. Na página **Propriedades da Conexão**, clique em **Editar configurações**. 3. Insira a senha para se conectar ao chassi HPE Moonshot e, em seguida, clique em **Salvar**. 4. Na página de **Aviso** que aparece, compare a impressão digital recebida com a do servidor para validar o certificado. 5. Se forem iguais, selecione **Confiar no certificado** e clique em **OK**.	

Atualizar valor da impressão digital

Após criar a conexão, você pode atualizar o valor do thumbprint de uma conexão usando o comando PowerShell `Set-Item`. Por exemplo, execute os seguintes comandos:

1. Obtenha os detalhes de conexão de uma conexão. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. Atualize o valor do thumbprint. Por exemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Verifique o valor do thumbprint atualizado. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

Observação:

A atualização falha se você fornecer um valor de thumbprint incorreto no comando `Set-Item`.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas da AWS, consulte Criar um catálogo de máquinas HPE Moonshot

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com o Microsoft Azure

Observação:

Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência a Azure Active Directory, Azure AD ou AAD agora se refere a Microsoft Entra ID.

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Azure Resource Manager.

Observação:

> Antes de criar uma conexão com o Microsoft Azure, você deve concluir a configuração da sua conta do Azure como um local de recurso. Consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Criar entidades de serviço e conexões

Antes de criar conexões, você deve configurar entidades de serviço que as conexões usam para acessar recursos do Azure. Você pode criar uma conexão de duas maneiras:

- Crie um principal de serviço e uma conexão juntos usando o Web Studio
- Criar uma conexão usando uma entidade de serviço criada anteriormente

Esta seção mostra como concluir estas tarefas:

- Crie um principal de serviço e uma conexão usando o Web Studio
- Criar uma entidade de serviço usando o PowerShell
- Obter o segredo do aplicativo no Azure
- Criar uma conexão usando uma entidade de serviço existente

Considerações

- A Citrix® recomenda usar o Principal de Serviço com a função de colaborador. No entanto, consulte a seção Permissões mínimas para obter a lista de permissões mínimas.
- Ao criar a primeira conexão, o Azure solicita que você conceda as permissões necessárias. Para futuras conexões, você ainda deve autenticar, mas o Azure se lembrará do seu consentimento anterior e não exibirá o prompt novamente.
- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- A conta usada para autenticação deve ser membro do diretório da assinatura. Existem dois tipos de contas a serem observados: 'Work or School' e 'personal Microsoft account'. Consulte CTX219211 para obter detalhes.
- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, podem ocorrer complicações se o usuário tiver recebido anteriormente acesso de convidado a um dos recursos do diretório. Nesse caso, ele pode ter uma entrada de espaço reservado no diretório que não concede as permissões necessárias, e um erro é retornado.

Corrija isso removendo os recursos do diretório e adicionando-os novamente explicitamente. No entanto, use esta opção com cuidado, pois ela pode ter efeitos indesejados em outros recursos que a conta pode acessar.

- Existe um problema conhecido em que certas contas são detectadas como convidados do diretório quando, na verdade, são membros. Configurações como essa geralmente ocorrem com contas de diretório mais antigas e estabelecidas. Solução alternativa: adicione uma conta ao diretório, que assume o valor de associação adequado.
- Grupos de recursos são simplesmente contêineres para recursos, e eles podem conter recursos de regiões diferentes da sua própria região. Isso pode ser potencialmente confuso se você esperar que os recursos exibidos na região de um grupo de recursos estejam disponíveis.
- Certifique-se de que sua rede e sub-rede sejam grandes o suficiente para hospedar o número de máquinas que você precisa. Isso requer alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientação sobre a capacidade do espaço de endereço.

Crie um principal de serviço e uma conexão usando o Web Studio

> **Importante:**

> Este recurso ainda não está disponível para assinaturas do Azure China.

> Com o Web Studio, você pode criar um principal de serviço e uma conexão em um único fluxo de trabalho. Os principais de serviço concedem às conexões acesso aos recursos do Azure. Quando você autenticar no Azure para criar um principal de serviço, um aplicativo é registrado no Azure. Uma chave secreta (chamada de segredo do cliente ou segredo do aplicativo) é criada para o aplicativo registrado. O aplicativo registrado (uma conexão neste caso) usa o segredo do cliente para autenticar no Azure AD.

Antes de começar, certifique-se de ter cumprido estes pré-requisitos:

- Você tem uma conta de usuário no locatário do Azure Active Directory da sua assinatura.
- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativo para autenticação. Essas permissões podem ser revogadas depois de criar a

conexão do host. Para obter mais informações sobre funções, consulte Funções internas do Azure AD.

Use o assistente **Adicionar Conexão e Recursos** para criar um principal de serviço e uma conexão juntos:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, insira seu ID de assinatura do Azure e um nome para a conexão. Depois de inserir o ID da assinatura, o botão **Criar novo** é ativado.

   > **Observação:**
   >
   > O nome da conexão pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.

4. Selecione **Criar novo** e, em seguida, insira o nome de usuário e a senha da conta do Azure Active Directory.
5. Selecione **Entrar**.
6. Selecione **Aceitar** para conceder ao Citrix Virtual Apps and Desktops™ as permissões listadas. O Citrix Virtual Apps and Desktops cria uma entidade de serviço que permite gerenciar recursos do Azure em nome do usuário especificado.
7. Depois de selecionar **Aceitar**, você retorna à página **Conexão** no assistente.

   > **Observação:**
   >
   > Depois de autenticar com sucesso no Azure, os botões **Criar novo** e **Usar existente** desaparecem. O texto **Conexão bem-sucedida** aparece, com uma marca de seleção verde, indicando a conexão bem-sucedida com sua assinatura do Azure.

8. Na página **Detalhes da Conexão**, selecione **Avançar**.

   > **Observação:**

> Você não pode prosseguir para a próxima página até que autenticar com sucesso no Azure e consinta em conceder as permissões necessárias.

9. Configure os recursos para a conexão. Os recursos compreendem a região e a rede.
   - Na página **Região**, selecione uma região.
   - Na página **Rede**, faça o seguinte:
     - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.
     - Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.
10. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

VISUALIZAR O ID DO APLICATIVO

Depois de criar uma conexão, você pode visualizar o ID do aplicativo que a conexão usa para acessar os recursos do Azure.

Na lista **Adicionar Conexão e Recursos**, selecione a conexão para visualizar os detalhes. A guia **Detalhes** mostra o ID do Aplicativo.

Criar um principal de serviço usando PowerShell

Para criar um principal de serviço usando PowerShell, conecte-se à sua assinatura do Azure Resource Manager e use os cmdlets do PowerShell fornecidos nas seções a seguir.

Certifique-se de ter estes itens prontos:

- **SubscriptionId:** `SubscriptionID` do Azure Resource Manager para a assinatura onde você deseja provisionar VDAs.
- **ActiveDirectoryID**: ID do locatário do aplicativo que você registrou no Azure AD.
- **ApplicationName:** Nome do aplicativo a ser criado no Azure AD.

As etapas detalhadas são as seguintes:

Conecte-se à sua assinatura do Azure Resource Manager.

```
`Connect-AzAccount`
```

1. Selecione a assinatura do Azure Resource Manager onde você deseja criar a entidade de serviço.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. Crie o aplicativo em seu locatário do AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Crie uma entidade de serviço.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Atribua uma função à entidade de serviço.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. Na janela de saída do console do PowerShell, anote o ApplicationId. Você fornece esse ID ao criar a conexão de host.

Obtenha o segredo do aplicativo no Azure

Para criar uma conexão usando uma entidade de serviço existente, você deve primeiro obter o ID do aplicativo e o segredo da entidade de serviço no portal do Azure.

As etapas detalhadas são as seguintes:

1. Obtenha o **ID do Aplicativo** no Web Studio ou usando o PowerShell.
2. Faça login no portal do Azure.
3. No Azure, selecione **Azure Active Directory**.
4. Em **Registros de aplicativo** no Azure AD, selecione seu aplicativo.
5. Vá para **Certificados e segredos**.
6. Clique em **Segredos do cliente**.

Criar uma conexão usando uma entidade de serviço existente

Se você já tiver uma entidade de serviço, poderá usá-la para criar uma conexão usando o Web Studio.

Certifique-se de ter estes itens prontos:

- SubscriptionId
- ActiveDirectoryID (ID do locatário)
- ID do Aplicativo
- Segredo do aplicativo

  Para obter mais informações, consulte Obter o segredo do aplicativo.
- Data de expiração do segredo

As etapas detalhadas são as seguintes:

No assistente **Adicionar Conexão e Recursos**:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, insira seu ID de assinatura do Azure e um nome para a conexão.

   > **Observação:**
   >
   > O nome da conexão pode conter 1 a 64 caracteres e não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.

4. Selecione **Usar existente**. Na janela **Detalhes do Principal de Serviço Existente**, insira as seguintes configurações para o principal de serviço existente. Depois de inserir os detalhes, o botão **Salvar** é ativado. Selecione **Salvar**. Você não pode prosseguir além desta página até fornecer detalhes válidos.

   - **ID da Assinatura**. Insira seu ID de assinatura do Azure. Para obter seu ID de assinatura, faça login no portal do Azure e navegar para **Assinaturas > Visão geral**.
   - **ID do Active Directory** (ID do locatário). Insira o ID do Diretório (locatário) do aplicativo que você registrou no Azure AD.
   - **ID do Aplicativo**. Insira o ID do Aplicativo (cliente) do aplicativo que você registrou no Azure AD.

- **Segredo do aplicativo**. Crie uma chave secreta (segredo do cliente). O aplicativo registrado usa a chave para autenticar no Azure AD. Recomendamos que você altere as chaves regularmente para fins de segurança. Certifique-se de salvar a chave, pois você não poderá recuperá-la mais tarde.
- **Data de expiração do segredo**. Insira a data após a qual o segredo do aplicativo expira. Você verá um ícone de aviso na conexão de host específica no nó **Hospedagem** a partir de 14 dias antes da expiração da chave secreta. No entanto, se a chave secreta expirar, você receberá erros.

> **Observação:**
>
> Para fins de segurança, o período de expiração não pode ser superior a dois anos a partir de agora.

- **URL de Autenticação**. Este campo é preenchido automaticamente e não é editável.
- **URL de Gerenciamento**. Este campo é preenchido automaticamente e não é editável.
- **Sufixo de armazenamento**. Este campo é preenchido automaticamente e não é editável.

  O acesso aos seguintes endpoints é necessário para criar um catálogo MCS no Azure. O acesso a esses endpoints otimiza a conectividade entre sua rede e o portal do Azure e seus serviços.

  - URL de autenticação: `<https://login.microsoftonline.com/>`
  - URL de gerenciamento: `<https://management.azure.com/>`. Esta é uma URL de solicitação para APIs do provedor do Azure Resource Manager. O endpoint para gerenciamento depende do ambiente. Por exemplo, para o Azure Global, é `<https://management.azure.com/>`, e para o Azure US Government, é `<https://management.usgovcloudapi.net/>`.
  - Sufixo de armazenamento: `<https://*.core.windows.net./>`. Este (*) é um caractere curinga para sufixo de armazenamento. Por exemplo, `https://demo.table.core.windows.net/`.

5. Após selecionar **Salvar**, você retorna à página **Detalhes da Conexão**. Selecione **Avançar** para continuar para a próxima página.
6. Configure os recursos para a conexão. Os recursos compreendem a região e a rede.

   - Na página **Região**, selecione uma região.

- Na página **Rede**, faça o seguinte:
  - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco nem os caracteres `\/;:#.*?=<>|[]{}"'()'`.
  - Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.

7. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

Gerenciar entidades de serviço e conexões

Esta seção detalha como você pode gerenciar entidades de serviço e conexões:

- Configurar as configurações de limitação do Azure
- Habilitar o compartilhamento de imagens no Azure
- Adicionar locatários compartilhados a uma conexão usando o Web Studio
- Implementar o compartilhamento de imagens usando o PowerShell
- Gerenciar o segredo do aplicativo e a data de expiração do segredo

Configurar as definições de limitação do Azure

O Azure Resource Manager limita as solicitações para assinaturas e locatários, roteando o tráfego com base em limites definidos, adaptados às necessidades específicas do provedor. Consulte Limitação de solicitações do Resource Manager no site da Microsoft para obter mais informações. Existem limites para assinaturas e locatários, onde o gerenciamento de muitas máquinas pode se tornar problemático. Por exemplo, uma assinatura contendo muitas máquinas pode apresentar problemas de desempenho relacionados a operações de energia.

> **Dica:**

> Para obter mais informações, consulte Melhorando o desempenho do Azure com o Machine Creation Services.

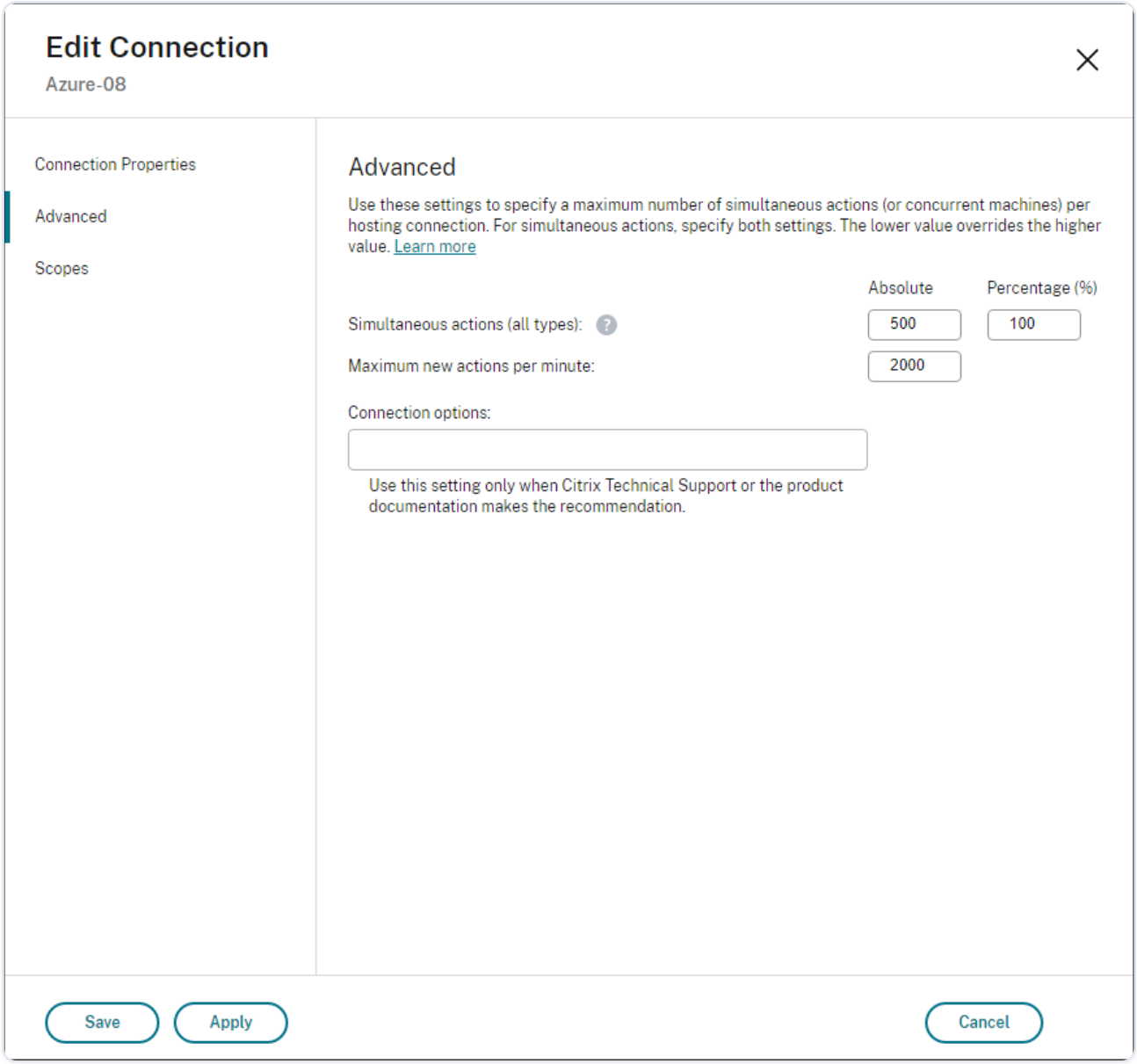
> Para ajudar a mitigar esses problemas, você pode remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

Recomendamos as seguintes configurações ideais ao ligar ou desligar VMs em grandes assinaturas, por exemplo, aquelas que contêm 1.000 VMs:

- Operações simultâneas absolutas: 500
- Máximo de novas operações por minuto: 2000
- Concorrência máxima de operações: 500

Use o Web Studio para configurar operações do Azure para uma determinada conexão do Azure:

1. No Web Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão.
3. No assistente **Editar Conexão**, selecione **Avançado**.
4. Na página **Avançado**, use as opções de configuração para especificar o número de ações simultâneas e o máximo de novas ações por minuto, e quaisquer opções de conexão adicionais.



O MCS suporta um máximo de 500 operações simultâneas por padrão. Alternativamente, você pode usar o SDK do PowerShell Remoto para definir o número máximo de operações simultâneas.

Use a propriedade **PowerShell**, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações de provisionamento simultâneas do Azure. Ao usar esta propriedade, considere:

- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` usando o comando PowerShell `Set-item`.

Habilitar o compartilhamento de imagens no Azure

Ao criar ou atualizar catálogos de máquinas, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas por meio da Galeria de Computação do Azure). Para habilitar o compartilhamento de imagens dentro ou entre locatários, você deve fazer as configurações necessárias no Azure:

- Compartilhar imagens dentro de um locatário (entre assinaturas)
- Compartilhar imagens entre locatários

COMPARTILHAR IMAGENS DENTRO DE UM LOCATÁRIO (ENTRE ASSINATURAS)

Para selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura diferente, a imagem deve ser compartilhada com o principal de serviço (SPN) dessa assinatura.

Por exemplo, se houver um principal de serviço (SPN 1), que está configurado no Studio como:

Principal de serviço: SPN 1

Assinatura: assinatura 1

Locatário: locatário 1

A imagem está em uma assinatura diferente, que é configurada no Studio como:

Assinatura: assinatura 2

Locatário: locatário 1

Se você quiser compartilhar a imagem na assinatura 2 com a assinatura 1 (SPN 1), vá para a assinatura 2 e compartilhe o grupo de recursos com o SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em função (RBAC) do Azure. O RBAC do Azure é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o RBAC do Azure, consulte o documento da Microsoft O que é o controle de acesso baseado em função do Azure (RBAC do Azure). Para conceder acesso, você atribui funções a entidades de serviço no escopo do grupo de recursos com a função Colaborador. Para atribuir funções do Azure, você deve ter a permissão `Microsoft.Authorization/roleAssignments/write`, como Administrador de Acesso do Usuário ou Proprietário. Para obter mais informações sobre como compartilhar imagens com outro SPN, consulte o documento da Microsoft Atribuir funções do Azure usando o portal do Azure.

Para obter informações sobre como selecionar uma imagem de uma assinatura diferente usando comandos do PowerShell, Selecionar uma imagem de uma assinatura diferente.

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 o Locatário 1, então:

1. Crie um registro de aplicativo para o Locatário 1. Para obter mais informações, consulte Criar o registro do aplicativo.
2. Conceda ao Locatário 2 acesso ao aplicativo solicitando um login usando um navegador. Substitua `Tenant2 ID` pelo ID do locatário do Locatário 1. Substitua `Application (client) ID` pelo ID do aplicativo do registro do aplicativo que você criou. Ao concluir as substituições, cole o URL em um navegador e siga os prompts de login para entrar no Locatário 2. Por exemplo:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   Para obter mais informações, consulte Conceder acesso ao Locatário 2.
3. Conceda ao aplicativo acesso ao grupo de recursos do Locatário 2. Faça login como Locatário 2 e conceda ao registro do aplicativo acesso ao grupo de recursos que contém a imagem da galeria. Para obter mais informações, consulte autenticar requests across tenants.

Para criar um catálogo usando uma imagem de um locatário diferente usando comandos do PowerShell:

1. Atualizar propriedades personalizadas de conexão de hospedagem com IDs de locatário compartilhadas.
2. Selecionar uma imagem de um locatário diferente.

Adicionar locatários compartilhados a uma conexão usando o Web Studio

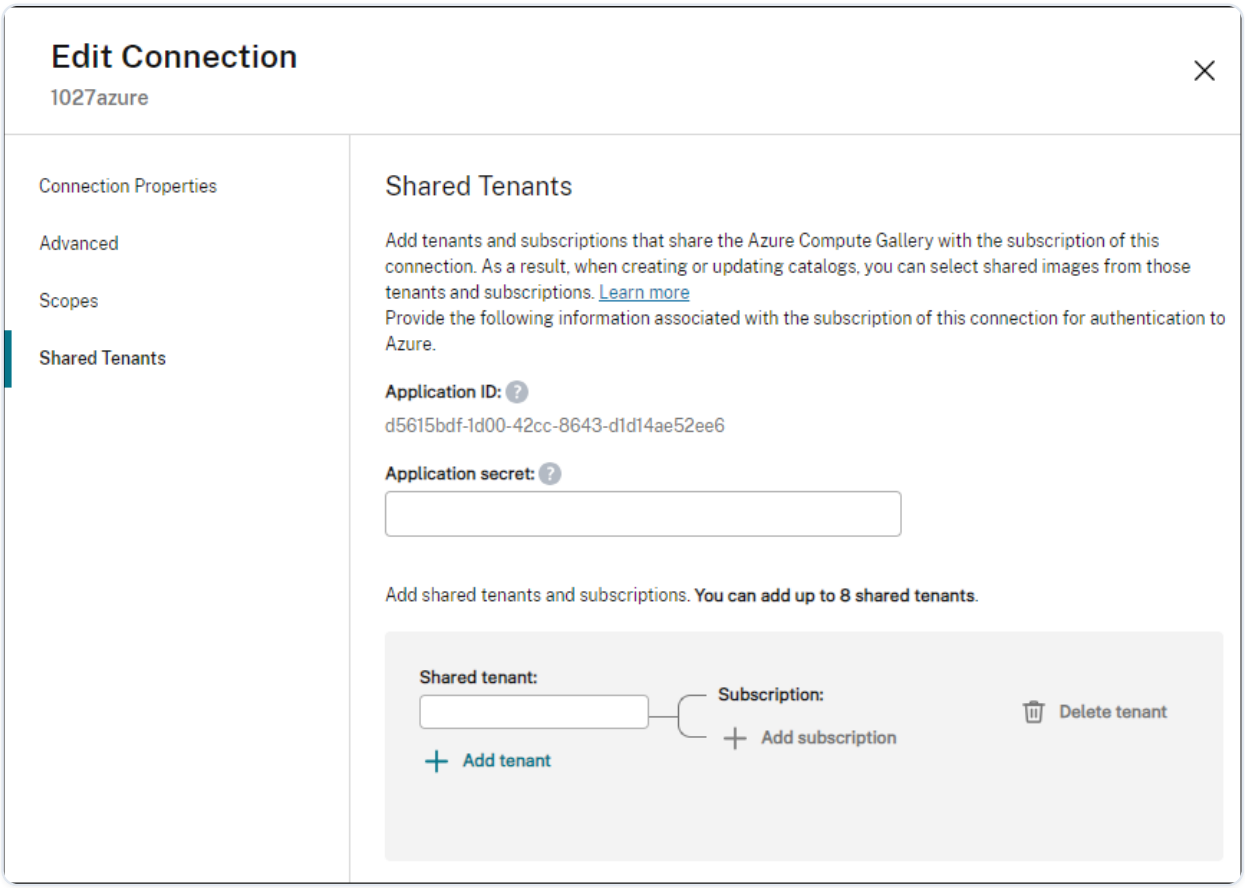
Ao criar ou atualizar catálogos de máquinas no Web Studio, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas por meio da Galeria de Computação do Azure). O recurso exige que você forneça informações de locatário e assinatura compartilhadas para as conexões de host associadas.

> **Observação:**

Certifique-se de ter configurado as configurações necessárias no Azure para habilitar o compartilhamento de imagens entre locatários. Para obter mais informações, consulte Compartilhar imagens entre locatários.

Conclua as seguintes etapas para uma conexão:

1. No Web Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.



3. Em **Locatários Compartilhados**, faça o seguinte:
   - Forneça o ID do aplicativo e o segredo do aplicativo associados à assinatura da conexão. O Citrix Virtual Apps and Desktops usa essas informações para autenticar no Azure AD.
   - Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura da conexão. Você pode adicionar até 8 locatários compartilhados e 8 assinaturas para cada locatário.
4. Quando terminar, selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Implementar o compartilhamento de imagens usando o PowerShell

Esta seção o orienta pelos processos de compartilhamento de imagens usando o PowerShell:

- Selecionar uma imagem de uma assinatura diferente
- Atualizar propriedades personalizadas de conexão de hospedagem com IDs de locatário compartilhados
- Selecionar uma imagem de um locatário diferente

SELECIONAR UMA IMAGEM DE UMA ASSINATURA DIFERENTE

Você pode selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura compartilhada diferente no mesmo locatário do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, o Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.
2. Liste todas as assinaturas compartilhadas em um locatário.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões de imagem dessa definição de imagem.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

ATUALIZAR PROPRIEDADES PERSONALIZADAS DE CONEXÃO DE HOSPEDAGEM COM IDS DE LOCATÁRIO COMPARTILHADAS

Use `Set-Item` para atualizar as propriedades personalizadas da conexão de hospedagem com IDs de locatário e IDs de assinatura compartilhadas. Adicione uma propriedade `SharedTenants` em `CustomProperties`. O formato de `Shared Tenants` é:

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

Por exemplo:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

Observação:

Você pode adicionar mais de um locatário. Cada locatário pode ter mais de uma assinatura.

SELECIONE UMA IMAGEM DE UM LOCATÁRIO DIFERENTE

Você pode selecionar uma imagem na Galeria de Computação do Azure que pertence a um locatário diferente do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, o Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.
2. Listar todas as assinaturas compartilhadas.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription
```

4. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup
```

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões de imagem dessa definição de imagem.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

Gerenciar o segredo do aplicativo e a data de expiração do segredo

Certifique-se de alterar o segredo do aplicativo para uma conexão antes que o segredo expire. Você verá um ícone de aviso na conexão de host específica no nó **Hospedagem** a partir de 14

dias antes da expiração da chave secreta. No entanto, se a chave secreta expirar, você receberá erros.

CRIAR UM SEGREDO DE APLICATIVO NO AZURE

Você pode criar um segredo de aplicativo para uma conexão através do portal do Azure.

1. Selecione **Azure Active Directory**.
2. Em **Registros de aplicativo** no Azure AD, selecione seu aplicativo.
3. Vá para **Certificados e segredos**.
4. Clique em **Segredos do cliente > Novo segredo do cliente**.
5. Forneça uma descrição do segredo e especifique uma duração. Quando terminar, selecione **Adicionar**.

> **Observação:**
>
> Certifique-se de salvar o segredo do cliente, pois você não poderá recuperá-lo mais tarde.

6. Copie o valor do segredo do cliente e a data de expiração.
7. No Web Studio, edite a conexão correspondente e substitua o conteúdo nos campos **Segredo do aplicativo** e **Data de expiração do segredo** pelos valores que você copiou.

ALTERAR A DATA DE EXPIRAÇÃO DO SEGREDO

Você pode usar o Web Studio para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

> **Observação:**
>
> Você verá um ícone de aviso na conexão de host específica no nó **Hospedagem** a partir de 14 dias antes da expiração da chave secreta.

1. No assistente **Adicionar Conexão e Recursos**, clique com o botão direito do mouse em uma conexão e clique em **Editar Conexão**.
2. Na página **Propriedades da Conexão**, clique em **Data de expiração do segredo** para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

Permissões do Azure necessárias

Esta seção contém as permissões mínimas e gerais necessárias para o Azure.

Permissões mínimas

As permissões mínimas oferecem melhor controle de segurança. No entanto, novos recursos que exigem permissões adicionais falham devido ao uso apenas de permissões mínimas.

CRIANDO UMA CONEXÃO DE HOST

Adicione uma nova conexão de host usando as informações obtidas do Azure.

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read"
```

GERENCIAMENTO DE ENERGIA DE VMS

Ligue ou desligue as instâncias da máquina.

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

CRIAR, ATUALIZAR OU EXCLUIR VMS

Crie um catálogo de máquinas, adicione, exclua, atualize máquinas e exclua o catálogo de máquinas.

A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é um disco gerenciado ou os instantâneos estão localizados na mesma região da conexão de hospedagem.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",
```

```
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",
```

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 que a conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- Se a imagem mestre for uma ImageVersion da Galeria de Imagens Compartilhadas:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- Se a imagem mestre for um disco gerenciado, então os instantâneos, ou VHD, estão em uma região diferente da região da conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Se você usar o grupo de recursos gerenciado pelo Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- Se você colocar a imagem mestre na Azure Compute Gallery (anteriormente Shared Image Gallery) em um locatário ou assinatura compartilhada:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- Se você usar o suporte a host dedicado do Azure:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- Se você usar Criptografia do Lado do Servidor (SSE) com Chaves Gerenciadas pelo Cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- Se você implantar VMs usando modelos ARM (perfil de máquina):

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",
```

```
"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Se você usar a especificação de modelo do Azure como um perfil de máquina:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

CRIANDO, ATUALIZANDO E EXCLUINDO MÁQUINAS COM DISCO NÃO GERENCIADO

A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é VHD e o grupo de recursos é fornecido pelo administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

Permissão geral

A função de Colaborador tem acesso total para gerenciar todos os recursos. Este conjunto de permissões não o impede de obter novos recursos.

O seguinte conjunto de permissões oferece a melhor compatibilidade daqui para frente, embora inclua mais permissões do que o necessário com o conjunto de recursos atual:

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",
```

```
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
```

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",
```

```
"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Resources/tenants/read",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

```
"Microsoft.Features/providers/features/read",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

Validar permissões na conexão do host

Você pode validar as permissões em uma conexão de host para realizar tarefas relacionadas à criação e gerenciamento de catálogos de máquinas MCS. Essa implementação ajuda você a descobrir as permissões ausentes necessárias para diferentes cenários, como criar, excluir e atualizar VMs, gerenciamento de energia de VMs, com antecedência para que você possa evitar ser bloqueado em momentos críticos.

Você pode validar as permissões em uma conexão de host usando o comando PowerShell `Test-HypHypervisorConnection`. O resultado do comando é capturado como uma lista, onde cada item da lista é dividido em três seções.

- Categoria: A ação ou tarefa que um usuário pode realizar para criar e gerenciar um catálogo de máquinas MCS.
- Ação Corretiva: A etapa que um administrador deve realizar para resolver uma discrepância de permissões ausentes dos usuários.
- Permissão ausente: A lista de permissões ausentes para uma categoria.

Para validar as permissões, faça o seguinte:

1. Crie uma conexão de host com o Azure.
2. Abra uma janela do PowerShell no host do Delivery Controller™.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Execute o seguinte comando para verificar se você tem as permissões necessárias para testar uma conexão.

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
```

Permissão de nível de função necessária para o SPN:

- Microsoft.Authorization/roleDefinitions/read (no nível da assinatura ou no nível do grupo de recursos, se o grupo de recursos for fornecido)
- Microsoft.Authorization/roleAssignments/read (no nível da assinatura ou no nível do grupo de recursos, se o grupo de recursos for fornecido)

Permissões de nível de API necessárias para o SPN:

Microsoft.Graph:

- Application.Read.All
- Directory.Read.All
- ServicePrincipalEndpoint.Read.All

5. Depois de adicionar as permissões ausentes necessárias para pesquisar suas permissões, execute o seguinte comando para verificar se você tem permissões nas várias categorias.

   Exemplo:

   Para testar uma conexão no nível da assinatura com um nível mais alto de autorização necessário:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   Exemplo:

   Para testar uma conexão no nível do grupo de recursos sem um alto nível de autorização:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   Observação:

   O parâmetro CustomProperties é usado para fornecer o nível do grupo de recursos porque o grupo de recursos é uma informação específica da conexão.

> Exemplo:

Para testar uma conexão com o nível mais alto de autorização no nível do grupo de recursos:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

Para obter informações sobre permissões, consulte Permissões do Azure necessárias.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do Azure, consulte Criar um catálogo do Microsoft Azure

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com o Microsoft System Center Virtual Machine Manager

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Microsoft System Center Virtual Machine Manager (VMM).

> **Observação:**

> Antes de criar uma conexão com o VMM, você precisa primeiro concluir a configuração da sua conta VMM como um local de recurso. Consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Criar uma conexão

Se você usou o MCS para provisionar VMs, faça o seguinte no assistente de criação de conexão:

- Insira o endereço como um nome de domínio totalmente qualificado do servidor host.

- Insira as credenciais para a conta de administrador que você configurou anteriormente. Esta conta deve ter permissão para criar novas VMs.
- Na caixa de diálogo Detalhes do Host, selecione o cluster ou host autônomo a ser usado ao criar VMs.

> **Importante**
>
> Procure um cluster ou host autônomo mesmo se você estiver usando uma implantação de host Hyper-V único.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para criar catálogos de máquinas com MCS em compartilhamento de arquivos SMB 3, consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com Nutanix

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Nutanix.

> **Nota:**
>
> Antes de criar uma conexão com o Nutanix, você precisa primeiro concluir a configuração da sua conta Nutanix como um local de recurso. Consulte Ambientes de virtualização Nutanix.

Criar uma conexão com Nutanix

As informações a seguir são um complemento às orientações em Conexões e recursos. Para criar uma conexão Nutanix, siga as orientações gerais desse artigo, observando os detalhes específicos do Nutanix.

No assistente **Adicionar Conexão e Recursos**, selecione o tipo de conexão Nutanix na página **Conexão** e, em seguida, especifique o endereço e as credenciais, além de um nome para a conexão. Na página **Rede**, selecione uma rede para a unidade de hospedagem.

Os seguintes tipos de conexão estão disponíveis para seleção: **Nutanix AHV**, **Nutanix AHV DRaaS** e **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique o endereço e as credenciais do cluster Prism Element (PE).
- Para **Nutanix AHV PC**, especifique o endereço e as credenciais do Prism Central (PC).

> **Observação:**
>
> Atualmente, o tipo de conexão Nutanix AHV PC é usado apenas para criar conexão com o Nutanix Cloud Cluster (NC2) no Azure. Além disso, um catálogo de máquinas só pode ser hospedado em um único cluster em uma conexão NC2 no Azure.

- Para **Nutanix AHV DRaaS**, especifique o endereço e o nome de usuário do locatário DRaaS. Importe seus arquivos de credenciais Nutanix DRaaS privados e públicos (`.pem`).

> **Dica:**
>
> Se você implantar máquinas usando o Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do Nutanix, consulte Criar um catálogo Nutanix

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com a nuvem Nutanix e soluções de parceiros

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos da nuvem Nutanix e das soluções de parceiros.

Citrix Virtual Apps and Desktops™ oferece suporte à seguinte solução de nuvem e parceira da Nutanix:

- Clusters de Nuvem Nutanix na AWS

> **Observação:**
>
> Antes de criar uma conexão com a solução de nuvem e parceira da Nutanix, você precisa primeiro concluir a configuração da sua respectiva conta como um local de recurso. Consulte Soluções de nuvem e parceiras da Nutanix.

Conectar-se ao Nutanix Prism

Depois de criar um cluster Nutanix, conecte-se ao Nutanix Prism.

Para se conectar ao Nutanix Prism:

1. Crie uma VM bastion na sub-rede 10.0.129.0/24.
2. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior.
3. Faça login usando as credenciais padrão: `admin:nutanix/4u`. Lembre-se de alterar a senha.

Crie uma VM no Cluster Nutanix

Depois de se conectar ao **Nutanix Prism**, crie VMs no cluster Nutanix.

Se a VM precisar de acesso à Internet

1. Vá para o console da AWS.
2. Crie uma nova sub-rede 10.0.130.0/24 na mesma VPC que a criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas desta sub-rede para direcionar todo o tráfego não local para o gateway NAT acima.
4. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
5. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a mesma sub-rede 10.0.130.0/24 usada na AWS.
6. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa nova sub-rede.

Se a VM não precisar de acesso à Internet

1. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
2. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a sub-rede 10.0.129.0/24.
3. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa sub-rede.

> **Dica:**
>
> Certifique-se de que as informações de hora e fuso horário nas VMs estejam configuradas corretamente. Isso é especialmente verdadeiro para o AD.

Criar conexão de host

1. Inicie o Web 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 da conexão**, insira `https://xxx.xxx.xxx.xxx:9440`.
4. Siga a interface do usuário para concluir o assistente.

> **Observação:**
>
> Para ver a opção Nutanix no Web Studio, todas as VMs do conector devem ter o plug-in nutanix instalado, mesmo que não sejam usadas na zona nutanix.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas da Nutanix, consulte Criar um catálogo Nutanix

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão com VMware

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

> **Observação:**
>
> Antes de criar uma conexão com o VMware, você precisa primeiro concluir a configuração da sua conta VMware como um local de recurso. Consulte Ambientes de virtualização VMware.

Criar uma conexão

No assistente de criação de conexão:

1. Selecione o tipo de conexão VMware.
2. Especifique o endereço do ponto de acesso para o SDK do vCenter.
3. Especifique as credenciais para uma conta de usuário VMware que você configurou anteriormente e que tem permissões para criar VMs. Especifique o nome de usuário no formato domínio/nome_de_usuário.

Impressão digital SSL do VMware

O recurso de impressão digital SSL do VMware elimina a necessidade de criar manualmente uma conexão de host com um hipervisor VMware vSphere. Não é mais necessário criar manualmente uma relação de confiança entre os Delivery Controllers no Site e o certificado do hipervisor antes de criar uma conexão.

O recurso de impressão digital SSL do VMware armazena a impressão digital do certificado não confiável no banco de dados do Site. Essa configuração garante que o hipervisor possa ser continuamente identificado como confiável pelo Citrix Virtual Apps and Desktops™, mesmo que não pelos Controllers.

Ao criar uma conexão de host vSphere no Studio, uma caixa de diálogo permite que você visualize o certificado da máquina à qual está se conectando. Você pode então escolher se deseja confiar nele.

Privilégios necessários

Crie uma conta de usuário VMware e uma ou mais funções VMware com um conjunto ou todas as permissões listadas neste artigo. Baseie a criação das funções no nível específico de granularidade exigido sobre as permissões do usuário para solicitar as várias operações do Citrix DaaS™ a qualquer momento. Para conceder as permissões específicas do usuário a qualquer momento, associe-as à função respectiva, no nível do data center no mínimo, com a opção **Propagate to children** selecionada.

As tabelas a seguir mostram os mapeamentos entre as operações do Citrix Virtual Apps and Desktops e os privilégios mínimos necessários do VMware.

> **Observação:**
>
> O nome de exibição da lista de permissões, especificamente a *User Interface*, é diferente para algumas versões do vSphere. Por exemplo, no vSphere 6.7, a permissão *User Interface* é **Change Memory** e **Change Settings**, em vez de **Settings** e **Memory**, conforme descrito nos privilégios necessários observados nesta página.

Adicionar conexões e recursos

SDK	INTERFACE DO USUÁRIO
System. Anonymous, System. Read e System.View	Adicionado automaticamente. Pode usar a função somente leitura integrada.

Gerenciamento de energia

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interação > Ligar
VirtualMachine.Interact.Reset	Máquina virtual > Interação > Reiniciar
VirtualMachine.Interact.Suspend	Máquina virtual > Interação > Suspender
Datastore.Browse	Datastore > Navegar no datastore

Provisionar máquinas (Machine Creation Services™)

Para provisionar máquinas usando o MCS, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	Datastore > Alocar espaço
Datastore.Browse	Datastore > Navegar no datastore
Datastore.FileManagement	Datastore > Operações de arquivo de baixo nível
Network.Assign	Network > Atribuir rede
Resource.AssignVMToPool	Recurso > Atribuir máquina virtual ao pool de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuração > Adicionar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuração > Adicionar novo disco
Máquina virtual.Configuração.Adicionar ou remover dispositivo	Máquina virtual > Configuração > Adicionar ou remover dispositivo
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuração > Avançado
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuração > Remover disco
VirtualMachine.Config.CPUCount	Máquina virtual > Configuração > Alterar contagem de CPU
VirtualMachine.Config.Memory	Máquina virtual > Configuração > Alterar memória
VirtualMachine.Config.Settings	Máquina virtual > Configuração > Alterar configurações
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interação > Ligar

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Interact.Reset	Máquina virtual > Interação > Redefinir
VirtualMachine.Interact.Suspend	Máquina virtual > Interação > Suspender
VirtualMachine.Inventory.CreateFromExisting	Máquina virtual > Inventário > Criar a partir de existente
VirtualMachine.Inventory.Create	Máquina virtual > Inventário > Criar nova
VirtualMachine.Inventory.Delete	Máquina virtual > Inventário > Remover
VirtualMachine.Provisioning.Clone	Máquina virtual > Provisionamento > Clonar máquina virtual
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1 e vSphere 6.x, Update 1: Máquina virtual > Estado > Criar instantâneo; vSphere 5.5: Máquina virtual > Gerenciamento de instantâneos > Criar instantâneo

Atualização e reversão de imagem

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	Datastore > Alocar espaço
Datastore.Browse	Datastore > Navegar no datastore
Datastore.FileManagement	Datastore > Operações de arquivo de baixo nível
Network.Assign	Rede > Atribuir rede
Resource.AssignVMToPool	Recurso > Atribuir máquina virtual ao pool de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuração > Adicionar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuração > Adicionar novo disco

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuração > Avançado
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuração > Remover disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interação > Ligar
VirtualMachine.Interact.Reset	Máquina virtual > Interação > Redefinir
VirtualMachine.Inventory.CreateFromExisting	Máquina virtual > Inventário > Criar a partir de existente
VirtualMachine.Inventory.Create	Máquina virtual > Inventário > Criar nova
VirtualMachine.Inventory.Delete	Máquina virtual > Inventário > Remover
VirtualMachine.Provisioning.Clone	Máquina virtual > Provisionamento > Clonar máquina virtual

Excluir máquinas provisionadas

SDK	INTERFACE DO USUÁRIO
Datastore.Browse	Datastore > Navegar no datastore
Datastore.FileManagement	Datastore > Operações de arquivo de baixo nível
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuração > Remover disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interação > Desligar
VirtualMachine.Inventory.Delete	Máquina virtual > Inventário > Remover

Perfil de Armazenamento (vSAN)

Para visualizar, criar ou excluir políticas de armazenamento durante a criação de catálogos em um datastore vSAN, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
StorageProfile.Update	ARMAZENAMENTO ORIENTADO POR PERFIL > Atualização de armazenamento orientado por perfil. Para vSphere 8: Políticas de armazenamento de VM > Atualizar políticas de armazenamento de VM
StorageProfile.View	ARMAZENAMENTO ORIENTADO POR PERFIL > Visualização de armazenamento orientado por perfil. Para vSphere 8: Políticas de armazenamento de VM > Visualizar políticas de armazenamento de VM

Tags e Atributos Personalizados

Tags e atributos personalizados permitem anexar metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e filtragem desses objetos. Para criar, editar, atribuir e excluir tags ou categorias, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
InventoryService.Tagging.CreateTag	Marcação vSphere > Criar Marcação vSphere
InventoryService.Tagging.CreateCategory	Marcação vSphere > Criar Categoria de Marcação vSphere
InventoryService.Tagging.EditTag	Marcação vSphere > Editar Marcação vSphere
InventoryService.Tagging.EditCategory	Marcação vSphere > Editar Categoria de Marcação vSphere
InventoryService.Tagging.DeleteTag	Marcação vSphere > Excluir Marcação vSphere
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Excluir Categoria de Tag do vSphere
InventoryService.Tagging.AttachTag	vSphere Tagging > Atribuir ou Desatribuir Tag do vSphere
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Atribuir ou Desatribuir Tag do vSphere em Objeto

SDK	INTERFACE DO USUÁRIO
Global.ManageCustomFields	Global > Gerenciar atributos personalizados
Global.SetCustomField	Global > Definir atributo personalizado

Observação:

Quando o MCS cria um catálogo de máquinas, ele marca as VMs de destino com tags de nome especiais. Essas tags diferenciam a imagem mestre das VMs criadas pelo MCS e impedem o uso de VMs criadas pelo MCS para preparação de imagem. Você pode identificar a diferença pelo valor do atributo `XdProvisioned` no vCenter. O atributo é definido como **True** se o MCS criar VMs.

Operações criptográficas

Os privilégios de operações criptográficas controlam quem pode realizar qual tipo de operação criptográfica em qual tipo de objeto. O vSphere Native Key Provider usa os privilégios `Cryptographer.*`. As seguintes permissões mínimas são necessárias para operações criptográficas:

Observação:

Essas permissões são necessárias para criar catálogos de máquinas MCS com VM equipada com vTPM.

SDK	INTERFACE DO USUÁRIO
Cryptographer.Access	Privilégios > Todos os Privilégios > Operações criptográficas > Acesso Direto
Cryptographer.AddDisk	Privilégios > Todos os Privilégios > Operações criptográficas > Adicionar disco
Cryptographer.Clone	Privilégios > Todos os Privilégios > Operações criptográficas > Clonar

SDK	INTERFACE DO USUÁRIO
Cryptographer.Encrypt	Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar
Cryptographer.EncryptNew	Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar novo
Cryptographer.Decrypt	Privilégios > Todos os Privilégios > Operações criptográficas > Descriptografar
Cryptographer.Migrate	Privilégios > Todos os Privilégios > Operações criptográficas > Migrar
Cryptographer.ReadKeyServersInfo	Privilégios > Todos os Privilégios > Operações criptográficas > Ler informações do KMS

Provisionar máquinas (Citrix Provisioning™)

Essas permissões para clonar e implantar um modelo são necessárias para provisionar VMs usando o Assistente de Configuração do Citrix Virtual Apps and Desktops e o Assistente de Exportação de Dispositivos através do console do Citrix Provisioning. Defina as permissões ao criar uma conexão de hospedagem. Você precisa de todas as permissões de Provisionar máquinas (Machine Creation Services) e as seguintes.

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.AddRemoveDevice	Máquina virtual > Configuração > Adicionar ou remover dispositivo
VirtualMachine.Config.CPUCount	Máquina virtual > Configuração > Alterar contagem de CPU
VirtualMachine.Config.Memory	Máquina virtual > Configuração > Memória
VirtualMachine.Config.Settings	Máquina virtual > Configuração > Configurações
VirtualMachine.Provisioning.CloneTemplate	Máquina virtual > Provisionamento > Clonar modelo

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Provisioning.DeployTemplate	Máquina virtual > Provisionamento > Implantar modelo
VApp.Export	vApp > Exportar

Observação:

O `VApp.Export` é necessário para criar catálogos de máquinas MCS usando o perfil da máquina.

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. Use um certificado digital emitido por uma autoridade de certificação que atenda à política de segurança da sua organização.

Se você não conseguir usar um certificado digital emitido por uma autoridade de certificação, poderá usar o certificado autoassinado instalado no VMware. Use este método apenas se a política de segurança da sua organização permitir. Adicione o certificado do VMware vCenter a cada Delivery Controller.

1. Adicione o nome de domínio totalmente qualificado (FQDN) do computador que executa o vCenter Server ao arquivo hosts nesse servidor, em `%SystemRoot%/WINDOWS/system32/Drivers/etc/`. Esta etapa é necessária apenas se o FQDN do computador que executa o vCenter Server ainda não estiver presente no sistema de nomes de domínio.
2. Obtenha o certificado do vCenter usando qualquer um dos três métodos a seguir:

   Do servidor vCenter.

   a. Copie o arquivo rui.crt do servidor vCenter para um local acessível em seus Delivery Controllers.

   b. No Controller, navegar até o local do certificado exportado e abra o arquivo rui.crt.

Baixe o certificado usando um navegador da web. Se você estiver usando o Internet Explorer, clique com o botão direito do mouse no Internet Explorer e escolha **Executar como administrador** para baixar ou instalar o certificado.

a. Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com)>`.
b. Aceite os avisos de segurança.
c. Clique na barra de endereço que exibe o erro de certificado.
d. Visualize 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. navegar até o local do certificado exportado e abra o arquivo .CER.

Importe diretamente do Internet Explorer executado como administrador.

- Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com)>`.
- Aceite os avisos de segurança.
- Clique na barra de endereço que exibe o erro de certificado.
- Visualize o certificado.

3. Importe o certificado para o armazenamento de certificados em cada um dos seus Controladores.

a. Clique na opção **Instalar certificado**, selecione **Máquina Local** e, em seguida, clique em **Avançar**.
b. Selecione **Place all certificates in the following store** e clique em **Browse**. Selecione **Trusted People** e clique em **OK**. Clique em **Next** e depois em **Finish**.

Se você alterar o nome do servidor vSphere após a instalação, deverá gerar um novo certificado autoassinado nesse servidor antes de importar o novo certificado.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do VMware, consulte Criar um catálogo VMware

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Conexão à nuvem VMware e soluções de parceiros

Após configurar cluster do Azure VMware Solution (AVS), Google Cloud VMware Engine e VMware Cloud no AWS, crie as conexões. Consulte Conexão com o VMware para criar conexões.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do VMware, consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html)

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Gerenciamento de imagens (Pré-visualização)

Introdução

O processo de criação ou atualização de catálogo do MCS tem duas fases:

- Masterização: uma imagem de origem é convertida em uma imagem publicada
- Clonagem: novas VMs são criadas a partir da imagem publicada

Com a funcionalidade de gerenciamento de imagens, o MCS separa a fase de masterização do fluxo de trabalho geral de provisionamento.

Você pode preparar várias versões de imagem do MCS (Imagem Preparada) a partir de uma única imagem de origem e usá-la em vários catálogos de máquinas MCS diferentes. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem.

Os benefícios de usar essa funcionalidade de gerenciamento de imagens são:

- Gerar imagens preparadas antecipadamente sem criar um catálogo.
- Reutilizar imagens preparadas em vários cenários, como criar e atualizar um catálogo.

- Reduzir significativamente o tempo de criação ou atualização do catálogo.

Observação:

- Este recurso é atualmente aplicável a ambientes de virtualização Azure e VMware.
- Você pode criar um catálogo de máquinas MCS sem usar imagens preparadas. Nesse caso, você não pode obter os benefícios do recurso.

Casos de uso

Alguns dos casos de uso da funcionalidade de gerenciamento de imagens são:

- *Gerenciamento de versões*: As versões de imagem permitem que você:
  - gerenciar diferentes iterações ou atualizações de uma imagem específica.
  - manter várias versões de uma imagem para diferentes propósitos.
- *Agrupamento lógico*: Você pode criar várias definições de imagem para:
  - agrupar logicamente as versões da imagem com base em vários critérios, como projeto, departamento ou tipo de aplicativo e desktop.
  - gerenciar imagens de forma mais eficiente dentro de uma organização.

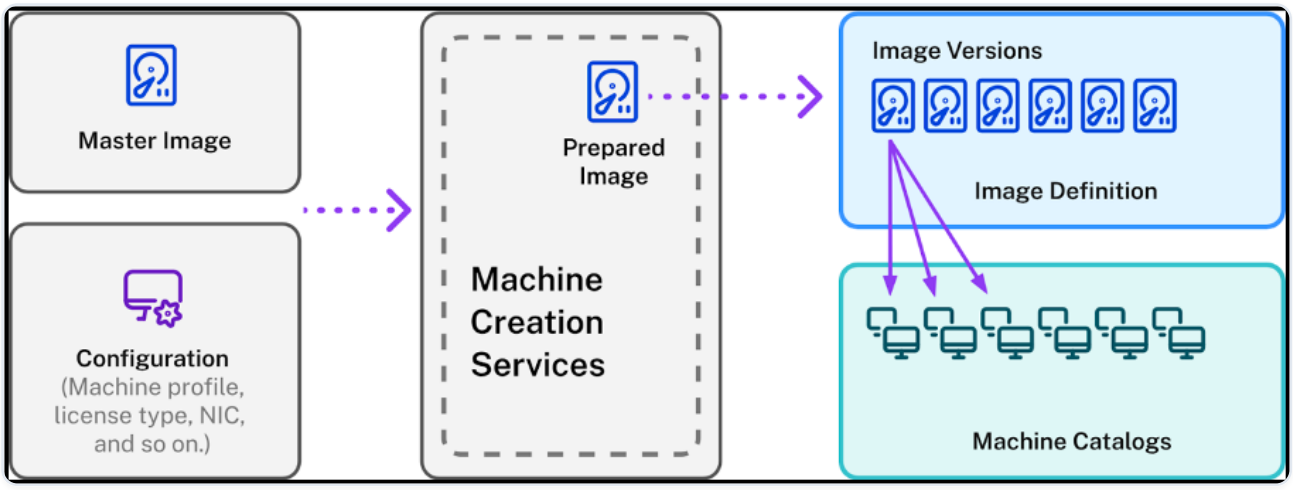
O que é uma imagem preparada?

Com a funcionalidade de gerenciamento de imagens, o MCS desvincula a fase de masterização do fluxo de trabalho geral de criação ou atualização de catálogo e divide o processo em duas etapas:

1. Crie imagens preparadas a partir de uma única imagem de origem.
2. Use a imagem preparada para criar ou atualizar um catálogo de máquinas MCS.

Você pode criar as imagens preparadas com antecedência. Você pode usar uma única imagem preparada para criar ou atualizar vários catálogos de máquinas provisionados pelo MCS.

Entenda como uma imagem preparada é usada em vários catálogos de máquinas MCS ao usar o Web Studio a partir da imagem:



Definição de imagem: As definições de imagem são um agrupamento lógico de versões de uma imagem. A definição de imagem contém informações sobre:

- por que a imagem foi criada
- para qual SO ela é
- outras informações sobre o uso da imagem.

Um catálogo não é criado a partir de uma definição de imagem, mas a partir das versões de imagem que são criadas com base na definição de imagem.

Versão da imagem: As versões da imagem gerenciam o versionamento para a definição da imagem. Uma definição de imagem pode ter várias versões de imagem. Use as versões da imagem como imagens preparadas para criar ou atualizar um catálogo.

Alternativamente, se você quiser usar comandos PowerShell para criar um esquema de provisionamento para criar ou atualizar um catálogo, então você deve criar uma especificação de versão de imagem preparada com base na especificação de versão de imagem mestre, conforme necessário para o seu ambiente.

Participe da Prévia Técnica

Se você estiver interessado em participar da Prévia Técnica, forneça suas informações de contato aqui.

Nós o ajudaremos a configurar o ambiente de teste e forneceremos suporte técnico, se necessário.

Requisito

- Para imagens mestre do Windows, apenas imagens VDA versão 2311 ou posterior são suportadas. O componente MCS/IO deve ser explicitamente selecionado e instalado. A

habilitação ou desabilitação da configuração de E/S do MCS deve ser determinada durante a criação ou atualização do catálogo de máquinas, pois não está habilitada por padrão.

Limitações

Atualmente, o recurso não suporta o seguinte:

- Múltiplas NICs no Azure
- Recurso de disco de dados persistente
- Hibernação para multi-sessão
- Alteração do tipo de imagem

Gerenciamento do ciclo de vida da imagem usando o Web Studio

O ciclo de vida da imagem ao usar o Web Studio é:

1. Criar uma imagem preparada: Crie uma definição de imagem e sua versão inicial da imagem.
2. Crie versões de imagem a partir da versão inicial da imagem.
3. Usar uma versão de imagem como uma imagem preparada para criar catálogos.
4. Atualizar um catálogo de máquinas com uma imagem preparada diferente.
5. Gerenciar as definições e versões de imagem: Editar o nome e a descrição das versões de imagem e a descrição de uma definição de imagem.
6. Excluir uma versão de imagem.
7. Excluir uma definição de imagem.

Alternativamente, você também pode gerenciar imagens usando o PowerShell. Consulte Gerenciamento do ciclo de vida da imagem usando o PowerShell.

Criar ou atualizar um catálogo usando uma imagem preparada

Crie imagens preparadas e use as imagens preparadas para criar ou atualizar um catálogo de máquinas MCS usando:

- Web Studio
- Comandos PowerShell

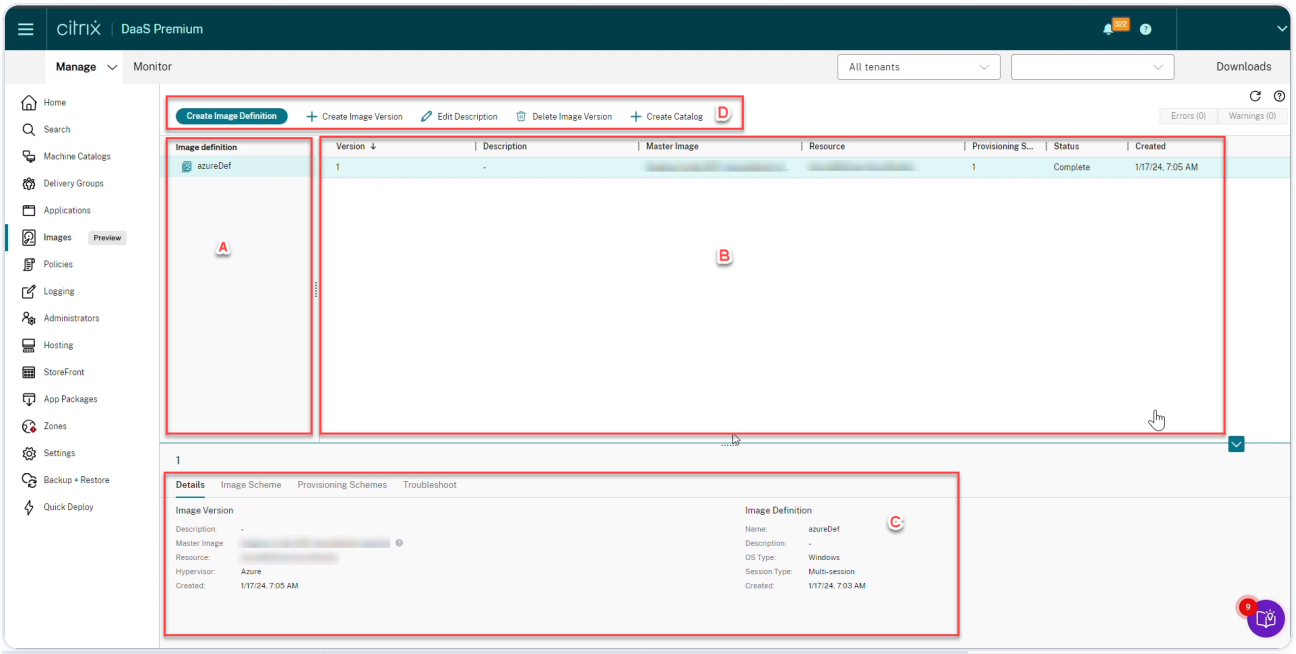
Usar o Web Studio

Consulte os seguintes tópicos:

- Entender o nó Imagens
- Criar uma definição de imagem e versão inicial da imagem
- Criar versões de imagem
- Criar um catálogo de máquinas a partir do nó Imagens
- Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas
- Atualizar um catálogo de máquinas com uma imagem preparada diferente
- Gerenciar as definições e versões de imagem

Compreender o nó Imagens

Use o nó **Imagens** para criar e gerenciar imagens preparadas pelo MCS. Sua exibição principal é dividida em quatro partes:



RÓTULO	PARTE	DESCRIÇÃO
A	Definições de imagem	Lista as definições de imagem criadas anteriormente.
B	Versões de imagem	Exibe as versões de imagem da definição de imagem selecionada.

RÓTULO	PARTE	DESCRIÇÃO
C	Detalhes	• A guia **Detalhes** exibe informações detalhadas sobre a definição ou versão de imagem selecionada, como Imagem Mestra, Recurso, Hypervisor, nome da definição de imagem, tipo de SO e tipo de sessão. • A guia **Esquema de Imagem** exibe informações sobre o modelo usado para preparar imagens, como disco rígido, tamanho da máquina, tipo de licença, conjunto de criptografia de disco, perfil da máquina e

RÓTULO	PARTE	DESCRIÇÃO
		assim por diante. • A guia **Esquemas de Provisionamento** exibe o nome do esquema de provisionamento usado para criar o catálogo. • A guia **Solução de Problemas** fornece o status de erro da versão de imagem selecionada.
D	Barra de ações	Lista as ações que você pode realizar em definições e versões de imagem, como **Criar Versão da Imagem**, **Editar Descrição**, **Excluir Versão da Imagem** e **Criar Catálogo**.

Criar um catálogo de máquinas usando a imagem preparada

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo.

Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. Faça login no Web Studio e selecione o nó **Imagens**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição da imagem.
3. Na página **Imagem**, selecione **Recursos** e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

   > **Observação:**
   >
   > Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. (Somente para Azure) Na página **Tipos de Armazenamento e Licenças**, selecione o tipo de armazenamento e licença a ser usado como parte do processo de preparação da imagem.

   > **Observação:**
   >
   > Se você selecionar um perfil de máquina na página **Imagem**, o tipo de licença do perfil de máquina será pré-selecionado com base na configuração do perfil.

5. Na página **Especificação da Máquina**:

   - Para Azure, selecione um tamanho de máquina. Se você selecionar um perfil de máquina na página **Imagem**, o tamanho da máquina do perfil de máquina será selecionado por padrão.
   - Para VMware, se você selecionar um perfil de máquina, poderá ver a contagem de CPU Virtual derivada do perfil de máquina e ela será inalterável. Se você não selecionar um perfil de máquina, poderá ver apenas o tamanho da memória derivado da imagem mestre.

6. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada.

   Para VMware, se você não selecionar um perfil de máquina, a NIC associada à imagem mestre será selecionada por padrão. Se você selecionar um perfil de máquina, as NICs serão derivadas do perfil de máquina e a contagem será inalterável.

> **Observação:**
>
> Múltiplas NICs não são suportadas no Azure.

7. (Somente para Azure) Na página **Configurações de Disco**, selecione a chave de criptografia gerenciada pelo cliente (CMEK). Se o perfil de máquina não tiver uma CMEK, mas a imagem mestre tiver, ele pré-selecionará a CMEK da imagem mestre.
8. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
9. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

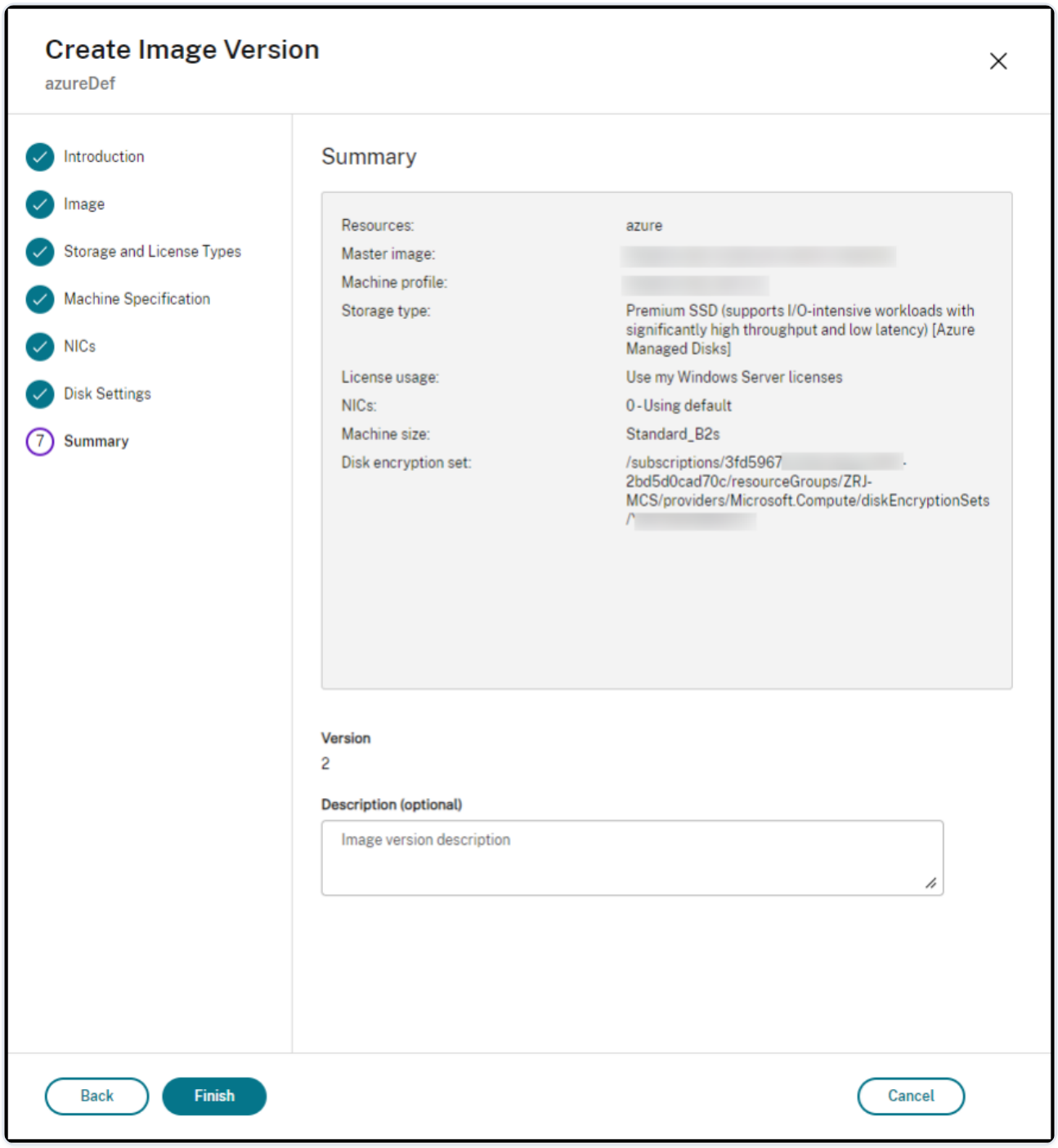
Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Observação:**
>
> A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá para o nó **Imagens**, selecione uma versão de imagem e selecione **Criar Versão da Imagem**.
2. Se você quiser que a configuração da versão da imagem seja diferente da versão da imagem configurada inicialmente, configure as definições nas páginas **Imagem**, **Tipos de Armazenamento e Licença**, **Especificação da Máquina**, **NICs** e **Configurações de Disco** da caixa de diálogo **Criar Versão da Imagem**.
3. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.



Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho necessária.
3. Da página **Imagem** à página **Configurações de Disco**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. (Para Azure) Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
5. Conclua as configurações nas páginas seguintes.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
7. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de Máquina** e **Gerenciamento de Máquinas**.
3. Na página **Imagem**:
    a. Selecione **Imagem preparada**.
    b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem.
    c. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
    d. Se a versão da imagem selecionada estiver configurada com um perfil de máquina, selecione um perfil de máquina. Se a versão da imagem selecionada não estiver configurada com um perfil de máquina, você não poderá optar por usar um perfil de máquina.
4. Configure as configurações nas páginas a seguir.
5. Na página **Configurações de Disco**, se a imagem preparada selecionada usar um conjunto de criptografia de disco, você não poderá remover o conjunto de criptografia, mas poderá alterar a chave para outra chave de criptografia.

6. (Para Azure) Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
7. Conclua as configurações nas páginas seguintes.
8. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

Atualizar um catálogo de máquinas com uma imagem preparada diferente

Para atualizar um catálogo de máquinas MCS existente com uma imagem preparada diferente, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo e selecione um catálogo de máquinas que você deseja atualizar. Clique com o botão direito e selecione **Alterar Imagem Preparada**.
2. Na página **Imagem**, selecione uma imagem preparada.
3. Na página **Estratégia de implantação**, selecione quando você deseja atualizar este catálogo com a imagem preparada selecionada.
4. Na página **Resumo**, verifique os detalhes. Clique em **Concluir**.

Você pode ver o histórico de alterações de imagem feitas em um catálogo. Para ver o histórico, faça o seguinte:

1. Selecione um catálogo de máquinas.
2. Na guia **Propriedades do Modelo**, no campo **Imagem preparada**, clique em **Exibir histórico da imagem**.

Gerenciar as definições e versões de imagem

Você pode editar e excluir as definições e versões de imagem para gerenciar o uso de várias versões e definições de imagem criadas.

Editar uma definição de imagem

Você pode editar o nome e a descrição de uma definição de imagem.

Para editar uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Editar Definição de Imagem**.

Editar versão da imagem

Você pode editar a descrição de uma versão de imagem para especificar a finalidade dessa versão de imagem.

Para editar uma versão de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem e selecione **Editar Descrição**.

Excluir uma versão de imagem

Para excluir uma versão de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem e selecione **Excluir Versão da Imagem**.

> **Observação:**
>
> Você não pode excluir uma versão de imagem se ela for usada por um catálogo de máquinas.

Excluir uma definição de imagem

Para excluir uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Excluir Definição da Imagem**.

> **Observação:**
>
> Você não pode excluir uma definição de imagem se ela contiver uma versão de imagem.

Gerenciamento do ciclo de vida da imagem usando PowerShell

Se você quiser usar comandos PowerShell para criar um esquema de provisionamento, deverá criar uma especificação de versão de imagem preparada com base na especificação de versão de imagem mestre, conforme necessário para seu ambiente.

Especificação de versão da imagem mestre: Uma especificação de versão da imagem mestre é uma imagem específica adicionada ou criada sob uma versão de imagem. Você pode adicionar uma imagem existente no hipervisor como uma especificação de versão da imagem mestre ou criar uma especificação de versão de imagem preparada com base na especificação de versão da

imagem mestre, conforme necessário para seu ambiente. A especificação de versão de imagem preparada pode ser usada para vários esquemas de provisionamento.

O ciclo de vida de uma imagem ao usar comandos PowerShell é:

1. Criar uma imagem:
    a. Criar uma definição de imagem.
    b. Criar uma versão de imagem.
    c. Adicionar uma especificação de versão de imagem mestre.
    d. Criar uma especificação de versão de imagem preparada.
2. Criar um catálogo de máquinas MCS usando uma especificação de versão de imagem preparada:
    a. Criar um catálogo de broker.
    b. Crie um pool de identidades.
    c. Criar um esquema de provisionamento com o parâmetro Uid da especificação de versão de imagem preparada usando o comando `New-ProvScheme`.
    d. Vincular o catálogo de broker ao esquema de provisionamento.
3. Criar VMs no catálogo de máquinas MCS.
4. Alterar a especificação de versão de imagem preparada de um esquema de provisionamento usando o comando `Set-ProvScheme`.
5. Gerenciar as definições e versões de imagem: Editar as versões e definições de imagem.
6. Excluir um catálogo de máquinas MCS: A ordem de exclusão é: especificação de versão de imagem preparada > especificação de versão de imagem mestre > versão de imagem > definição de imagem. Antes de excluir a especificação de versão de imagem, certifique-se de que a especificação de versão de imagem preparada não esteja associada a nenhum catálogo de máquinas MCS.

Usar PowerShell

Você pode fazer o seguinte usando comandos PowerShell:

- Criar uma imagem preparada
- Criar um catálogo usando a especificação de versão de imagem preparada
- Atualizar um catálogo usando a especificação de versão de imagem preparada

- Excluir definição de imagem, versão de imagem e especificação de versão de imagem preparada
- Gerenciar definição de imagem e versão de imagem
- Obter detalhes da definição de imagem, versão de imagem, especificação de versão de imagem preparada e esquema de provisionamento

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

   ```
   New-ProvImageVersion -ImageDefinitionName image1 -Description "version
   1"
   ```

4. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

   ```
   Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
   ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
   \HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
   22-snapshot.snapshot"
   ```

   Observação:

> Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

5. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"

-ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

> **Observação:**
>
> Uma unidade de hospedagem e tipo de preparação podem ter apenas uma instância preparada.

Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada no Azure:

```
$ImageDefintion = New-ProvImageDefinition

-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
MultiSession

 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win2022-
```

```
snapshot.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName azure -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"} -ServiceOffering
"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"></CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada no VMware:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2
-OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously
```

```
Get-ProvTask -TaskId $Task.TaskId
```

Observação:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.
- Não é possível especificar um grupo de recursos ao criar uma especificação de versão de imagem.

Criar um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
```

```
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo no Azure:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /></
CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo no VMware:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Atualizar um catálogo usando uma especificação de versão de imagem preparada

Você pode atualizar um catálogo usando o comando `Set-ProvSchemeImage`. Por exemplo,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

Ou,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

Exemplo do conjunto completo de comandos Powershell para atualizar um catálogo:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"

Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

Excluir definição de imagem, versão de imagem e especificação de versão de imagem preparada

Considere o seguinte antes de excluir uma definição de imagem, versão de imagem e especificação de versão de imagem preparada:

- Uma definição de imagem não pode ser excluída se contiver alguma versão de imagem.
- Uma versão de imagem não pode ser excluída se contiver alguma especificação de versão de imagem.
- Uma especificação de versão de imagem mestre não pode ser excluída se for usada por qualquer outra especificação de versão de imagem preparada.
- Uma especificação de versão de imagem preparada não pode ser excluída se for usada por qualquer esquema de provisionamento.

Os passos detalhados são os seguintes:

1. Remover uma especificação de versão de imagem preparada. Por exemplo,

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec
   -ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
   "PreparationType -eq 'Mcs'"

   Remove-ProvImageVersionSpec -ImageVersionSpecUid
   $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
   ```

   Observação:

   A especificação de versão de imagem mestre só pode ser excluída quando não houver nenhuma especificação de versão de imagem preparada associada.

2. Remover especificação de versão de imagem mestre. Por exemplo,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

3. Remover uma versão de imagem. Por exemplo,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

4. Remover uma definição de imagem. Por exemplo,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos do PowerShell:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1

Remove-ProvImageDefinition -ImageDefinitionName image1
```

Gerenciar definição de imagem e versão de imagem

Você pode renomear e editar uma definição de imagem, e editar uma versão de imagem.

- Renomear uma definição de imagem usando o comando `Rename-ProvImageDefinition`. Por exemplo:

```
Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
-NewImageDefinitionName <string>
```

Ou,

```
Rename-ProvImageDefinition -ImageDefinitionName <string>
-NewImageDefinitionName <string>
```

- Editar uma definição de imagem usando o comando `Set-ProvImageDefinition`. Por exemplo:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
<string>]
```

Ou,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- Editar uma versão de imagem usando o comando `Set-ProvImageVersion`. Por exemplo:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

Ou,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

Obter detalhes de definição de imagem, versão de imagem, especificação de versão de imagem preparada e esquema de provisionamento

- Obtenha detalhes da definição da imagem usando o comando `Get-ProvImageDefinition`. Por exemplo:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- Obtenha detalhes da versão da imagem usando o comando `Get-ProvImageVersion`. Por exemplo:
  - Para listar as versões de imagem em uma definição de imagem,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Para obter um detalhe da versão da imagem,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    -ImageVersionNumber <int>
    ```

- Obtenha a especificação da versão da imagem preparada usando o comando `Get-ProvImageVersionSpec`. Por exemplo:
  - Para listar todas as especificações de versão de imagem preparada em uma versão de imagem,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - Para listar as especificações da versão da imagem mestre em uma especificação da versão da imagem preparada,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "None"'
    ```

  - Para listar as especificações da versão da imagem preparada em uma versão da imagem, que está associada a uma imagem mestre,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

- Para obter especificações de versão de imagem preparada bem-sucedidas em uma versão de imagem,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

- Para obter um detalhe da especificação da versão da imagem preparada,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Obtenha detalhes do esquema de provisionamento usando o comando `Get-ProvScheme`. Por exemplo:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- Obtenha o histórico da especificação da versão da imagem preparada de um esquema de provisionamento usando o comando `Get-ProvSchemeImageVersionSpecHistory`. Por exemplo:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

Criar catálogos de máquinas

Importante:

A partir do Citrix Virtual Apps and Desktops™ 7 2006, se sua implantação atual usar alguma das seguintes tecnologias, você poderá atualizar sua implantação para a versão atual somente após remover os itens de Fim de Vida (EOL) que usam essas tecnologias.

- vDisks Pessoais (PvDs)
- AppDisks™
- Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic

Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

Nota:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Se você deseja usar conexões de host de nuvem pública para sua implantação, você precisa de uma Licença de Direitos Híbridos para concluir sua nova instalação ou atualização para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização pausa ou para. Uma mensagem explicativa aparece. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Introdução

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 multi-sessão ou SO de sessão única, e máquinas Windows ou Linux.

O Web Studio o guia para criar o primeiro catálogo de máquinas depois de criar o site. Depois de criar o primeiro catálogo, o Web Studio o guia para criar o primeiro grupo de entrega. Mais tarde, você pode alterar o catálogo que criou e criar mais catálogos.

Dica:

A atualização de uma implantação existente habilita o recurso de otimização de armazenamento do Machine Creation Services (MCS) (MCS I/O), nenhuma configuração adicional é necessária. A atualização do Virtual Delivery Agent (VDA) e do Delivery Controller manipular a atualização do MCS I/O.

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.

Considere:

- O MCS suporta um único disco de sistema da imagem da máquina virtual. Ele ignora o restante dos discos de dados anexados a essa imagem.
- Se você usa o MCS para provisionar VMs, você fornece uma imagem mestre (ou snapshot de uma imagem) para criar VMs idênticas no catálogo. Antes de criar o catálogo, você primeiro usa as ferramentas para criar e configurar a imagem mestre. Este processo inclui a instalação de um Virtual Delivery Agent (VDA) na imagem. Em seguida, você cria o catálogo de máquinas no Web Studio. Você seleciona essa imagem (ou snapshot), especifica o número de VMs a serem criadas no catálogo e configura informações adicionais.
- Se suas máquinas já estiverem disponíveis, você ainda deve criar um ou mais catálogos de máquinas para essas máquinas.
- Se você estiver criando um catálogo usando o SDK do PowerShell diretamente, poderá especificar um modelo de hipervisor (**VMTemplates**), em vez de uma imagem ou um instantâneo.
- Usar um modelo para provisionar um catálogo é considerado um recurso experimental. Ao usar esse método, a preparação da máquina virtual pode falhar. Como resultado, o catálogo não pode ser publicado usando o modelo.

Ao usar o MCS ou o Citrix Provisioning™ para criar o primeiro catálogo, você usa a conexão de host que configurou ao criar o site. Mais tarde (depois de criar seu primeiro catálogo e grupo de entrega), você pode alterar informações sobre essa conexão ou criar mais conexões.

Depois de concluir o assistente de criação de catálogo, os testes são executados automaticamente para garantir que ele esteja configurado corretamente. Quando os testes são concluídos, você pode visualizar um relatório de teste. Execute os testes a qualquer momento no Web Studio.

> **Observação:**
>
> O MCS não oferece suporte ao Windows 10 IoT Core e ao Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

> Para obter detalhes técnicos sobre as ferramentas do Citrix Provisioning, consulte Gerenciamento de Imagens do Citrix Virtual Apps and Desktops.

Verificação de licença RDS

Atualmente, o Web Studio não verifica licenças RDS da Microsoft válidas ao criar um catálogo de máquinas que contém máquinas de SO multi-sessão do Windows. Para visualizar o status da licença RDS da Microsoft para uma **máquina de SO multi-sessão** do Windows, vá para o Citrix Director. Visualize o status da licença RDS da Microsoft no painel **Detalhes da Máquina**. Este painel está na página **Detalhes da Máquina e Detalhes do Usuário**. Para obter mais informações, consulte Integridade da licença RDS da Microsoft.

Registro de VDA

Um VDA deve ser registrado em um Delivery Controller™ ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos que, de outra forma, estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador pode solucionar. O Web Studio fornece informações de solução de problemas no assistente de criação de catálogo e depois que você adiciona máquinas de um catálogo a um grupo de entrega.

Depois de adicionar máquinas existentes usando o assistente, a lista de nomes de contas de computador indica se cada máquina é adequada para ser adicionada ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre essa máquina.

Se a mensagem identificar uma máquina problemática, remova essa máquina ou adicione-a. Por exemplo, se uma mensagem indicar que as informações podem não ser obtidas sobre uma máquina, adicione a máquina de qualquer maneira.

Para obter mais informações, consulte:

- CTX136668 para orientação sobre solução de problemas de registro de VDA
- Versões e níveis funcionais do VDA
- Métodos de registro de VDA

Resumo da criação de catálogo MCS

Aqui está uma breve visão geral das ações padrão do MCS depois que você fornece informações no assistente de criação de catálogo.

- Se você selecionou uma imagem mestre (em vez de um instantâneo), o MCS cria um instantâneo.
- O MCS cria uma cópia completa do snapshot e a coloca em cada local de armazenamento definido na conexão do host.
- O MCS adiciona as máquinas ao Active Directory, o que cria identidades exclusivas.
- O MCS cria o número de VMs especificado no assistente, com dois discos definidos para cada VM. Além dos dois discos por VM, um mestre também é armazenado no mesmo local de armazenamento. Se você tiver vários locais de armazenamento definidos, cada um receberá os seguintes tipos de disco:
    - A cópia completa do 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 única. Cada VM recebe um disco de identidade.
    - Um disco de diferença exclusivo para armazenar gravações feitas na VM. Este disco é provisionado de forma dinâmica (se suportado pelo armazenamento do host) e aumenta para o tamanho máximo da imagem mestre, se necessário. Cada VM recebe um disco de diferença. O disco de diferença mantém as alterações feitas durante as sessões. É permanente para desktops dedicados. Para desktops agrupados, ele é excluído e um novo é criado após cada reinício via controlador de entrega.

Alternativamente, ao criar VMs para entregar desktops estáticos, você pode especificar (na página **Máquinas** do assistente de criação de catálogo) clones de VM espessos (cópia completa). Clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem seu próprio arquivo.

Considerações de armazenamento do MCS

Existem muitos fatores ao decidir sobre soluções de armazenamento, configurações e capacidades para o MCS. As informações a seguir fornecem considerações adequadas para a capacidade de armazenamento:

Considerações de capacidade:

- Discos

  Os discos Delta ou de Diferença (Diff) consomem a maior quantidade de espaço na maioria das implantações do MCS para cada VM. Cada VM criada pelo MCS recebe no mínimo 2 discos na criação.

  - Disk0 = Disco de Diferença: contém o SO quando copiado da Imagem Base Mestra.
  - Disk1 = Disco de Identidade: 16 MB - contém dados do Active Directory para cada VM.

  À medida que o produto evolui, pode ser necessário adicionar mais discos para satisfazer certos casos de uso e consumo de recursos. Por exemplo:

  - Otimização de Armazenamento MCS cria um disco estilo cache de gravação para cada VM.
  - O MCS adicionou a capacidade de usar clones completos em oposição ao cenário de disco Delta descrito na seção anterior.

  Recursos do hipervisor também podem entrar na equação. Por exemplo:

  - XenServer IntelliCache cria um Disco de Leitura no armazenamento local para cada XenServer. Esta opção economiza IOPS em relação à imagem mestre, que pode estar localizada no armazenamento compartilhado.

- Sobrecarga do hypervisor

  Diferentes hypervisors usam arquivos específicos que criam sobrecarga para VMs. Os hypervisors também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir a sobrecarga para:

  - Arquivos de log
  - Arquivos específicos do hipervisor. Por exemplo:
    - O VMware adiciona mais arquivos à pasta **VM storage**. Consulte Melhores Práticas do VMware.

        - Calcule os requisitos totais de tamanho da sua máquina virtual. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de troca e 100 MB para arquivos de log, consumindo um total de 36,1 GB.

    - Snapshots para XenServer; Snapshots para VMware.

- Sobrecarga de processo

  A criação de um catálogo, a adição de uma máquina e a atualização de um catálogo têm implicações de armazenamento únicas. Por exemplo:

    - Criação inicial do catálogo requer que uma cópia do disco base seja copiada para cada local de armazenamento.

        - Também exige que você crie uma VM de Preparação temporariamente.

    - Adicionar uma máquina a um catálogo não requer a cópia do disco base para cada local de armazenamento. A criação do catálogo varia com base nos recursos selecionados.
    - Atualizar o catálogo para criar um disco base extra em cada local de armazenamento. As atualizações do catálogo também experimentam um pico temporário de armazenamento onde cada VM no catálogo tem 2 discos Diff por um certo período de tempo.

Mais considerações:

- **Dimensionamento da RAM:** Afeta o tamanho de certos arquivos e discos do hypervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de snapshot.
- **Thin / Thick provisioning:** O armazenamento NFS é preferido devido aos recursos de provisionamento thin.

Otimização de armazenamento do Machine Creation Services (MCS)

Com o recurso de otimização de armazenamento do Machine Creation Services (MCS), referido como MCS I/O:

- O contêiner de cache de gravação é *baseado em arquivo*, a mesma funcionalidade encontrada no Citrix Provisioning. Por exemplo, o nome do arquivo de cache de gravação do Citrix Provisioning é `D:\vdiskdif.vhdx` e o nome do arquivo de cache de gravação do MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico incluindo suporte para um arquivo de despejo de memória do Windows gravado no disco de cache de gravação.

- O MCS I/O mantém a tecnologia *cache na RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação de várias camadas mais otimizada. Essa funcionalidade permite que um administrador equilibre o custo em cada camada, RAM e disco, e o desempenho para atender à expectativa de carga de trabalho desejada.

A atualização do método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. O MCS I/O não oferece mais suporte a cache somente RAM. Especifique um tamanho de disco no Web Studio durante a criação do catálogo de máquinas.
2. O disco de cache de gravação da VM é criado e formatado automaticamente ao inicializar uma VM pela primeira vez. Assim que a VM estiver ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.
3. O arquivo de paginação é redirecionado para este volume formatado, `MCSWCDisk`. Como resultado, esse tamanho de disco considera a quantidade total de espaço em disco. Ele inclui o delta entre o tamanho do disco e a carga de trabalho gerada mais o tamanho do arquivo de paginação. Isso geralmente está associado ao tamanho da RAM da VM.

Habilitando atualizações de otimização de armazenamento do MCS

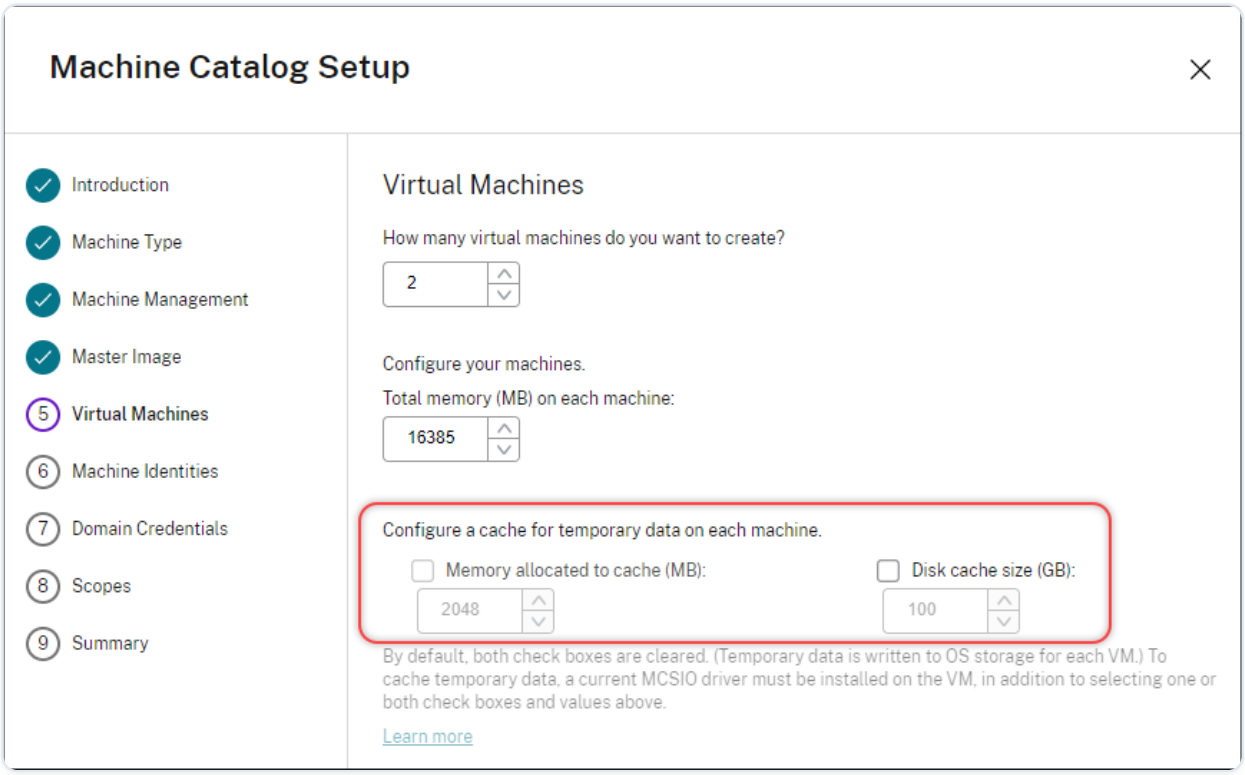
Para habilitar a funcionalidade de otimização de armazenamento do MCS I/O, atualize o Delivery Controller e o VDA para a versão mais recente do Citrix Virtual Apps and Desktops.

> **Observação:**

> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será necessária. A atualização do VDA e do Delivery Controller manipular a atualização do MCS I/O.

> Ao habilitar a atualização de otimização de armazenamento do MCS, considere o seguinte:

- Ao criar um catálogo de máquinas, o administrador pode configurar o tamanho da RAM e do disco.



- Atualizar um catálogo de máquinas existente para um novo snapshot de VM contendo um VDA configurado para a versão 1903 resulta no seguinte comportamento: o novo snapshot continua a usar a configuração de E/S do MCS do catálogo existente para RAM e tamanho do disco. O disco bruto existente é formatado.

Importante:

A otimização de armazenamento do MCS mudou com o Citrix Virtual Apps and Desktops versão 1903. Esta versão suporta tecnologia de cache de gravação baseada em arquivo, proporcionando melhor desempenho e estabilidade. A nova funcionalidade fornecida pelo MCS I/O pode exigir um requisito de armazenamento de cache de gravação maior em comparação com as versões anteriores do Citrix Virtual Apps and Desktops. A Citrix recomenda que você reavalie o tamanho do disco para garantir que ele tenha espaço em disco suficiente para o fluxo de trabalho alocado e um tamanho de arquivo de paginação extra. O tamanho do arquivo de paginação geralmente está relacionado à quantidade de RAM do sistema. Se o tamanho do disco do catálogo existente for insuficiente, crie um catálogo de máquinas e aloque um disco de cache de gravação maior.

Atribuir uma letra de unidade específica ao disco de cache de write-back do MCS I/O

Você pode atribuir uma letra de unidade específica ao disco de cache de write-back do MCS I/O. Essa implementação ajuda a evitar conflitos entre a letra da unidade de quaisquer aplicativos que você usa e a letra da unidade do disco de cache de write-back do MCS I/O. Para atribuir uma letra de unidade ao disco de cache de write-back do MCS I/O, você pode usar comandos PowerShell. Os hipervisores suportados são Azure, GCP, VMware, SCVMM e XenServer.

> **Observação:**
>
> Este recurso requer a versão 2305 do VDA ou posterior.

Limitações

- Aplicável apenas ao sistema operacional Windows
- Letra de unidade aplicável para disco de cache de write-back: `E` a `Z`
- Não aplicável quando o disco temporário do Azure é usado como disco de cache de write-back
- Aplicável somente ao criar um novo catálogo de máquinas

Atribuir uma letra de unidade ao disco de cache de write-back

Para atribuir uma letra de unidade a um disco de cache de write-back:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades se ainda não tiver sido criado.
4. Crie um esquema de provisionamento usando o comando `New-ProvScheme` com a propriedade `WriteBackCacheDriveLetter`. Por exemplo:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `
```

```
-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />
```

```
<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. Conclua a criação do catálogo. Para obter informações, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

Preparar uma imagem mestre

Para obter informações sobre como criar hosts de conexão, consulte Conexões e recursos.

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

É bom saber:

- Uma imagem mestre também pode ser conhecida como imagem clone, imagem dourada, VM base ou imagem base. Os fornecedores de host usam termos diferentes.
- Certifique-se de que o host tenha processadores, memória e armazenamento suficientes para acomodar o número de máquinas criadas.
- Configure a quantidade correta de espaço em disco rígido necessário para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo de máquinas.
- Os catálogos de máquinas do Acesso Remoto para PC não usam imagens mestre.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou VMware tools). Se você omitir esta etapa, os aplicativos e desktops podem não funcionar corretamente.
- Um VDA. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros conforme necessário, como software antivírus ou agentes de distribuição eletrônica de software. Configure os serviços com configurações apropriadas para os usuários e o tipo de máquina (como recursos de atualização).

- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda virtualizar aplicativos. A virtualização reduz custos, eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduzem o tamanho dos discos rígidos da imagem mestre, o que economiza custos de armazenamento.
- Clientes App-V com as configurações recomendadas, se você planeja publicar aplicativos App-V. O cliente App-V está disponível na Microsoft.
- Ao usar o MCS, se você localizar o Microsoft Windows, instale as localidades e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam as localidades e os pacotes de idiomas instalados.

> **Importante:**
>
> Se você estiver usando o MCS, não execute o Sysprep em imagens mestre.

Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e, em seguida, instale o sistema operacional, além de todos os service packs e atualizações. Especifique o número de vCPUs. Você também pode especificar o valor da vCPU se criar o catálogo de máquinas usando o PowerShell. Você não pode especificar o número de vCPUs ao criar um catálogo usando o Web Studio. Configure a quantidade de espaço em disco rígido necessária para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo.
2. Certifique-se de que o disco rígido esteja conectado no local do dispositivo 0. A maioria dos modelos de imagem mestre padrão configura este local por padrão, mas alguns modelos personalizados podem não fazê-lo.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, junte a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas. Se você estiver usando o MCS, não é necessário unir a imagem mestre a um domínio. As máquinas provisionadas são unidas ao domínio especificado no assistente de criação de catálogo.

5. A Citrix recomenda que você crie e nomeie um snapshot da sua imagem mestre. Se você especificar uma imagem mestre em vez de um snapshot ao criar um catálogo, o Web Studio criará um snapshot. Você não pode nomeá-lo.

Ativação de licenciamento por volume

O MCS oferece suporte à ativação de licenciamento por volume para automatizar e gerenciar a ativação de sistemas operacionais Windows e Microsoft Office. Os três modelos que o MCS oferece suporte para ativação de licenciamento por volume são:

- Serviço de Gerenciamento de Chaves (KMS)
- Ativação baseada no Active Directory (ADBA)
- Chave de Ativação Múltipla (MAK)

Você pode alterar a configuração de ativação depois de criar o catálogo de máquinas.

Serviço de Gerenciamento de Chaves (KMS)

O KMS é um serviço leve que não requer um sistema dedicado e pode ser facilmente co-hospedado em um sistema que fornece outros serviços. Essa funcionalidade é suportada em todas as versões do Windows suportadas pela Citrix. Durante a preparação da imagem, o MCS faz o rearm do KMS do Microsoft Windows e do Microsoft Office. Você pode pular o rearm executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre o Rearm do KMS do Microsoft Windows e do Microsoft Office 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 Activate using Key Management Service.

> **Nota:**
>
> Todos os catálogos de máquinas criados após a execução do comando `Set-Provserviceconfigurationdata` têm a mesma configuração fornecida no comando.

Ativação baseada no Active Directory (ADBA)

O ADBA permite ativar máquinas por meio de suas conexões de domínio. As máquinas são ativadas imediatamente quando ingressam no domínio. Essas máquinas permanecem ativadas enquanto permanecerem ingressadas no domínio e em contato com ele. Essa funcionalidade é suportada em todas as versões do Windows compatíveis com Citrix. Para obter mais informações

sobre a ativação baseada no Active Directory, consulte Ativar usando ativação baseada no Active Directory.

Chave de Ativação Múltipla (MAK)

MAK é uma forma de ativar o volume e autenticar o sistema Windows com a ajuda do servidor Microsoft. Você deve comprar a chave MAK da Microsoft, que é atribuída a um número fixo de contagens de ativação. Cada vez que um sistema Windows é ativado, a contagem de ativação é reduzida. Existem duas maneiras de ativar o sistema:

- Ativação Online: Se o sistema Windows que você deseja ativar tiver acesso à internet, o sistema ativa automaticamente o Windows ao instalar a chave do produto. Esse processo reduz a contagem de ativação em 1 para o MAK correspondente.
- Ativação Offline: Se o sistema Windows não conseguir se conectar à internet para fazer a ativação online, o MCS obtém um ID de confirmação e um ID de instalação do servidor Microsoft para ativar o sistema Windows. Essa forma de ativação é útil para catálogos de máquinas não persistentes.

> **Nota:**
>
> - O MCS não oferece suporte à ativação do Microsoft Office usando MAK.
> - A versão mínima do VDA necessária é 2303.

Requisitos principais

- O Delivery Controller deve ter acesso à internet.
- Crie um novo catálogo se a nova imagem a ser atualizada tiver uma Chave MAK diferente da original.
- Instale a chave MAK na imagem mestre. Consulte Implantar Ativação MAK para obter as etapas para instalar a Chave MAK em um Sistema Windows.
- Se você não estiver usando a preparação de imagem:

  a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

  b. Defina o valor como `1`.

Contagens de Ativação

Para visualizar o número de ativações restantes para a Chave MAK ou para verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação de Volume (VAMT). Consulte Instalar VAMT.

Ativar o sistema Windows usando MAK

Para ativar o sistema Windows usando MAK:

1. Instale a chave do produto na imagem mestre. Esta etapa consome uma contagem de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagem:

   a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

   b. Defina o valor como `1`.

   Este método desabilita a opção de ativação online.
4. Adicione VMs ao catálogo de máquinas.
5. Ligar as VMs.
6. Dependendo se é ativação online ou offline, o sistema Windows é ativado.

   - Se a ativação for online, o sistema Windows é ativado após a instalação da chave do produto.
   - Se a ativação for offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. O MCS então recupera um ID de confirmação e um ID de instalação do servidor Microsoft. Esses IDs são usados para ativar o sistema Windows.

Solução de problemas

Se a VM provisionada não for ativada com a chave MAK instalada, execute o comando `Get-ProvVM` ou `Get-ProvScheme` em uma janela do PowerShell.

- O comando `Get-ProvScheme`: Consulte o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS da imagem mestre mais recente.

- O comando `Get-ProvVM`. Consulte os parâmetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Você pode verificar o erro e as etapas para resolver o problema.

Criar um catálogo de máquinas usando o Web Studio

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 e outros recursos que hospedam suas máquinas.
- Se você criou uma imagem mestre para provisionar máquinas, certifique-se de ter instalado um VDA nessa imagem.

Para iniciar o assistente de criação de catálogo:

1. Se este for o primeiro catálogo a ser criado, você será guiado para a seleção correta (como "Configurar as máquinas e criar catálogos de máquinas para executar aplicativos e desktops"). O assistente de criação de catálogo é aberto.
2. Se você já criou um catálogo e deseja criar outro, siga estas etapas:
    a. Faça login no Web Studio, selecione **Catálogos de Máquinas** no painel esquerdo e, em seguida, selecione **Criar Catálogo de Máquinas** na barra de ações.
    b. Para organizar catálogos usando pastas, crie pastas sob a pasta padrão **Catálogos de Máquinas**. Para obter mais informações, consulte Criar uma pasta de catálogo.
    c. Selecione a pasta onde você deseja criar o catálogo e clique em **Criar Catálogo de Máquinas**. O assistente de criação de catálogo é aberto.

O assistente o guiará pelos seguintes itens. As páginas do assistente que você vê diferem, dependendo das seleções que você faz.

Sistema operacional

Cada catálogo contém máquinas de apenas um tipo. Selecione um.

- **SO de várias sessões:** Um catálogo de SO de várias sessões fornece desktops compartilhados hospedados. As máquinas podem estar executando versões compatíveis dos

sistemas operacionais Windows ou Linux, mas o catálogo não pode conter ambos. (Consulte a documentação do Linux VDA para obter detalhes sobre esse SO.)

- **SO de sessão única:** Um catálogo de SO de sessão única fornece desktops VDI que você pode atribuir a vários usuários diferentes.
- **Acesso Remoto a PC:** Um catálogo de Acesso Remoto a PC fornece aos usuários acesso remoto às suas máquinas de desktop físicas do escritório. O Acesso Remoto a PC não requer uma VPN para fornecer segurança.

Gerenciamento de máquinas

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

A página **Gerenciamento de Máquinas** indica como as máquinas são gerenciadas e quais ferramentas você usa para implantar máquinas.

Escolha se as máquinas no catálogo são gerenciadas por energia através do Web Studio.

- As máquinas são gerenciadas em termos de energia através do Web Studio, por exemplo, VMs ou PCs blade. Esta opção está disponível apenas se você já configurou uma conexão com um host.
- As máquinas não são gerenciadas em termos de energia através do Web Studio, por exemplo, máquinas físicas.

Se você indicou que as máquinas são gerenciadas em termos de energia através do Web Studio, escolha qual ferramenta usar para criar VMs.

- Tecnologia Citrix Provisioning
    - **Citrix Machine Creation Services (MCS)** Cria um catálogo de VMs provisionadas e com imagem usando o MCS. O MCS copia imagens clonadas de uma imagem mestre para essas VMs.
    - **Citrix Provisioning Services (PVS)** Cria um catálogo de VMs provisionadas usando o MCS e com imagem usando o PVS. Essas VMs servem como dispositivos de destino PVS e o servidor PVS pode transmitir uma única imagem de disco compartilhada para elas.

> **Observação:**

- Esta opção está disponível apenas para sites PVS registrados com o Citrix Cloud™ e está atualmente limitada a recursos do Azure.
- Ao criar um catálogo do Citrix Provisioning, na página **Target Device**, você pode ver que no menu suspenso para selecionar a farm e o site para as máquinas a serem provisionadas, há farms e sites listados que não existem mais. Como solução alternativa, você pode executar o comando PowerShell `Unregister-HypPvsSite` para remover as farms e os sites do banco de dados. Para obter informações sobre o comando PowerShell, consulte Unregister-HypPvsSite.

- **Outro serviço ou tecnologia** Uma ferramenta que gerencia máquinas já existentes no data center. A Citrix recomenda que você use o Microsoft System Center Configuration Manager ou outro aplicativo de terceiros para garantir que as máquinas no catálogo sejam consistentes.

Tipos de desktop (experiência de desktop)

Observação:

As opções na página **Experiência de Desktop** variam de acordo com o tipo de máquina que você seleciona na página **Tipo de Máquina**.

- Para máquinas com **SO multi-sessão**, os usuários recebem um desktop aleatório cada vez que fazem logon. Selecione uma das seguintes opções:
  - **Sim, salve as alterações no disco local da máquina que hospeda os desktops virtuais.** (Persistente)
  - **Não, descarte todas as alterações e limpe os desktops virtuais quando o usuário fizer logoff.** (Não persistente)

  Observação:

  Para máquinas multissessão persistentes, as alterações que os usuários fazem nos desktops serão salvas e acessíveis a todos os usuários autorizados.

- Para máquinas com **SO de sessão única**, você obtém as seguintes opções na página **Experiência de Desktop**:

- **Quero que os usuários se conectem a um novo desktop (aleatório) cada vez que fizerem logon.**
- **Quero que os usuários se conectem ao mesmo desktop (estático) cada vez que fizerem logon.**

  Para desktops estáticos, você pode decidir se as alterações feitas pelos usuários serão salvas ou descartadas após o logoff.

Imagem e perfil da máquina

Esta página aparece apenas quando você está usando o MCS para criar VMs.

1. Selecione um tipo de imagem para o catálogo de máquinas e, em seguida, selecione uma imagem. Dois tipos de imagem estão disponíveis:

   - **Imagem mestre.** Uma imagem que ainda não passou pelo processo de preparação de imagem. O processo de preparação de imagem é iniciado automaticamente quando a criação do catálogo começa.

     > **Observação:**
     >
     > - Ao usar o MCS, não execute o Sysprep em imagens mestre.
     > - Se você especificar uma imagem mestre em vez de um instantâneo, o Web Studio criará um instantâneo, mas você não poderá nomeá-lo.

   - **Imagem preparada.** Uma imagem que passou pelo processo de preparação de imagem e pode ser usada diretamente para a criação de VMs. Optar por imagens preparadas em vez de imagens mestre durante a criação do catálogo garante uma criação de catálogo de máquinas mais rápida e confiável, juntamente com um gerenciamento simplificado do ciclo de vida da imagem.

     > **Observação:**
     >
     > - VMs criadas usando imagens preparadas não suportam hibernação.
     > - Atualmente, a criação de catálogos usando imagens preparadas está disponível apenas em ambientes Azure e VMware.

Para obter mais informações sobre como criar imagens preparadas, consulte Gerenciamento de imagens (visualização).

Ao selecionar uma imagem, você pode adicionar uma nota para a imagem selecionada, se necessário.

Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada. Não altere a seleção mínima padrão do VDA. No entanto, se você precisar usar uma versão anterior do VDA, consulte Versões do VDA e níveis funcionais.

Uma mensagem de erro aparece se você selecionar um snapshot ou VM que não seja compatível com a tecnologia de gerenciamento de máquinas selecionada anteriormente no assistente.

2. Para usar uma VM existente como perfil de máquina, selecione **Usar um perfil de máquina** e, em seguida, selecione a VM.

   Observação:

   Atualmente, o uso de perfis de máquina é restrito a VMs do Azure, AWS, GCP e VMware.

   Para implantações VMware, ao criar um catálogo de máquinas usando um perfil de máquina, você deve especificar a pasta onde deseja manter as máquinas virtuais.

   Para fornecer o local da pasta da máquina virtual, no assistente de criação de catálogo, vá para a página **Máquinas Virtuais**, e vá para a seção **Selecionar uma pasta para colocar as máquinas** e selecione o local da pasta da máquina virtual. Se não for especificado, o sistema considera a pasta do perfil de máquina selecionado como o local padrão.

3. Selecione o nível funcional mínimo para o catálogo. Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada.

Máquinas

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

O título desta página depende do que você selecionou na página **Gerenciamento de Máquinas**: **Máquinas**, **Máquinas Virtuais** ou **VMs e usuários**.

Ao usar o MCS:

- Especifique quantas máquinas virtuais devem ser criadas. Digite **0** (zero) se não quiser criar nenhuma. Mais tarde, você pode criar VMs para um catálogo vazio executando **Adicionar máquinas**.
- Escolha a quantidade de memória (em MB) que cada VM terá.
- Cada VM criada tem um disco rígido. Seu tamanho é definido na imagem mestre. Você não pode alterar o tamanho do disco rígido no catálogo.
- Se sua implantação contiver mais de uma zona, você poderá selecionar uma zona para o catálogo.
- Se você estiver criando VMs de desktop estáticas, selecione um modo de cópia de máquina virtual. Consulte Modo de cópia de máquina virtual.
- Se você estiver criando VMs de desktop aleatórias que não usam vDisks, poderá configurar um cache para ser usado para dados temporários em cada máquina. Consulte Configurar cache para dados temporários.

Ao usar outras ferramentas:

Adicione (ou importe uma lista de) nomes de contas de máquina do Active Directory. Você pode alterar o nome da conta do Active Directory para uma VM depois de adicioná-la/importá-la. Se você especificou máquinas estáticas na página **Experiência da Área de Trabalho**, você pode, opcionalmente, especificar o nome de usuário do Active Directory para cada VM que adicionar.

Depois de adicionar ou importar nomes, você pode usar o botão **Remover** para excluir nomes da lista, enquanto ainda estiver nesta página.

Ao usar outras ferramentas (mas não o MCS):

Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada) ajudam a identificar máquinas que podem não ser elegíveis para adicionar ao catálogo ou que não conseguem se registrar em um Delivery Controller. Para obter detalhes, consulte Versões de VDA e níveis funcionais.

Adicionar SIDs ao criar máquinas virtuais

Agora você pode adicionar o parâmetro `ADAccountSid` para identificar exclusivamente as máquinas ao criar novas máquinas virtuais.

Para fazer isso:

1. Crie um catálogo com o tipo de identidade compatível.
2. Adicione máquinas ao catálogo usando `NewProvVM`. Por exemplo:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta AD que não está no pool de identidades do catálogo
- Uma conta AD que não está em estado disponível

Modo de cópia da máquina virtual

O modo de cópia que você especifica na página **Máquinas** determina se o MCS cria clones finos (cópia rápida) ou espessos (cópia completa) a partir da imagem mestre. (Padrão = clones finos)

- Use clones de cópia rápida para um uso de armazenamento mais eficiente e criação de máquina mais rápida.
- Use clones de cópia completa para melhor recuperação de dados e suporte à migração, com IOPS potencialmente reduzidos após a criação das máquinas.

Versões de VDA e níveis funcionais

O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto requer um novo VDA. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não podem se registrar.

Um menu na parte inferior da página **Máquinas** (ou **Dispositivos**) permite selecionar o nível mínimo de VDA. Isso define o nível funcional mínimo do catálogo. Por padrão, o nível funcional mais atual é selecionado para implantações locais. Se você seguir a recomendação da Citrix de sempre instalar e atualizar VDAs e componentes principais para a versão mais recente, não precisará alterar essa seleção. No entanto, se você precisar continuar usando versões mais antigas do VDA, selecione o valor correto.

Uma versão do Citrix Virtual Apps and Desktops pode não incluir uma nova versão do VDA, ou o novo VDA não afeta o nível funcional. Nesses casos, o nível funcional pode indicar uma versão do

VDA anterior aos componentes instalados ou atualizados. O artigo Novidades de cada versão indica qualquer alteração no nível funcional padrão.

O nível funcional selecionado afeta a lista de máquinas acima dele. Na lista, uma dica de ferramenta ao lado de cada entrada indica se o VDA da máquina é compatível com o catálogo nesse nível funcional.

Mensagens são publicadas na página se o VDA em cada máquina não atender ou exceder o nível funcional mínimo selecionado. Você pode continuar com o assistente. É provável que essas máquinas não consigam se registrar em um Controller mais tarde. Alternativamente, você pode:

- Remover as máquinas que contêm VDAs mais antigos da lista, atualizar seus VDAs e, em seguida, adicioná-las de volta ao catálogo.
- Escolher um nível funcional inferior que impede o acesso aos recursos mais recentes do produto.

Uma mensagem também é publicada se uma máquina não foi adicionada ao catálogo porque é do tipo de máquina errado. Exemplos incluem tentar adicionar um servidor a um catálogo de SO de sessão única, ou adicionar uma máquina de SO de sessão única originalmente criada para alocação aleatória a um catálogo de máquinas estáticas.

> **Importante:**

> Na versão 1811, um nível funcional extra foi adicionado: **1811 (ou mais recente)**. Esse nível é destinado ao uso com futuros recursos do Citrix Virtual Apps and Desktops. A seleção **7.9 (ou mais recente)** permanece como padrão. Esse padrão é válido para todas as implantações agora.

> Se você selecionar **1811 (ou mais recente)**, quaisquer versões anteriores do VDA nesse catálogo não conseguirão se registrar em um Controller. No entanto, se o catálogo contiver apenas VDAs na versão 1811 ou versões posteriores suportadas, todos eles serão elegíveis para registro. Isso inclui catálogos que contêm VDAs configurados para versões posteriores do Citrix Virtual Apps and Desktops, incluindo a versão 1903 e outras versões 19XX antes da versão atual.

Configurar cache para dados temporários

Ao usar o MCS para gerenciar máquinas aleatórias não persistentes em um catálogo, você pode habilitar o Write-Back Cache para as máquinas para melhorar o desempenho de E/S.

O Write-back Cache é conhecido como MCSIO. Para obter mais informações, consulte este artigo do blog.

Pré-requisitos

Para habilitar o cache de write-back, o catálogo deve atender aos seguintes requisitos:

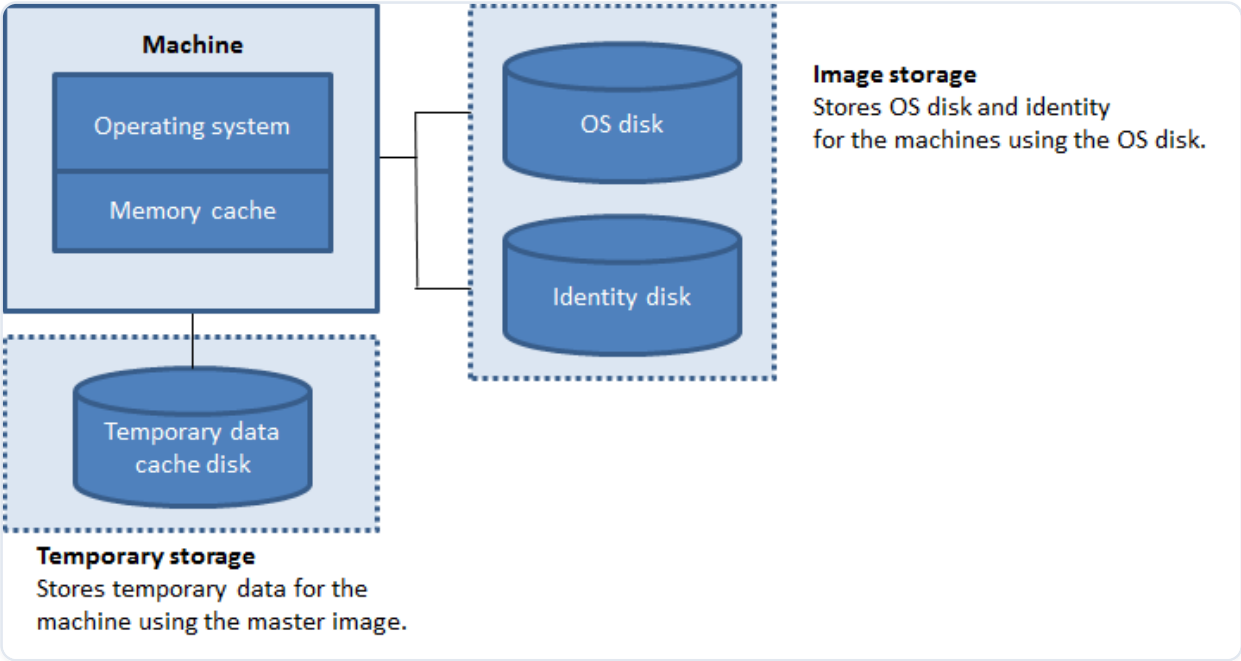
- Usa uma conexão que especifica o armazenamento para dados temporários. Para obter mais informações, consulte Conexões e recursos.
- Os VDAs devem ser pelo menos da versão 7.9 e instalados com um driver MCSIO atual.

> **Observação:**
>
> A instalação deste driver é uma opção ao instalar ou atualizar um VDA. Por padrão, esse driver não é instalado.

- Para habilitar a atribuição de letra de unidade para caches de disco, as VMs devem atender aos seguintes requisitos adicionais:
  - Sistema Operacional: Windows
  - Versão do VDA: 2305 ou posterior

Considerações

- Os caches de write-back vêm em cache de *Memória* e cache de *Disco*. Por padrão, seus valores padrão diferem de acordo com o tipo de conexão. Geralmente, os valores padrão são suficientes para a maioria dos casos; no entanto, considere o espaço necessário para:
  - Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
  - Dados de perfil de usuário.
  - Dados do ShareFile que são sincronizados com as sessões dos usuários.
  - Dados que podem ser criados ou copiados por um usuário da sessão ou quaisquer aplicativos que os usuários possam instalar dentro da sessão.



- A configuração do cache de write-back com apenas um cache de disco e sem cache de memória foi descontinuada. Para habilitar um cache para dados temporários, recomendamos selecionar **Tamanho do cache de disco (GB)** e **Memória alocada para cache (MB)** e especificar um tamanho maior que 0 para o cache de memória. Os dados temporários são inicialmente gravados 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 **Tamanho do cache de memória (MB) (recomendado)**, considere aumentar a quantidade total de memória em cada máquina.
- Se você deixar a caixa de seleção **Memory cache size (MB) (recommended)** desmarcada, os dados temporários são gravados diretamente no cache de disco, usando uma quantidade mínima de memória.
- Alterar o **Tamanho do cache de disco (GB)** de seu valor padrão pode afetar o desempenho. O tamanho deve corresponder aos requisitos do usuário e à carga colocada na máquina.

> **Importante:**
>
> Se o cache de disco ficar sem espaço, a sessão do usuário se torna inutilizável.

- Se você desmarcar a caixa de seleção **Tamanho do cache de disco**, nenhum disco de cache é criado. Nesse caso, especifique um valor de **Memória alocada para cache** que seja grande o suficiente para armazenar todos os dados temporários. Isso é viável apenas se grandes quantidades de RAM estiverem disponíveis para alocação a cada VM.

- Se você desmarcar as duas caixas de seleção, os dados temporários não são armazenados em cache. Eles são gravados no disco de diferença (localizado no armazenamento do SO) para cada VM. (Esta é a ação de provisionamento em versões anteriores à 7.9.)
- Não habilite o cache se você pretende usar este catálogo para criar AppDisks.
- Você não pode alterar os valores de cache em um catálogo de máquinas depois que ele é criado.

NIC

Esta página não aparece ao criar catálogos de Acesso Remoto para PC.

Na página **Network Interface Cards**, 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 nesta página.

Contas de máquina

Esta página aparece somente ao criar catálogos de Acesso Remoto para PC.

Na página **Machine Accounts**, especifique as contas de máquina do Active Directory ou Unidades Organizacionais (OUs) a serem adicionadas que correspondem a usuários ou grupos de usuários. Não use uma barra (/) em um nome de OU.

Ao adicionar OUs, você pode fazer o seguinte se o domínio não for mostrado na lista:

- Pesquisar por ele usando uma correspondência exata.
- Navegar por todos os domínios para encontrá-lo.

Você pode escolher uma conexão de gerenciamento de energia configurada anteriormente ou optar por não usar o gerenciamento de energia. Se você quiser usar o gerenciamento de energia, mas uma conexão adequada ainda não tiver sido configurada, você pode criar essa conexão mais tarde e, em seguida, editar o catálogo de máquinas para atualizar as configurações de gerenciamento de energia.

Identidades de máquina

Esta página aparece somente ao usar o MCS para criar VMs.

Cada máquina no catálogo deve ter uma identidade exclusiva. Esta página permite configurar identidades para máquinas no catálogo. As máquinas são unidas à identidade após serem provisionadas. Você não pode alterar o tipo de identidade após criar o catálogo.

Um fluxo de trabalho geral para configurar as definições nesta página é o seguinte:

1. Selecione uma identidade na lista.
2. Indique se deseja criar contas ou usar as existentes, e o local (domínio) para essas contas.

Você pode selecionar uma das seguintes opções:

- **On-premises Active Directory**. Máquinas de propriedade de uma organização e conectadas com uma conta do Active Directory que pertence a essa organização. Elas existem no local.
- **Hybrid Azure Active Directory joined**. Máquinas de propriedade de 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 Hybrid Azure Active Directory joined.

> **Observação:**
>
> - Antes de usar o ingresso híbrido no Azure Active Directory, certifique-se de que seu ambiente Azure atenda aos pré-requisitos. Consulte `<https://docs.microsoft.com/pt-br/azure/active-directory/devices/hybrid-azuread-join-managed-domains>`.
> - Esta opção exige que a imagem mestre atenda ao pré-requisito do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft: `<https://learn.microsoft.com/pt-br/azure/active-directory/devices/concept-azure-ad-join-hybrid>`.

> **Importante:**
>
> - Se você selecionar **Active Directory local** ou **Ingresso híbrido no Azure Active Directory** como tipo de identidade, cada máquina no catálogo deve ter uma conta de computador do Active Directory correspondente.

> Se você criar contas, deverá ter permissão para criar contas de computador na UO onde as máquinas residem. Cada máquina no catálogo deve ter um nome exclusivo. Especifique o esquema de nomenclatura de conta para as máquinas que você deseja criar. Para obter mais informações, consulte Esquema de nomenclatura de conta de máquina.

> **Observação:**

> Certifique-se de que os nomes das UOs não usem barras (`/`).

> Se você usar contas existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo .csv contendo nomes de conta. O conteúdo do arquivo importado deve usar o formato:

- ADcomputeraccountname.domain

Certifique-se de que há contas suficientes para todas as máquinas que você está adicionando. A interface do Web Studio gerencia essas contas. Portanto, permita que essa interface redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

Para catálogos contendo máquinas físicas ou existentes, selecione ou importe contas existentes e atribua cada máquina a uma conta de computador do Active Directory e a uma conta de usuário.

Esquema de nomenclatura de contas de máquina

Cada máquina em um catálogo deve ter um nome exclusivo. Você deve especificar um esquema de nomenclatura de contas de máquina ao criar um catálogo. Use curingas (sinais de cerquilha) como espaços reservados para números ou letras sequenciais que aparecem no nome.

Ao especificar um esquema de nomenclatura, esteja ciente das seguintes regras:

- O esquema de nomenclatura deve conter pelo menos um curinga. Você deve colocar todos os curingas juntos.
- O nome completo, incluindo curingas, deve conter no mínimo 2 e no máximo 15 caracteres. Deve incluir pelo menos um caractere não numérico e um caractere # (curinga).
- O nome não deve incluir espaços ou qualquer um dos seguintes caracteres: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`.
- O nome não pode terminar com um hífen (-).

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 nomenclatura resulta em um ou mais nomes de máquina 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 selecionado, os curingas especificados se resolvem em números sequenciais.

  > **Observação:**
  >
  > Se houver apenas um curinga (#), os nomes das contas começam com 1. Se houver dois, os nomes das contas começam com 01. Se houver três, os nomes das contas começam com 001, e assim por diante.

- **A-Z**. Se selecionado, os curingas especificados se resolvem em letras sequenciais.

Por exemplo, um esquema de nomenclatura de PC-Sales-## (com **0-9** selecionado) resulta em contas nomeadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

Opcionalmente, você pode especificar com o que os nomes das contas começam.

- Se você selecionar **0-9**, as contas são nomeadas sequencialmente, começando com os números especificados. Insira um ou mais dígitos, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira dois dígitos ou mais.
- Se você selecionar **A-Z**, as contas são nomeadas sequencialmente, começando com as letras especificadas. Insira uma ou mais letras, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira duas letras ou mais.

Credenciais de domínio

Selecione **Inserir credenciais** e insira as credenciais de um administrador com permissão para realizar operações de conta no domínio do Active Directory de destino.

Use a opção **Verificar nome** 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 de domínio. Se a verificação for aprovada, o nome de domínio será preenchido automaticamente.

> **Observação:**
>
> Se o tipo de identidade selecionado em **Identidades da Máquina** for **Ingresso híbrido no Azure Active Directory**, as credenciais inseridas devem ter recebido a permissão `Write userCertificate`.

Resumo, nome e descrição

Na página **Resumo**, revise as configurações que você especificou. Insira um nome e uma descrição para o catálogo. Esta informação aparece no Web Studio.

Quando terminar, clique em **Concluir** para iniciar a criação do catálogo. Quando terminar, selecione **Concluir** para iniciar a criação do catálogo.

Em **Catálogos de Máquinas**, o novo catálogo aparece com uma barra de progresso em linha.

Para visualizar os detalhes do progresso da criação:

1. Passe o mouse sobre o catálogo de máquinas.
2. Na dica de ferramenta que aparece, clique em **Exibir detalhes**.

   Um gráfico de progresso passo a passo aparece onde você pode ver o seguinte:

   - Histórico de etapas
   - Progresso e tempo de execução da etapa atual
   - Etapas restantes

Sincronização de tempo do MCS

A sincronização de tempo é determinada pela imagem mestre e pelo tipo de catálogo unido à identidade da máquina. Você obtém o seguinte método de sincronização de tempo de acordo com a imagem mestre e o catálogo:

IMAGEM MESTRE	CATÁLOGO	MÉTODO DE SINCRONIZAÇÃO DE TEMPO RESULTANTE
NDJ	AD ou Azure AD Híbrido	Por padrão, NT5DS. Você pode desabilitar o MCS de alterar a configuração de sincronização de tempo usando as configurações de registro na imagem mestre
NDJ	NDJ ou Azure AD	Mesmo que a configuração original de sincronização de tempo
AD ou Azure AD Híbrido	AD ou Azure AD Híbrido	O mesmo que a configuração original de sincronização de tempo
Azure AD	Azure AD	O mesmo que a configuração original de sincronização de tempo

Observação:

A sincronização de tempo original é controlada pela seguinte configuração de registro e não pode ser alterada:

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

Valor: MaxAllowedPhaseOffset, MaxNegPhaseCorrection e MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

Valor: Type

> Para desabilitar o MCS de alterar a configuração de sincronização de tempo, defina o valor da seguinte configuração de registro na imagem mestre:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nome: TimeSyncMethodKeep
- Tipo: DWORD
- 0 (Ou, valor TimeSyncMethodKeep não configurado): Não mantém a configuração original de sincronização de tempo.
- 1: Mantém a configuração original de sincronização de tempo e os valores padrão dos parâmetros.

Consideração importante sobre a configuração de propriedades personalizadas

As propriedades personalizadas devem ser definidas corretamente em `New-ProvScheme` e `Set-ProvScheme` em ambientes GCP e Azure. Se você especificar uma propriedade ou propriedades personalizadas inexistentes, receberá a seguinte mensagem de erro e os comandos falharão ao serem executados.

- No Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- No GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

Solução de problemas

> **Importante:**

> Depois de criar o catálogo de máquinas usando o Web Studio, não é mais possível usar o comando PowerShell `Get-ProvTask` para recuperar as tarefas associadas à criação do catálogo de máquinas. Essa restrição é resultado do Web Studio excluir essas tarefas após a criação do catálogo de máquinas, independentemente de o catálogo ser criado com sucesso.

> A Citrix recomenda coletar logs para ajudar a equipe de Suporte a fornecer soluções. Ao usar o Citrix Provisioning, use o seguinte procedimento para gerar arquivos de log:

1. Na imagem mestre, crie a seguinte chave de registro com o valor 1 (como um valor DWORD (32 bits)): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Desligue a imagem mestre e crie um instantâneo.
3. No Delivery Controller, execute o seguinte comando PowerShell: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Crie um catálogo com base nesse instantâneo.
5. Quando a VM de preparação for criada no hipervisor, faça login e extraia os seguintes arquivos da raiz de `C:\`: Image-prep.log e PvsVmAgentLog.txt.
6. Desligue a máquina, momento em que ela relata a falha.
7. Execute o seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS

Você pode atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS. Essa implementação ajuda a evitar conflitos entre a letra de unidade de quaisquer aplicativos que você usa e a letra de unidade do disco de cache de write-back de E/S do MCS. Para fazer isso, você pode usar comandos PowerShell. Os hipervisores suportados são Azure, GCP, VMware, SCVMM e XenServer.

> **Observação:**
>
> Este recurso requer a versão 2305 do VDA ou posterior.

Limitações

- Aplicável apenas ao sistema operacional Windows
- Letra de unidade aplicável para disco de cache de write-back: `E` a `Z`
- Não aplicável quando o disco temporário do Azure é usado como disco de cache de write-back
- Aplicável somente ao criar um novo catálogo de máquinas

Atribuir uma letra de unidade a um disco de cache de write-back

Para atribuir uma letra de unidade ao disco de cache de write-back:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades, se ainda não tiver sido criado. Para obter informações, consulte Criando um Catálogo.
4. Crie um esquema de provisionamento usando o comando `New-ProvScheme` com a propriedade `WriteBackCacheDriveLetter`. Por exemplo:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />
```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. Conclua a criação do catálogo.

Validar a configuração antes de criar um catálogo de máquinas MCS

Você pode validar as configurações antes de criar um catálogo de máquinas MCS usando o parâmetro `-validate` no comando `New-ProvScheme`. Depois de executar este comando PowerShell com o parâmetro, você receberá uma mensagem de erro apropriada se um parâmetro incorreto for usado ou se um parâmetro entrar em conflito com outro. Você pode então usar a mensagem de erro para resolver o problema e criar com sucesso um catálogo de máquinas MCS usando o PowerShell. Atualmente, esse recurso é aplicável a ambientes de virtualização Azure, GCP e VMware.

Nota:

> Durante a validação, você não deve criar um catálogo de máquinas MCS real. Você deve usar o resultado do comando para corrigir os erros e, em seguida, criar um catálogo bem-sucedido. Portanto, ao executar o comando `New-ProvScheme`, use um nome de pool de identidades falso.

> Para validar a configuração, siga os passos abaixo:

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando `New-ProvScheme` e use o parâmetro `-validate`. Forneça um nome de pool de identidades falso para que o comando funcione. Por exemplo,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate

$result.TerminatingError | Format-List -Property *
```

Mensagem de erro:

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
```

```
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. Após validar a configuração, você pode criar um catálogo de máquinas MCS com um nome de pool de identidades real e parâmetros corretos.

Próximos passos

Para obter informações sobre como criar catálogos de serviços de nuvem específicos, consulte:

- Criar um catálogo AWS
- Criar um catálogo XenServer
- Criar um catálogo Google Cloud Platform
- Criar um catálogo Microsoft Azure
- Criar um catálogo Microsoft System Center Virtual Machine Manager
- Criar um catálogo Nutanix
- Criar um catálogo VMware

Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega.

Para revisar todo o processo de configuração, consulte Instalar e configurar.

Você pode criar um catálogo do Citrix Provisioning usando o Web Studio e o PowerShell. Esta implementação oferece as seguintes vantagens:

- Um único console unificado para gerenciar catálogos MCS e Citrix Provisioning.
- Ter novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Atualmente, este recurso está disponível apenas para cargas de trabalho do Azure e VMware. No entanto, em ambientes VMware, você pode atualmente criar os catálogos usando apenas comandos do PowerShell. Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de diferentes tipos de junção
- Gerenciar catálogos de máquinas

Criar um catálogo AWS

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização AWS.

> **Observação:**
>
> Antes de criar um catálogo AWS, você precisa concluir a criação de uma conexão com a AWS. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-aws.html).

Limitação

A partir do Citrix Virtual Apps and Desktops™ 2203 LTSR e posterior, o plug-in MCS AWS faz a chamada de API AWS `DescribeInstanceTypes` e, se for bem-sucedida, o MCS usa o nome de inventário criado a partir da resposta da API.

Portanto, ao atualizar do CVAD 1912 para 2203 ou posterior, desabilite a permissão `DefineInstanceType` na AWS e, em seguida, atualize o catálogo existente usando o comando `Set-ProvScheme` para corresponder ao esquema de nomenclatura da AWS. Em seguida, adicione as permissões `DescribeInstanceType` de volta após a conclusão da atualização do catálogo e o serviço oferecido corresponder ao esquema de nomenclatura da 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. Esta VM de preparação é desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. Este grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, onde GUID é gerado aleatoriamente.

Configurar a tenancy da AWS

A AWS oferece as seguintes opções de tenancy:

- Tenancy compartilhada (o tipo padrão): Múltiplas instâncias do Amazon EC2 de diferentes clientes podem residir na mesma peça de hardware físico.
- Tenancy dedicada: Suas instâncias EC2 são executadas apenas em hardware com outras instâncias que você implantou. Outros clientes não usam a mesma peça de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando o PowerShell.

Configurar a tenancy de host dedicado da AWS usando o PowerShell

Você pode criar um catálogo de máquinas com tenancy de host definida via PowerShell.

Um host dedicado Amazon é um servidor físico com capacidade de instância que é totalmente dedicado, permitindo que você use licenças de software existentes por soquete ou por VM.

Hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado de tipos de instância C4 Large é limitado a executar 16 instâncias. Consulte o site da AWS para obter mais informações.

Os requisitos para provisionamento em hosts AWS incluem:

- Uma imagem BYOL (traga sua própria licença) importada (AMI). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para satisfazer as solicitações de provisionamento.
- habilitar **auto-placement**.

Para provisionar em um host dedicado na AWS usando PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro `TenancyType` definido como *Host*.

Consulte a Documentação do Desenvolvedor Citrix para obter mais informações.

Capturar propriedades de máquina de AMIs

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, você seleciona uma AMI para representar a imagem mestre/golden desse catálogo. Dessa AMI, o MCS usa um instantâneo do disco. Em versões anteriores, se você quisesse funções ou tags em suas máquinas, usaria o console da AWS para configurá-las individualmente. Essa funcionalidade é habilitada por padrão.

> **Dica:**

> Para usar a captura de propriedades de instância da AWS, você deve ter uma VM associada à AMI.

> Para melhorar esse processo, o **MCS lê** as propriedades da instância da qual a AMI foi tirada e aplica a função de Gerenciamento de Acesso de Identidade (IAM) e as tags da máquina às máquinas provisionadas para um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo encontra a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são então armazenadas em um Modelo de Inicialização da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades de instância capturadas.

As propriedades capturadas incluem:

- Funções IAM – aplicadas a instâncias provisionadas.
- Tags - aplicadas a instâncias provisionadas, seus discos e NICs. Essas tags são aplicadas a recursos transitórios do Citrix®, incluindo: bucket e objetos S3, e AMIs, instantâneos e modelos de inicialização.

> **Dica:**

> A marcação de recursos transitórios do Citrix é opcional e configurável usando a propriedade personalizada `AwsOperationalResourcesTagging`.

Capturar a propriedade da instância da AWS

Você pode usar esse recurso especificando uma propriedade personalizada, `AwsCaptureInstanceProperties`, 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 Desenvolvedor Citrix para obter mais informações.

> **Observação:**

> O `AwsCaptureInstanceProperties` está obsoleto. Recomendamos usar perfis de máquina para especificar propriedades de máquina para VMs.

Capturar propriedades da máquina de perfis de máquina

Ao criar um catálogo para provisionar máquinas AWS usando MCS, você pode usar um perfil de máquina para predefinir certas configurações de propriedade da máquina.

Para fazer isso, siga estas etapas:

1. Armazene os perfis de máquina na mesma zona de disponibilidade que os recursos onde você está criando este catálogo.
2. Na página **Modelo de Máquina** do assistente de criação de catálogo, selecione **Usar um perfil de máquina**. Os perfis de máquina localizados na mesma zona disponível que os recursos selecionados são exibidos.
3. Selecione um perfil de máquina conforme necessário.

> **Observação:**

> Você pode usar um perfil de máquina ou uma AMI para capturar propriedades da máquina. No Web Studio, ao selecionar **Usar um perfil de máquina**, a opção **Aplicar propriedades do modelo de máquina a máquinas virtuais** é automaticamente ocultada.

Marcar recurso operacional AWS

Ao criar um catálogo para provisionar máquinas na AWS usando MCS, você pode controlar se as propriedades de função IAM e de tag são aplicadas a essas máquinas. Você também pode controlar se as tags de máquina são aplicadas a recursos operacionais.

Uma Amazon Machine Image (AMI) representa um tipo de appliance virtual usado para criar uma máquina virtual dentro do ambiente Amazon Cloud, comumente referido como EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Ao criar um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem dourada para esse catálogo.

> **Importante:**

> A criação de catálogos capturando uma propriedade de instância e um modelo de inicialização é necessária para usar a marcação de recursos operacionais.

> Para criar um catálogo AWS, você deve primeiro criar uma AMI para a instância que deseja que seja a imagem dourada. O MCS lê as tags dessa instância e as incorpora ao modelo de inicialização. As tags do modelo de inicialização são então aplicadas a todos os recursos Citrix criados em seu ambiente AWS, incluindo:

- Máquinas Virtuais
- Discos de VM
- Interfaces de rede de VM
- Buckets S3
- Objetos S3
- Modelos de inicialização
- AMIs

Marcar um recurso operacional

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell a partir do host DDC.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.

Para marcar um recurso para uma VM provisionada, use a nova propriedade personalizada `AwsOperationalResourcesTagging`. A sintaxe para esta propriedade é:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das fontes de perfil da

máquina (instância de VM AWS ou versão de modelo de inicialização AWS). Este recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes.

Observação:

- No console do AWS EC2, você não pode ver os valores de **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver as especificações da tag.
- Se uma fonte de perfil de máquina (VM ou versão de modelo de inicialização) tiver duas interfaces de rede (eni-1 e eni-2), e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, então a VM receberá as tags de ambas as interfaces de rede.

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 versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades que são capturadas podem incluir, por exemplo, propriedades de volume EBS, tipo de instância, otimização EBS, opções de CPU, tipo de locação, capacidade de hibernação e outras configurações AWS suportadas.

Você pode usar uma instância AWS EC2 (VM) ou uma versão de modelo de inicialização AWS como entrada do perfil da máquina.

Observação:

- As propriedades do volume EBS são derivadas apenas de um perfil de máquina.
- O MCS provisiona VMs com discos de identidade do tipo de volume GP3. Como o tipo de volume GP3 é a opção mais barata oferecida pela AWS, esse recurso minimiza os custos. A implementação é aplicável apenas às VMs adicionadas a um novo catálogo e às novas VMs adicionadas a um catálogo existente. As VMs existentes criadas antes desse recurso continuarão a ter discos de ID com tipo de volume GP2, a menos que o disco de ID seja redefinido.

Considerações importantes

As considerações importantes ao criar um catálogo de máquinas MCS:

- Se você adicionar parâmetros de propriedade de hardware da máquina nos comandos `New-ProvScheme` e `Set-ProvScheme`, os valores fornecidos nos parâmetros sobrescreverão os valores no perfil da máquina.
- Se você definir `AwsCaptureInstanceProperties` como `true` e não definir a propriedade `MachineProfile`, então apenas as funções e tags do IAM serão capturadas.
- Você não pode definir `AwsCaptureInstanceProperties` e `MachineProfile` ao mesmo tempo.

  > **Nota:
  >
  > O `AwsCaptureInstanceProperties` está obsoleto.

- Se um perfil de máquina não for fornecido, você deve fornecer explicitamente os valores das seguintes propriedades:
  - Grupo de Segurança
  - ENI ou Rede Virtual
- Você pode habilitar `AwsOperationalResourcesTagging` somente se habilitar `AwsCaptureInstanceProperties` ou especificar um perfil de máquina.

As considerações importantes após a criação de um catálogo de máquinas MCS:

- Você não pode alterar um catálogo de 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 `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. Execute o comando New-ProvScheme. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. Conclua a criação do catálogo. Para obter mais informações, consulte Citrix PowerShell SDK.

Atualizar o perfil da máquina

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina, faça o seguinte. Você também pode alterar o tipo de locação e a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS.

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Criar um catálogo com a versão do modelo de inicialização

Você pode criar um catálogo de máquinas MCS com uma versão de modelo de inicialização como entrada de perfil de máquina. Você também pode atualizar a entrada de um catálogo de perfil de

máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM.

No console AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de inicialização junto com o número da versão. Ao especificar a versão do modelo de inicialização como entrada de perfil de máquina durante a criação ou atualização de um catálogo de máquinas, as propriedades dessa versão do modelo de inicialização são copiadas para as VMs VDA provisionadas.

As seguintes propriedades podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidas nos comandos `New-ProvScheme` ou `Set-ProvScheme`, elas terão precedência sobre os valores do perfil da máquina dessas propriedades.

- Oferta de Serviço
- Redes
- Grupos de Segurança
- Tipo de Tenancy

> **Observação:**

> Se a oferta de serviço não for fornecida no modelo de inicialização do perfil da máquina ou como um parâmetro no comando `New-ProvScheme`, você receberá um erro apropriado.

> Para criar um catálogo usando a versão do modelo de inicialização como entrada de perfil de máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Obtenha a lista de versões de modelo de inicialização de um modelo de inicialização. Por exemplo:

   ```
   XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
   Select FullPath
   ```

4. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão de modelo de inicialização como entrada de perfil de máquina. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Registre o esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
```

```
-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Conclua a criação do catálogo. Para obter mais informações, consulte Citrix PowerShell SDK

Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- Para atualizar a entrada de um catálogo de perfil de máquina de uma versão de modelo de inicialização para uma VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

Criptografar discos de SO e ID

Você pode criar um catálogo persistente e não persistente de VMs com chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) que podem ser usadas para criptografar o disco do SO e o disco de identidade.

- As chaves gerenciadas pela AWS são rotacionadas automaticamente todos os anos.
- As chaves gerenciadas pelo cliente são opcionais para rotação automática e podem ser gerenciadas manualmente.

Você pode consultar os seguintes documentos da AWS para obter mais informações sobre chaves KMS:

- Conceitos do AWS KMS
- Como funciona a rotação automática de chaves.

Para criptografia de discos de SO e ID, configure uma das seguintes opções:

- Use uma imagem mestre criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz EBS criptografado com chave KMS)
- Use uma fonte de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz EBS criptografado.

Limitações

Considere as seguintes limitações:

- Atualmente, o MCS suporta apenas um disco na AMI da imagem mestre.
- Você não pode criptografar diretamente volumes ou snapshots EBS existentes não criptografados, nem modificar a chave KMS de um volume criptografado existente. Para fazer isso, você deve:

  a. Criar um novo snapshot desse volume.

  b. Crie um novo volume a partir desse snapshot.

  c. Criptografar o novo volume.

Consulte os seguintes documentos da AWS:

- Criptografar recursos não criptografados
- Limitações da criptografia automática ou padrão de volumes EBS: Criptografar automaticamente volumes EBS existentes e novos da Amazon.

Criar um catálogo com criptografia de disco

Você pode criar um catálogo de máquinas MCS com criptografia de disco usando:

- Imagem mestre
- Perfil de máquina

Considerações ao usar a entrada de perfil de máquina para criptografia de disco:

- A chave KMS da entrada do perfil de máquina tem precedência sobre a chave KMS da imagem mestre.
- Se nenhuma entrada de perfil de máquina for fornecida, a chave KMS da AMI da imagem mestre será usada para criptografar os discos das VMs do catálogo.
- Se o perfil de máquina tiver Mapeamentos de Dispositivo de Bloco presentes, então os dispositivos de bloco presentes no modelo de imagem mestre (AMI) e no perfil de máquina devem corresponder. Por exemplo, se a AMI tiver um dispositivo definido em `/dev/sda1`, então o Perfil de Máquina também deve ter um dispositivo definido em `/dev/sda1`.
- Se não houver chave na origem do perfil de máquina e a imagem mestre não estiver criptografada, os discos das VMs do catálogo não serão criptografados.
- Quando a imagem mestre é criptografada, uma VM de origem de perfil de máquina ou um modelo de inicialização deve ter um volume raiz criptografado para ser considerado uma entrada válida.

Modificar um catálogo existente

Você pode modificar um catálogo existente usando `Set-ProvScheme` para ter:

- Uma entrada de perfil de máquina com um volume contendo uma nova chave KMS.
- Um modelo de imagem mestre AMI criptografado com uma nova chave KMS.

Considerações importantes

- Os volumes das novas VMs adicionadas ao catálogo são criptografados com a nova chave KMS.
- Para atualizar as configurações de criptografia quando houver um perfil de máquina existente, execute `Set-ProvScheme` com um novo perfil de máquina.
- Você não pode modificar um catálogo existente de volumes criptografados para volumes não criptografados. Você não pode fazer uma atualização de imagem de uma AMI mestre criptografada para uma AMI mestre não criptografada.

Filtrar instâncias de VM

Uma instância AWS EC2 que você usa como VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criado e funcione corretamente. Para listar as instâncias AWS EC2 que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode paginar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

Paginação:

Get-HypInventoryItem oferece suporte a dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens ignorar desde o início absoluto (ou fim absoluto) da lista no hipervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:
  - `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.
  - `-ContinuationToken`: Retorna os itens imediatamente depois (ou antes, se `ForwardDirection` for **false**), mas não incluindo o item fornecido em `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem o `TotalItemsCount` e o `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- Para retornar um array de registros terminando com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- Para retornar um array de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtragem:

Os seguintes parâmetros opcionais adicionais são suportados para filtragem. Você pode combinar esses parâmetros com as opções de paginação.

- `-ContainsName "my_name"`: Se a string fornecida corresponder a parte de um nome de AMI, a AMI será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **Observação:**
>
> Dois valores de tag são suportados. O valor da tag **Não Marcado** corresponde a itens que não possuem a tag fornecida em sua lista de tags. O valor da tag **Todos os valores** corresponde a itens que possuem a tag, independentemente do valor da tag. Caso contrário, a correspondência ocorre apenas se o item tiver a tag e o valor for igual ao que é fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtragem no parâmetro AdditionalData:

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em AdditionalData. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs são incluídas com um campo `AdditionalData` chamado **Aviso**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo AWS

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com AWS
- Criar catálogos de máquinas

Criar um catálogo XenServer®

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização XenServer.

Observação:

> Antes de criar um catálogo XenServer, você precisa concluir a criação de uma conexão com o XenServer. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-citrix-hypervisor.html).

Criar um catálogo de máquinas usando uma conexão XenServer

Máquinas com capacidade de GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure máquinas com capacidade de GPU para permitir que a VM opere com software que usa a GPU para operações.

1. No XenCenter®, crie uma VM com VGA padrão, redes e vCPU.
2. Atualize a configuração da VM para habilitar o uso de GPU (Passthrough ou vGPU).
3. Instale um sistema operacional compatível e habilite o RDP.
4. Instale o Citrix VM Tools e os drivers NVIDIA.
5. Limpe o Console de Administração do Virtual Network Computing (VNC) para otimizar o desempenho e, em seguida, reinicie a VM.
6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e, em seguida, reinicie a VM.
7. Opcionalmente, crie um snapshot para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente que são configurados no XenCenter e usam recursos de GPU.

Limitações

- Se uma implantação do Citrix Virtual Apps and Desktops com suas VMs hospedadas no Citrix Hypervisor 8.2 Cumulative Update 1 usar vários SRs GFS2 em um único catálogo MCS, as VMs no catálogo não poderão acessar os VDIs durante a implantação. O erro “VDI is currently in use” é relatado.
- O Citrix Hypervisor 8.2 Cumulative Update 1 não suporta VMs de clone completo do MCS com SRs GFS2.

Para obter mais informações, consulte Restrições.

Essas restrições não se aplicam ao XenServer 8 e versões posteriores.

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 de hardware serão capturadas da VM ou instantâneo da imagem mestre.

> **Observação:**
>
> Atualmente, você pode usar apenas 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 a janela do PowerShell.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas. Por exemplo:

   ```
   New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
   "ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
   "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
   ```

4. Crie as contas de computador AD necessárias no Active Directory.

   ```
   $password = "password123" | ConvertTo-SecureString -AsPlainText -Force

   New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
   -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
   ```

```
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. Registre o esquema de provisionamento como um catálogo de broker. Por exemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. Adicione VMs ao catálogo.

Para atualizar um catálogo com um novo perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

Para obter mais informações sobre o comando Set-ProvScheme, consulte Set-ProvScheme.

Observação:

- O comando `Set-ProvScheme` neste caso não altera o perfil de máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.
- Você não pode converter um catálogo de máquinas baseado em perfil de máquina para um catálogo de máquinas não baseado em perfil de máquina.

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo XenServer

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com XenServer
- Criar catálogos de máquinas

Criar um catálogo do Google Cloud Platform

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

Nota:

> Antes de criar um catálogo do Google Cloud Platform (GCP), você precisa concluir a criação de uma conexão com o GCP. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-gcp.html).

Preparar uma instância de VM mestre e um disco persistente

> **Dica:**

> Disco persistente é o termo do Google Cloud para disco virtual.

> Para preparar sua instância de VM mestre, crie e configure uma instância de VM com propriedades que correspondam à configuração desejada para as instâncias VDA clonadas em seu catálogo de máquinas planejado. A configuração não se aplica apenas ao tamanho e tipo da instância. Ela também inclui atributos da instância, como metadados, tags, atribuições de GPU, tags de rede e propriedades da conta de serviço.

Como parte do processo de masterização, o MCS usa sua instância de VM mestre para criar o *modelo de instância* do Google Cloud. O modelo de instância é então usado para criar as instâncias VDA clonadas que compõem o catálogo de máquinas. As instâncias clonadas herdam as propriedades (exceto as propriedades de VPC, sub-rede e disco persistente) da instância de VM mestre a partir da qual o modelo de instância foi criado.

Depois de configurar as propriedades da instância de VM mestre de acordo com suas especificações, inicie a instância e, em seguida, prepare o disco persistente para a instância.

Recomendamos que você crie manualmente um snapshot do disco. Isso permite que você use uma convenção de nomenclatura significativa para rastrear 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 seu próprio snapshot, o MCS criará um snapshot temporário para você (que é excluído ao final do processo de provisionamento).

Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas usando o Web Studio
- Criar um catálogo de máquinas usando o PowerShell

Criar um catálogo de máquinas usando o Web Studio

> **Observação:**
>
> Crie seus recursos antes de criar um catálogo de máquinas. Use as convenções de nomenclatura estabelecidas pelo Google Cloud ao configurar catálogos de máquinas. Consulte Diretrizes de nomenclatura de buckets e objetos para obter mais informações.

> Siga as orientações em Criar catálogos de máquinas. A descrição a seguir é exclusiva para catálogos do Google Cloud.

1. Faça login no Web Studio e selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione **Criar Catálogo de Máquinas** na barra de ações.
3. Na página **Sistema Operacional**, selecione **SO multissessão** e, em seguida, selecione **Avançar**.
   - O Citrix Virtual Apps and Desktops™ também oferece suporte a SO de sessão única.
4. Na página **Gerenciamento de Máquinas**, selecione as opções **Máquinas que têm o gerenciamento de energia ativado** e **Citrix Machine Creation Services™** e, em seguida, selecione **Avançar**. Se houver vários recursos, selecione um no menu.
5. Na página **Imagem**, conclua estas etapas conforme necessário e, em seguida, clique em **Avançar**.
   a. Selecione um snapshot ou VM como a imagem mestre. Se você quiser usar a funcionalidade de locação exclusiva, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente. Consulte Habilitar seleção de zona.
   b. Para usar uma VM existente como perfil de máquina, selecione Usar um perfil de máquina e, em seguida, selecione a VM.

      > **Observação:**
      >
      > Atualmente, as VMs neste 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 para o catálogo. Para usar a funcionalidade de locação exclusiva, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente.

6. Na página **Tipos de Armazenamento**, selecione o tipo de armazenamento usado para conter o sistema operacional para este catálogo de máquinas. Cada uma das seguintes opções de armazenamento tem características únicas de preço e desempenho. (Um disco de identidade é sempre criado usando o disco persistente padrão zonal.)

   - Disco persistente padrão
   - Disco persistente balanceado
   - Disco persistente SSD

   Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte `<https://cloud.google.com/compute/docs/disks/>`.

7. Na página **Máquinas Virtuais**, especifique quantas VMs você deseja criar, visualize a especificação detalhada das VMs e, em seguida, selecione **Avançar**. Se você usar grupos de nós de locatário único para catálogos de máquinas, certifique-se de selecionar **apenas** as zonas onde os nós de locatário único reservados estão disponíveis. Consulte Habilitar seleção de zona.

8. Na página **Contas de Computador**, selecione uma conta do Active Directory e, em seguida, selecione **Avançar**.

   - Se você selecionar **Criar novas contas do Active Directory**, selecione um domínio e, em seguida, insira a sequência de caracteres que representa o esquema de nomenclatura para as contas de computador de VM provisionadas criadas no Active Directory. O esquema de nomenclatura da conta pode conter de 1 a 64 caracteres e não pode conter espaços em branco, caracteres não ASCII ou caracteres especiais.
   - Se você selecionar **Usar contas existentes do Active Directory**, selecione **Procurar** para navegar até as contas de computador do Active Directory existentes para as máquinas selecionadas.

9. Na página **Credenciais de Domínio**, selecione **Inserir credenciais**, digite o nome de usuário e a senha, selecione **Salvar** e, em seguida, selecione **Avançar**.

   - A credencial que você digita deve ter permissões para realizar operações de conta do Active Directory.

10. Na página **Resumo**, confirme as informações, especifique um nome para o catálogo e, em seguida, selecione **Concluir**.

> **Observação:**
>
> A partir da versão 2402, os nomes de catálogo do GCP devem estar em conformidade com estas regras:
>
> - Começar com uma letra minúscula.
> - Incluir apenas letras minúsculas (a-z), números e hífens.
> - Terminar com uma letra minúscula ou um número. Ao tentar renomear catálogos GCP existentes que não estão em conformidade com estas regras, mensagens de erro aparecem e o guiam para renomeá-los de acordo com as regras atualizadas.

A criação do catálogo de máquinas pode levar muito tempo para ser concluída. Para verificar se as máquinas são criadas nos grupos de nós de destino, vá para o console do Google Cloud.

Importar máquinas do Google Cloud criadas manualmente

Você pode *criar uma conexão com o Google Cloud* e, em seguida, *criar um catálogo contendo máquinas do Google Cloud*. Depois, você pode reiniciar manualmente as máquinas do Google Cloud através do Citrix Virtual Apps and Desktops. Com este recurso, você pode:

- Importar máquinas OS multi-sessão do Google Cloud criadas manualmente para um catálogo de máquinas do Citrix Virtual Apps and Desktops.
- Remover máquinas OS multi-sessão do Google Cloud criadas manualmente de um catálogo do Citrix Virtual Apps and Desktops.
- Usar os recursos de gerenciamento de energia existentes do Citrix Virtual Apps and Desktops para gerenciar a energia de máquinas OS multi-sessão do Google Cloud Windows. Por exemplo, definir um agendamento de reinicialização para essas máquinas.

Esta funcionalidade não requer alterações em um 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 no Web Studio em vez de importar máquinas do Google Cloud criadas manualmente.

Nuvem Privada Virtual Compartilhada

Nuvens Privadas Virtuais Compartilhadas (VPCs) compreendem um projeto host, a partir do qual as sub-redes compartilhadas são disponibilizadas, e um ou mais projetos de serviço que usam o recurso. As VPCs Compartilhadas são opções desejáveis para instalações maiores porque fornecem controle centralizado, uso e administração de recursos corporativos compartilhados da nuvem do Google. Para mais informações, consulte o site de Documentação do Google.

Com este recurso, o Machine Creation Services (MCS) oferece suporte ao provisionamento e gerenciamento de catálogos de máquinas implantados em VPCs Compartilhadas. Este suporte, que é funcionalmente equivalente ao suporte atualmente fornecido em VPCs locais, difere em duas áreas:

1. Você deve conceder permissões extras à Conta de Serviço usada para criar a Conexão de Host. Este processo permite que o MCS acesse e use Recursos de 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 da imagem.

Novas permissões necessárias

Uma conta de serviço do Google Cloud com permissões específicas é necessária ao criar a conexão do host. Essas permissões adicionais devem ser concedidas a quaisquer contas de serviço usadas para criar conexões de host baseadas em VPC Compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas para o Citrix Virtual Apps and Desktops. 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 compartilhados.

> Um máximo de quatro permissões extras devem ser concedidas à conta de serviço associada à conexão do host para suportar o VPC Compartilhado:

1. **compute.firewalls.list** - Esta permissão é obrigatória. Ela permite que o MCS recupere a lista de regras de firewall presentes no VPC Compartilhado.
2. **compute.networks.list** - Esta permissão é obrigatória. Ela permite que o MCS identifique as redes VPC Compartilhadas disponíveis para a conta de serviço.
3. **compute.subnetworks.list** – Esta permissão é opcional, dependendo de como você usa os VPCs. Ela permite que o MCS identifique as sub-redes dentro dos VPCs Compartilhados

visíveis. Esta permissão já é exigida ao usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.

4. **compute.subnetworks.use** - Esta permissão é opcional, dependendo de como você usa os VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionados. Esta permissão já é exigida para usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.

Ao usar essas permissões, considere que existem diferentes abordagens com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão em nível de projeto:
  - Permite acesso a todos os VPCs Compartilhados dentro do projeto host.
  - Requer que as permissões #3 e #4 sejam atribuídas à conta de serviço.
- Permissão em nível de sub-rede:
  - Permite acesso a sub-redes específicas dentro do VPC Compartilhado.
  - As permissões #3 e #4 são intrínsecas à atribuição em nível de sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que melhor se adapta às suas necessidades organizacionais e padrões de segurança.

> **Dica:**

> Para obter mais informações sobre as diferenças entre permissões em nível de projeto e em nível de sub-rede, consulte 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 disco de sistema da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total; uma para tráfego de entrada e outra para tráfego de saída. Ao usar 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 o número de novas permissões necessárias para usar VPCs Compartilhadas no mínimo. As VPCs Compartilhadas são recursos corporativos de nível superior e geralmente possuem protocolos de segurança mais rígidos em vigor. Por esse motivo, crie um par de regras de firewall no projeto host nos recursos da VPC compartilhada, uma para entrada e outra para saída. Atribua a mais alta prioridade a elas. Aplique uma nova tag de destino a cada uma dessas regras, usando o seguinte valor:

```
citrix-provisioning-quarantine-firewall
```

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura por regras de firewall que contenham esta tag de destino. Em seguida, ele examina as regras quanto à correção e as aplica à máquina usada para preparar a imagem mestre para o catálogo. Se as regras de firewall não forem encontradas, ou se as regras forem encontradas, mas as regras ou suas prioridades estiverem incorretas, uma mensagem semelhante à seguinte aparecerá:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

Configurando a VPC compartilhada

Antes de adicionar a VPC Compartilhada como uma conexão de host no Web Studio, conclua as seguintes etapas para adicionar contas de serviço do projeto no qual você pretende provisionar:

1. Crie uma função IAM.
2. Adicione a conta de serviço usada para criar uma conexão de host CVAD à função IAM do projeto host da VPC Compartilhada.
3. Adicione a conta de serviço do Cloud Build do projeto no qual você pretende provisionar à função IAM do projeto host da VPC Compartilhada.
4. Crie regras de firewall.

CRIAR UMA FUNÇÃO IAM

Determine o nível de acesso da função — *acesso em nível de projeto* ou um modelo mais restrito usando *acesso em nível de sub-rede*.

Acesso em nível de projeto para função IAM. Para a função IAM em nível de projeto, inclua as seguintes permissões:

- compute.firewalls.list

- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função IAM em nível de projeto:

1. No console do Google Cloud, navegar até **IAM e administrador > Funções**.
2. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
3. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

Função IAM em nível de sub-rede. Esta função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` após selecionar **CRIAR FUNÇÃO**. Para este nível de acesso IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função IAM em nível de sub-rede:

1. No console do Google Cloud, navegar até **Rede VPC** > **VPC compartilhada**. A página **VPC compartilhada** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.
2. Na página **VPC Compartilhada**, selecione a sub-rede que você deseja acessar.
3. No canto superior direito, selecione **ADICIONAR MEMBRO** para adicionar uma conta de serviço.
4. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar um papel** e, em seguida, **Usuário da Rede de Computação**.
    c. Selecione **SALVAR**.
5. No console do Google Cloud, navegar para **IAM e Administrador** > **Funções**.

6. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
7. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

ADICIONAR UMA CONTA DE SERVIÇO À FUNÇÃO IAM DO PROJETO HOST

Após criar uma função IAM, siga as etapas abaixo para adicionar uma conta de serviço para o projeto host:

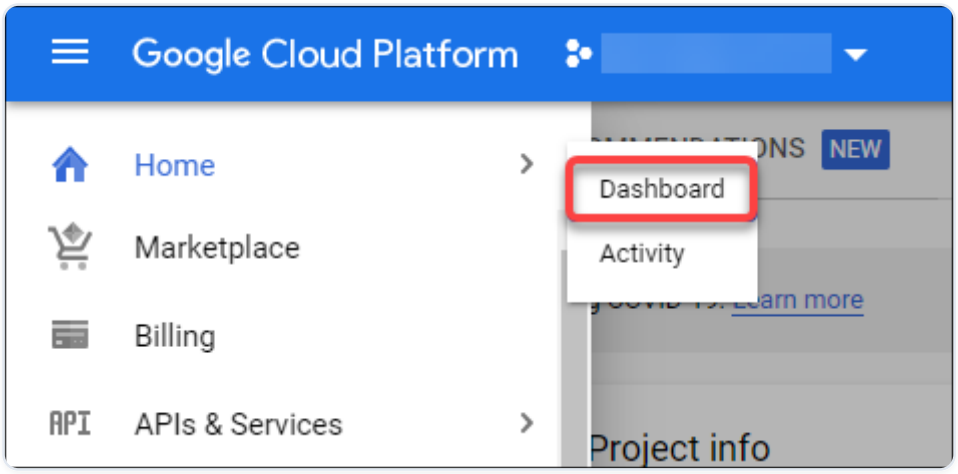
1. No console do Google Cloud, navegar para o projeto host e, em seguida, para **IAM e Administrador > IAM**.
2. Na página **IAM**, selecione **ADICIONAR** para adicionar uma conta de serviço.
3. Na página **Adicionar membros**:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione um campo de função, digite a função IAM que você criou e selecione a função no menu.
    c. Selecione **SALVAR**.

A conta de serviço agora está configurada para o projeto host.

ADICIONAR A CONTA DE SERVIÇO DE COMPILAÇÃO EM NUVEM AO VPC COMPARTILHADO

Cada assinatura do Google Cloud tem uma conta de serviço que é nomeada após o número de ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar qual é o número de ID do projeto para o seu projeto selecionando **Home** e **Dashboard** no console do Google Cloud:



Encontre o **Project Number** abaixo da área **Project Info** da tela.

Execute as seguintes etapas para adicionar a conta de serviço do Cloud Build ao VPC Compartilhado:

1. No console do Google Cloud, navegar até o projeto host e depois para **IAM e administrador** > **IAM**.
2. Na página **Permissões**, selecione **ADICIONAR** para adicionar uma conta.
3. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da conta de serviço do Cloud Build e selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar uma função**, digite `Computer Network User` e selecione a função no menu.
    c. Selecione **SALVAR**.

CRIAR REGRAS DE FIREWALL

Como parte do processo de masterização, o MCS copia a imagem de máquina selecionada e a usa para preparar o disco de sistema da imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que então executa scripts de preparação. 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 requer duas regras de firewall de *negação total* (uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall no *Projeto Host* da seguinte forma:

1. No console do Google Cloud, navegar até o projeto host e depois para **Rede VPC > Firewall**.
2. Na página **Firewall**, selecione **CRIAR REGRA DE FIREWALL**.
3. Na página **Criar uma regra de firewall**, preencha o seguinte:

- **Nome**. Digite um nome para a regra.
- **Rede**. Selecione a rede VPC Compartilhada à qual a regra de firewall de entrada se aplica.
- **Prioridade**. Quanto menor o valor, maior a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
- **Direção do tráfego**. Selecione **Entrada**.
- **Ação na correspondência**. Selecione **Negar**.
- **Destinos**. Use o padrão, **Tags de destino especificadas**.
- **Tags de destino**. Digite `citrix-provisioning-quarantine-firewall`.
- **Filtro de origem**. Use o padrão, **Intervalos de IP**.
- **Intervalos de IP de origem**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
- **Protocolos e portas**. Selecione **Negar tudo**.

4. Selecione **CRIAR** para criar a regra.
5. Repita as etapas 1–4 para criar outra regra. Para **Direção do tráfego**, selecione **Saída**.

ADICIONAR UMA CONEXÃO

Adicione uma conexão aos ambientes da nuvem do Google. Consulte Adicionar uma conexão.

Habilitar seleção de zona

O Citrix Virtual Apps and Desktops oferece suporte à seleção de zona. Com a seleção de zona, você especifica as zonas onde deseja criar VMs. Com a seleção de zona, os administradores podem colocar nós de locatário único em zonas de sua escolha. Para configurar a locação única, você deve concluir o seguinte no Google Cloud:

- Reservar um nó de locatário único do Google Cloud
- Criar a imagem mestre do VDA

Reservando um nó de locatário único do Google Cloud

Para reservar um nó de locatário único, consulte a documentação do Google Cloud.

> **Importante:**

> Um modelo de nó é usado para indicar as características de desempenho do sistema que é reservado no grupo de nós. Essas características incluem o número de vGPUs, a

quantidade de memória alocada ao nó e o tipo de máquina usado para máquinas criadas no nó. Para obter mais informações, consulte a documentação do Google Cloud.

Criando a imagem mestre do VDA

Para implantar máquinas no nó de locatário único com sucesso, você precisa seguir etapas extras ao criar uma imagem mestre de VM. As instâncias de máquina no Google Cloud têm uma propriedade chamada *rótulos de afinidade de nó*. As instâncias usadas como imagens mestras para catálogos implantados no nó de locatário único exigem um *rótulo de afinidade de nó* que corresponda ao nome do **grupo de nós de destino**. Para conseguir isso, tenha em mente o seguinte:

- Para uma nova instância, defina o rótulo no console do Google Cloud ao criar uma instância. Para obter detalhes, consulte 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.

Observação:

Se você pretende usar a locação única com uma VPC compartilhada, consulte Virtual Private Cloud Compartilhada.

DEFINIR UM RÓTULO DE AFINIDADE DE NÓ AO CRIAR UMA INSTÂNCIA

Para definir o rótulo de afinidade de nó:

1. No console do Google Cloud, navegar para **Compute Engine > VM instances**.
2. Na página **VM instances**, selecione **Create instance**.
3. Na página **Instance creation**, digite ou configure as informações necessárias e, em seguida, 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, em seguida, selecione **Select** para retornar à guia **Sole tenancy**. O campo de rótulos de afinidade de nó é

preenchido com as informações selecionadas. Essa configuração garante que os catálogos de máquinas criados a partir da instância serão 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 de nó:

1. Na janela do 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 onde 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. navegar para a página de **detalhes da instância da VM** da instância e verifique se o campo **Afinidades de Nó** é preenchido com o rótulo.

CRIAR UM CATÁLOGO DE MÁQUINAS

Após definir o rótulo de afinidade de nó, configure o catálogo de máquinas.

Chaves de Criptografia Gerenciadas pelo Cliente (CMEK)

Você pode usar Chaves de Criptografia Gerenciadas pelo Cliente (CMEK) para catálogos MCS. Ao usar essa funcionalidade, você atribui a função `CryptoKey Encrypter/Decrypter` do Google Cloud Key Management Service ao Agente de Serviço do Compute Engine. A conta do Citrix Virtual Apps and Desktops deve ter as permissões corretas no projeto onde a chave está armazenada. Consulte Ajudando a proteger recursos usando chaves do Cloud KMS para obter mais informações.

Seu Agente de Serviço do Compute Engine está no seguinte formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato é diferente da Conta de Serviço padrão do Compute Engine.

Observação:

Esta Conta de Serviço do Compute Engine pode não aparecer na exibição **Permissões de IAM** do Google Console. Nesses casos, use o comando `gcloud` conforme descrito em Ajudando a proteger recursos usando chaves do Cloud KMS.

Atribuir permissões à conta do Citrix Virtual Apps and Desktops

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões KMS *no nível do projeto* ou permissões KMS *no nível do recurso*. Consulte Permissões e funções para obter mais informações.

PERMISSÕES EM NÍVEL DE PROJETO

Uma opção é fornecer à conta do Citrix Virtual Apps and Desktops permissões em nível de projeto para navegar pelos recursos do Cloud KMS. Para fazer isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua esta função personalizada ao seu Citrix Virtual Apps and Desktops. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

PERMISSÕES EM NÍVEL DE RECURSO

Para a outra opção, permissões em nível de recurso, no console do Google Cloud, navegue até o `cryptoKey` que você usa para provisionamento MCS. Adicione a conta do Citrix Virtual Apps and Desktops a um conjunto de chaves ou a uma chave que você usa para provisionamento de catálogo.

Dica:

Com esta opção, você não pode procurar chaves regionais para seu projeto no inventário porque a conta do Citrix Virtual Apps and Desktops não tem permissões de lista em nível de projeto nos recursos do Cloud KMS. No entanto, você ainda pode provisionar um catálogo

> usando CMEK especificando o `cryptoKeyId` correto nas propriedades personalizadas `ProvScheme`, conforme descrito abaixo.

Provisionamento com CMEK usando propriedades personalizadas

Ao criar seu Esquema de Provisionamento via PowerShell, especifique uma propriedade `CryptoKeyId` em `ProvScheme CustomProperties`. Por exemplo:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

O `cryptoKeyId` deve ser especificado no seguinte formato:

`projectId:location:keyRingName:cryptoKeyName`

Por exemplo, se você quiser usar a chave `my-example-key` no anel de chaves `my-example-key-ring` na região `us-east1` e no projeto com ID `my-example-project-1`, suas configurações personalizadas `ProvScheme` seriam semelhantes a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

Todos os discos e imagens provisionados pelo MCS relacionados a este esquema de provisionamento usam esta chave de criptografia gerenciada pelo cliente.

> **Dica:**

> Se você usar chaves globais, o local das propriedades do cliente deve dizer `global` e não o nome da **região**, que no exemplo acima é **us-east1**. Por exemplo: `<Property`

`xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`.

Rotação de chaves gerenciadas pelo cliente

O Google Cloud não oferece suporte à rotação de chaves em discos persistentes ou imagens existentes. Uma vez que uma máquina é provisionada, ela está vinculada à versão da chave em uso no momento em que foi criada. No entanto, uma nova versão da chave pode ser criada e essa nova chave é usada para máquinas recém-provisionadas ou recursos criados quando um catálogo é atualizado com uma nova imagem mestre.

CONSIDERAÇÕES IMPORTANTES SOBRE CONJUNTOS DE CHAVES

Os conjuntos de chaves não podem ser renomeados ou excluídos. Além disso, você pode incorrer em cobranças imprevistas ao configurá-los. Ao excluir ou remover um conjunto de chaves, o Google Cloud exibe uma mensagem de erro:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

Dica:

Para obter mais informações, consulte Editar ou excluir um conjunto de chaves do console.

Compatibilidade de acesso uniforme em nível de bucket

O Citrix Virtual Apps and Desktops é compatível com a política de controle de acesso uniforme em nível de bucket no Google Cloud. Essa funcionalidade aumenta o uso da política IAM que concede

permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com o controle de acesso uniforme em nível de bucket, o Citrix Virtual Apps and Desktops 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 em nível de bucket para obter informações gerais sobre o acesso uniforme em nível de bucket do Google Cloud. Para obter informações de configuração, consulte Exigir acesso uniforme em nível de bucket.

Criar um catálogo de máquinas usando PowerShell

Esta seção detalha como você pode criar catálogos usando PowerShell:

- Criar um catálogo com disco de cache de write-back persistente
- Melhorar o desempenho de inicialização com MCSIO
- Criar um catálogo de máquinas usando um perfil de máquina
- Criar um catálogo de máquinas com perfil de máquina como um modelo de instância
- Usar PowerShell para criar um catálogo com VM blindada
- Criar VMs do Windows 11 no nó de locatário único

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 PowerShell `New-ProvScheme` `CustomProperties`.

> **Dica:**
>
> Use o parâmetro PowerShell aqui apenas para conexões de hospedagem baseadas em nuvem. Se você quiser provisionar máquinas usando um disco de cache de write-back persistente para uma solução local (por exemplo, XenServer®), o PowerShell não é necessário porque o disco persiste automaticamente.
>
> Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

Nota:

Esse comportamento se aplica tanto ao Azure quanto ao GCP, onde o disco de cache de write-back MCSIO padrão é excluído e recriado durante o ciclo de energia. Você pode optar por manter o disco para evitar a exclusão e recriação do disco de cache de write-back MCSIO.

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 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 da interface de gerenciamento.

Nota:

Se a propriedade `PersistWBC` for omitida, a propriedade assume o valor padrão `false` e o cache de write-back é excluído quando a máquina é desligada da interface de gerenciamento.

Por exemplo, usando o parâmetro CustomProperties para definir `PersistWBC` como `true`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
```

```
</CustomProperties>
```

Nota:

A propriedade `PersistWBC` só pode ser definida usando o cmdlet PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como `true`:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"
```

```
-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Melhorar o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO está habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

Para habilitar este recurso, defina a propriedade personalizada `PersistOSDisk` como `true`. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
```
```

```
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS), você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Quando o parâmetro `MachineProfile` não é usado, as propriedades de hardware são capturadas da VM da imagem mestre ou do snapshot. Algumas propriedades que você define explicitamente, por exemplo, `StorageType`, `CatalogZones` e `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"`. Este comando não altera o perfil de máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.
- Você também pode atualizar a imagem mestre, no entanto, ao atualizar a imagem mestre, as propriedades de hardware não são atualizadas. Se você quiser atualizar as propriedades de hardware, deve atualizar o perfil da máquina usando o comando `Set-ProvScheme`. Essas alterações se aplicarão apenas às novas máquinas no catálogo. Para atualizar as propriedades de hardware de uma máquina existente, você pode usar o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

> **Nota:**
>
> - `StartsNow` indica que a hora de início agendada é a hora atual.
> - `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

Criar um catálogo de máquinas com perfil de máquina como um modelo de instância

Você pode selecionar um modelo de instância do GCP como entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP e, portanto, são muito econômicos.

Criar um novo catálogo de máquinas com perfil de máquina como um modelo de instância

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Encontre um modelo de instância em seu projeto GCP usando o seguinte comando:

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. Crie um novo catálogo de máquinas com perfil de máquina como um modelo de instância usando o comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

Para obter mais informações sobre o comando New-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Conclua a criação do catálogo de máquinas usando comandos PowerShell. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância

As etapas detalhadas para alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância são:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Para obter informações sobre o comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Usar PowerShell para criar um catálogo com VM blindada

Você pode criar um catálogo de máquinas MCS com propriedades de VM blindada. Uma máquina virtual blindada é reforçada por um conjunto de controles de segurança que fornecem integridade verificável de suas instâncias do Compute Engine, usando recursos avançados de segurança da

plataforma, como inicialização segura, um módulo de plataforma confiável virtual, firmware UEFI e monitoramento de integridade.

O MCS oferece suporte à criação do catálogo usando o fluxo de trabalho de perfil de máquina. Se você usar o fluxo de trabalho de perfil de máquina, deverá habilitar as propriedades de VM blindada de uma instância de VM. Você pode então usar esta instância de VM como entrada de perfil de máquina.

Para criar um catálogo de máquinas MCS com VM blindada usando o fluxo de trabalho de perfil de máquina.

1. Habilite as opções de VM blindada de uma instância de VM no console do Google Cloud. Consulte Início rápido: Habilitar opções de VM blindada.
2. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina usando a instância de VM.
    a. Abra uma janela do PowerShell.
    b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
    c. Crie um pool de identidades se ainda não tiver sido criado.
    d. Execute o comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. Conclua a criação do catálogo de máquinas.

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
```

Para aplicar a alteração feita em `Set-ProvScheme` às VMs existentes, execute o comando `Set-ProvVMUpdateTimeWindow`.

1. Execute o comando `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. Reinicie as VMs.

Criar VMs do Windows 11 no nó de locatário único

Você pode criar VMs do Windows 11 no GCP. No entanto, se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, você deve habilitar o vTPM na origem do perfil da máquina (VM ou modelo de instância).

As principais etapas para criar VMs do Windows 11 no nó de locatário único são:

1. Configure os ambientes de virtualização do Google Cloud. Para obter informações, consulte Ambientes do Google Cloud.
2. Instale o VDA. Consulte Instalar VDAs.
3. Crie uma conexão com os ambientes do Google Cloud. Para obter informações, consulte Conexão com ambientes do Google Cloud.
4. Crie uma imagem mestre do Windows 11 Bring Your Own License (BYOL) e importe a imagem para o Google Cloud. Consulte Criar uma imagem mestre BYOL do Windows 11.
5. Crie a origem do perfil da máquina: Provisione a VM no nó de locatário único e habilite o vTPM do perfil da máquina de origem. Consulte Provisionar VM no nó de locatário único.
6. Crie um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11 habilitada com vTPM. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único. Consulte Criar um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11.

Criar uma imagem mestre BYOL do Windows 11

Existem duas opções para criar uma imagem mestre BYOL do Windows 11 e importar a imagem mestre para o Google Cloud:

- Usar as Ferramentas de Compilação do Google Cloud
- Criar a imagem mestre em qualquer outro hipervisor

USAR AS FERRAMENTAS DE COMPILAÇÃO DO GOOGLE CLOUD

1. Carregue os arquivos ISO do Windows 11, GCP SDK, .NET framework e instalador do PowerShell para o bucket de armazenamento do GCP.
2. Forneça o local do arquivo no arquivo `.yaml` de compilação na nuvem como parâmetro.
3. Execute o seguinte Cloud Build a partir da linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

Para obter informações completas, consulte Criar imagens BYOL personalizadas do Windows.

CRIAR A IMAGEM MESTRE EM QUALQUER OUTRO HIPERVISOR

1. Crie a imagem mestre do Windows 11 usando qualquer outro hipervisor.
2. Exporte a imagem mestre em formato OVF para a máquina local.
3. Carregue os arquivos OVF para o bucket de armazenamento do GCP usando a CLI gcloud local.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. Execute o seguinte Cloud Build a partir da linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

Nota:

Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

Provisionar VM em nó de locatário único

Use nós de locatário único para manter suas VMs fisicamente separadas de VMs em outros projetos, ou para agrupar suas VMs no mesmo hardware de host. Para obter informações sobre o nó de locatário único, consulte o documento do GCP Visão geral da locação única.

Para provisionar uma VM (origem do perfil da máquina) no nó de locatário único, consulte o documento do GCP Provisionar VMs em nós de locatário único.

Nota:

- Selecione o mesmo tipo de instância e região que o grupo de nós.
- Habilite o vTPM na seção VM Blindada. Para obter mais informações, consulte Início rápido: Habilitar opções de VM Blindada.
- Desative o Bitlocker na VM de origem.

Criar um catálogo de máquinas MCS usando a origem do perfil de máquina do Windows 11

Você pode criar um catálogo de máquinas MCS para criar VMs do Windows 11 usando o Web Studio ou comandos PowerShell.

Nota:

- Para a imagem mestre, selecione o Snapshot ou a VM do Windows 11.

- Para a origem do perfil da máquina, selecione a VM do Windows 11 como perfil da máquina. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único.

Para obter informações sobre como usar o Web Studio, consulte Criar um catálogo de máquinas usando o Web Studio.

Para obter informações sobre comandos PowerShell, consulte Criar um catálogo de máquinas usando um perfil de máquina

Depois de criar o catálogo e ligar as VMs, você pode ver as VMs do Windows 11 sendo executadas no nó de locatário único no console do Google Cloud.

VMs e discos com rótulos herdados

As VMs e discos do catálogo de máquinas MCS (Disco de Identidade, Disco de Retorno de Cache de Gravação e disco do SO) podem herdar os rótulos de uma fonte de perfil de máquina (instância de VM GCP ou modelo de instância). Você pode usar os rótulos para distinguir instâncias pertencentes a diferentes equipes (por exemplo, team:research e team:analytics) e usá-los ainda mais para contabilidade de custos ou orçamento. Para obter mais informações sobre rótulos, consulte o documento do GCP Organizar recursos usando rótulos.

Você pode criar um novo catálogo, atualizar um catálogo existente e atualizar VMs existentes para herdar os rótulos usando a fonte do perfil da máquina.

Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Você pode fazer o seguinte:

- Criar um catálogo com rótulos herdados
- Atualizar um catálogo existente com rótulos herdados
- Atualizar VMs existentes com rótulos herdados
- Recuperar informações para rótulos de VM e disco de inicialização
- Remover uma VM

Criar um catálogo com rótulos herdados

Para criar um catálogo de máquinas MCS onde VMs e discos herdam rótulos da fonte do perfil da máquina, faça o seguinte:

1. Crie uma fonte de perfil de máquina (instância de VM ou modelo de instância) com rótulos. Para obter informações sobre como criar VMs com rótulos, consulte o documento do GCP Criar recursos com rótulos. Um modelo de instância é criado a partir da VM e assume os rótulos definidos na VM.
2. Crie um catálogo MCS usando o Web Studio ou comandos PowerShell.
3. Se estiver usando o Web Studio, na página **Imagem**, selecione **Usar um perfil de máquina** e, em seguida, selecione a VM ou o modelo.
4. Se estiver usando comandos do PowerShell, faça o seguinte:

    a. Abra a janela do PowerShell.

    b. Execute asnp citrix*.

    c. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas.

    d. Crie as contas de computador AD necessárias no Active Directory.

    e. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

    New-ProvScheme com modelo como entrada de perfil de máquina (Catálogo persistente):

    ```
    New-ProvScheme `

    -ProvisioningSchemeName "catalog-name" `

    -HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

    -IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

    -MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

    -MachineProfile "XDHyp:\HostingUnits\hosting-unit-
    name\instanceTemplates.folder\instance-template-name.template" `
    ```

    New-ProvScheme com modelo de instância como entrada de perfil de máquina (Catálogo não persistente):

    ```
    New-ProvScheme `

    -ProvisioningSchemeName "catalog-name" `
    ```

```
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

New-ProvScheme com instância de VM como entrada de perfil de máquina (Catálogo persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme com instância de VM como entrada de perfil de máquina (Catálogo não persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

```
-CleanOnBoot
```

f. Registre o esquema de provisionamento como um catálogo de broker.

g. Adicione VMs ao catálogo.

Atualizar um catálogo existente com rótulos herdados

Para atualizar um catálogo existente para ter um novo perfil de máquina, execute o comando Set-ProvScheme. Depois de executar o comando, todas as novas VMs adicionadas ao catálogo terão os rótulos da nova origem do perfil de máquina. O catálogo não persistente é atualizado na próxima inicialização.

Por exemplo:

Set-ProvScheme com modelo de instância como entrada de perfil de máquina:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme com instância de VM como entrada de perfil de máquina:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

Atualizar VMs existentes com rótulos herdados

Para atualizar as VMs existentes com a fonte de perfil de máquina atualizada, execute os seguintes comandos:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

3. Reinicie as VMs.

Recuperar informações para rótulos de VM e disco de inicialização

Após criar as VMs, você pode obter as informações do rótulo da VM e do disco de inicialização usando o comando `Get-Item` com o parâmetro `AdditionalData`.

Para recuperar informações do rótulo da VM, execute o seguinte comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

Para recuperar informações do rótulo do disco de inicialização, execute o seguinte comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

Nota:

Para manter a consistência entre os vários hipervisores, usamos o termo Tags para exibir os rótulos do GCP.

Remover uma VM

Você pode optar por remover uma VM de um catálogo, mas não excluir a VM do GCP. Nesse caso, apenas os rótulos Citrix são removidos da VM. Todos os outros rótulos adicionados não são excluídos da VM. Você pode remover uma VM usando o Web Studio ou comandos PowerShell.

USANDO O WEB STUDIO

1. Selecione e clique com o botão direito na VM.
2. Clique em **Excluir**.
3. Selecione **Remover as máquinas virtuais do catálogo, mas não excluir as máquinas virtuais**.

USANDO COMANDOS POWERSHELL

Execute `Remove-ProvVM` com o parâmetro `ForgetVM`. Para obter mais informações, consulte a documentação do SDK Remove-ProvVM.

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 apenas o fluxo de trabalho de perfil de máquina para este recurso.

Para pesquisar o produto Citrix VDA VM através do Google Cloud Marketplace, acesse https://console.cloud.google.com/marketplace.

Você pode usar uma imagem personalizada ou uma imagem Citrix ready® no **Google Cloud Marketplace** para atualizar uma imagem de um catálogo de máquinas.

> **Nota:**
>
> Se o perfil da máquina não contiver informações de tipo de armazenamento, o valor será derivado das propriedades personalizadas.

> As imagens suportadas do Google Cloud Marketplace são:

- Windows 2019 Single Session
- Windows 2019 Multissessão
- Ubuntu

Exemplo de uso de uma imagem pronta para Citrix como fonte para criar um catálogo de máquinas:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Google Cloud Platform

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas

Criar um catálogo de máquinas HPE Moonshot

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes HPE Moonshot.

> **Observação:**
>
> - Criar uma conexão com o HPE Moonshot
> - Certifique-se de ter um ou mais nós HPE Moonshot disponíveis e instale VDAs nesses nós.
> - Para obter informações sobre como criar a imagem inicial do cartucho HPE Moonshot, consulte o Guia do Usuário de Implantação de SO no Moonshot.

> Você pode criar um catálogo de máquinas HPE Moonshot usando:

- Web Studio
- Comandos PowerShell

Criar um catálogo de máquinas usando o Web Studio

No assistente de **Configuração do Catálogo de Máquinas**:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e **Outro serviço ou tecnologia**.

3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode fazer o seguinte:

    - Clique em **Adicionar Máquinas** para adicionar máquinas manualmente. A janela **Selecionar VMs** é exibida. Expanda a conexão do chassi HPE Moonshot que você criou anteriormente e selecione os nós (VMs) que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.
    - Clique em **Adicionar arquivo CSV** para adicionar máquinas em massa. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

As páginas **Escopos** e **Resumo** não contêm informações específicas do HPE Moonshot.

Criar um catálogo de máquinas usando comandos PowerShell

Execute os comandos PowerShell `New-BrokerCatalog` e `New-BrokerMachine` para criar um catálogo de broker e importar máquinas para o catálogo de broker.

Por exemplo:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -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"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo HPE Moonshot

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o HPE Moonshot
- Criar catálogos de máquinas

Criar um catálogo do Microsoft Azure

> **Nota:**
>
> Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência a Azure Active Directory, Azure AD ou AAD agora se refere a Microsoft Entra ID.

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de criar um catálogo do Microsoft Azure, você precisa concluir a criação de uma conexão com o Microsoft Azure. Consulte Conexão com o Microsoft Azure.

Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio
- Criar um catálogo de máquinas usando PowerShell

Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio

Uma imagem pode ser um disco, um instantâneo ou uma versão de imagem de uma definição de imagem dentro da Galeria de Computação do Azure que é usada para criar as VMs em um catálogo de máquinas. Antes de criar o catálogo de máquinas, crie uma imagem no Azure Resource Manager. Para obter informações gerais sobre imagens, consulte Criar catálogos de máquinas.

> **Observação:**
>
> O suporte para usar uma imagem mestre de uma região diferente da configurada na conexão do host foi descontinuado. Use a Galeria de Computação do Azure para replicar a imagem mestre para a região desejada.

> Ao criar um catálogo de máquinas MCS, uma VM temporária é criada com base na VM original para executar tarefas de preparação, como habilitar DHCP e rearmar a licença. Essa VM temporária é chamada de VM de preparação. O nome dessa VM de preparação segue o formato **Preparati-84x9n**, onde os últimos cinco caracteres são gerados aleatoriamente para evitar duplicação. A convenção de nomenclatura para essa VM de preparação é fixa e não pode ser personalizada. Após a conclusão das tarefas de preparação, a VM de preparação é destruída.

Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. O grupo de segurança de rede é criado automaticamente uma vez por catálogo. O nome do grupo de segurança de rede é `Citrix-Deny-All-a3pgu-GUID`, onde GUID é gerado aleatoriamente. Por exemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

No assistente de criação de catálogo de máquinas:

- As páginas **Tipo de Máquina** e **Gerenciamento de Máquinas** não contêm informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.
- Na página **Imagem**, escolha uma imagem que você deseja usar como modelo para criar máquinas neste catálogo.

  Se você selecionar **Imagem mestre** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e siga estas etapas para selecionar uma imagem mestre conforme necessário:

a. (Aplicável apenas a conexões configuradas com imagens compartilhadas dentro ou entre locatários) Selecione uma assinatura onde a imagem reside.
b. Selecione um grupo de recursos.
c. navegar para o VHD do Azure, a Galeria de Computação do Azure ou a versão da imagem do Azure. Adicione uma nota para a imagem selecionada, se necessário.

Ao selecionar uma imagem, considere o seguinte:

- Verifique se um Citrix VDA está instalado na imagem.
- Se você selecionar um VHD anexado a uma VM, deverá desligar a VM antes de prosseguir para a próxima etapa.

Observação:

- A assinatura correspondente à conexão (host) que criou as máquinas no catálogo é indicada com um ponto verde. As outras assinaturas são aquelas que têm a Azure Compute Gallery compartilhada com essa assinatura. Nessas assinaturas, apenas galerias compartilhadas são mostradas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens dentro de um locatário (entre assinaturas) e Compartilhar imagens entre locatários.
- O uso de um perfil de máquina com inicialização confiável como **Tipo de Segurança** é obrigatório ao selecionar uma imagem ou instantâneo que tenha a inicialização confiável habilitada. Você pode então habilitar ou desabilitar o SecureBoot e o vTPM especificando seus valores no perfil da máquina. A Inicialização Confiável não é suportada para a Galeria de Imagens Compartilhadas. Para obter informações sobre a inicialização confiável do Azure, consulte `<https://docs.microsoft.com/pt-br/azure/virtual-machines/trusted-launch>`.
- Você pode criar um esquema de provisionamento usando disco de SO efêmero no Windows com inicialização confiável. Ao selecionar uma imagem com inicialização confiável, você deve selecionar um perfil de máquina com inicialização confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
- Quando a replicação da imagem estiver em andamento, você pode prosseguir e selecionar a imagem como imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode levar mais tempo para ser concluída enquanto a imagem

está sendo replicada. O MCS exige que a replicação seja concluída em uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo falhará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.

- Ao selecionar uma imagem mestre para catálogos de máquinas no Azure, o MCS identifica o tipo de SO com base na imagem mestre e no perfil de máquina que você seleciona. Se o MCS não conseguir identificá-lo, selecione o tipo de SO que corresponde à imagem mestre.
- Você pode provisionar um catálogo de VMs Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem mais antiga que não tenha informações de geração é uma imagem Gen1.

Se você selecionar **Imagem preparada** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e selecione uma imagem preparada conforme necessário.

Para garantir a criação bem-sucedida da VM, verifique se a imagem tem o Citrix VDA 2311 ou posterior instalado e se o MCSIO está presente no VDA.

Depois de selecionar uma imagem, a caixa de seleção **Usar um perfil de máquina (obrigatório para Azure Active Directory)** é selecionada automaticamente. Clique em **Selecionar um perfil de máquina** para navegar até uma VM ou uma especificação de modelo ARM de uma lista de grupos de recursos. As VMs no catálogo podem herdar configurações do perfil de máquina selecionado.

Valide a especificação do modelo ARM para garantir que ela possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Existem duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Avançar**. Mensagens de erro aparecerão se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`

- `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Exemplos de configurações que as VMs podem herdar de um perfil de máquina incluem:

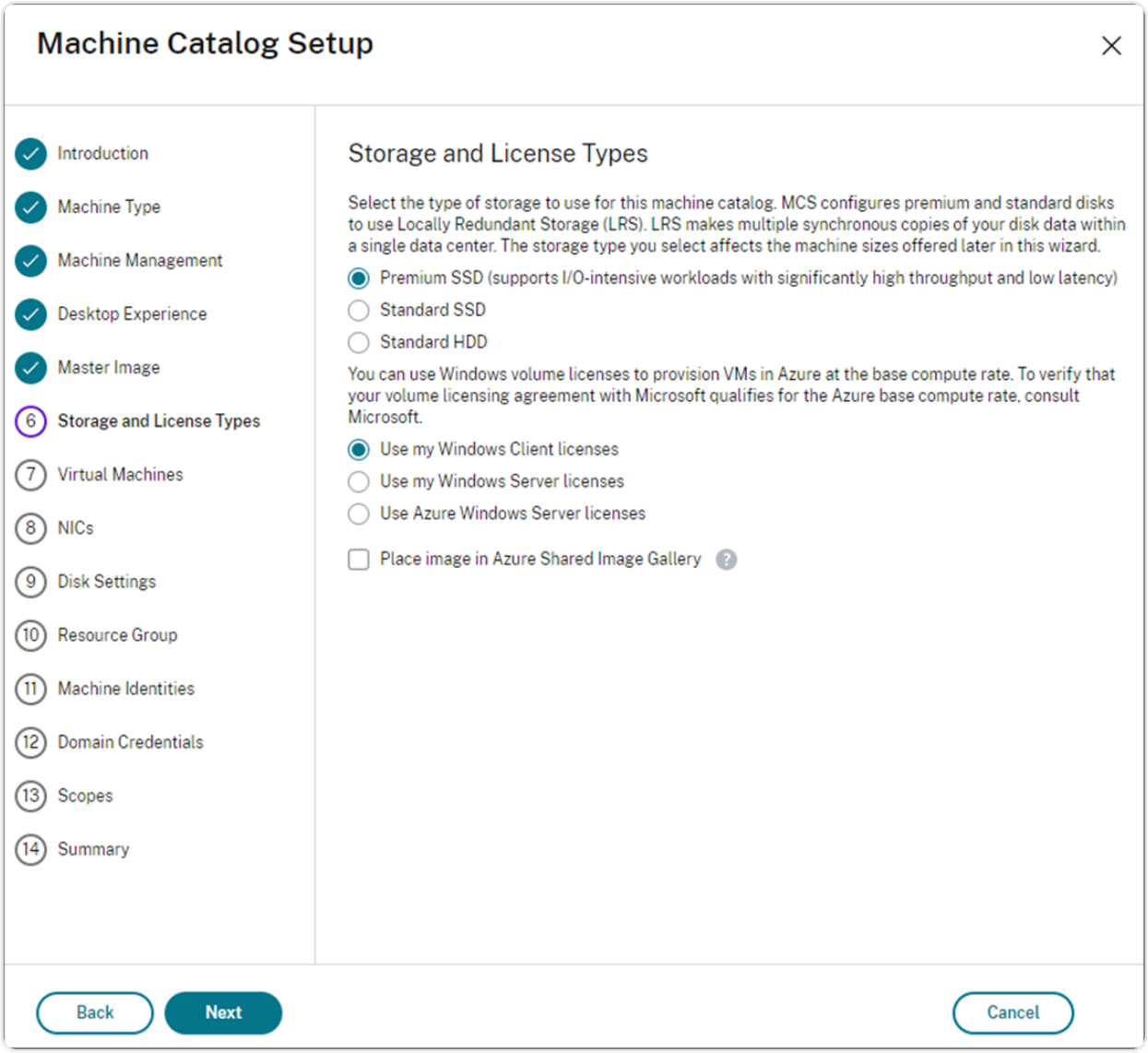
- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado a discos de SO e MCSIO)
- Tamanho da máquina (salvo especificação em contrário)
- Tags colocadas na VM

Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Catálogos de Máquinas**, selecione o catálogo para visualizar seus detalhes no painel inferior. Em seguida, clique na guia **Propriedades do Modelo** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **Visualizar tudo**.

Se você deseja que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts dedicado** e, em seguida, 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 VMs. Seu servidor é dedicado à sua assinatura do Azure, não sendo compartilhado com outros assinantes. Ao usar um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em execução nesse host. Esse recurso é adequado para cenários em que você precisa atender a requisitos regulatórios ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

> **Importante:**
>
> - Somente os grupos de hosts que têm o posicionamento automático do Azure habilitado são exibidos.
> - O uso de um grupo de hosts altera a página **Máquinas Virtuais** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são exibidos nessa página. Além disso, as Zonas de Disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Tipos de Armazenamento e Licença** aparece somente quando você usa uma imagem do Azure Resource Manager.



Você tem os seguintes tipos de armazenamento para usar no catálogo de máquinas:

- **SSD Premium**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência, adequada para VMs com cargas de trabalho intensivas em E/S.
- **SSD Standard**. Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
- **Standard HDD**. Oferece uma opção de armazenamento em disco confiável e de baixo custo, adequada para VMs que executam cargas de trabalho insensíveis à latência.
- **Disco de SO efêmero do Azure**. Oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Alternativamente, você pode usar o PowerShell para criar máquinas que usam discos de

SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Esteja ciente das seguintes considerações ao usar um disco de SO efêmero:

- O disco de SO efêmero do Azure e o MCS I/O não podem ser habilitados ao mesmo tempo.
- Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
- Você não pode usar a opção **Manter VM e disco do sistema durante ciclos de energia** oferecida posteriormente no assistente.

> **Observação:**
>
> 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 standard para usar o Armazenamento Redundante Local (LRS). O LRS faz várias cópias síncronas dos dados do seu disco dentro de um único datacenter. 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/pt-br/azure/storage/common/storage-introduction/>`
> - `<https://docs.microsoft.com/pt-br/azure/virtual-machines/premium-storage-performance/>`
> - `<https://docs.microsoft.com/pt-br/azure/storage/common/storage-redundancy/>`

Selecione se deseja usar licenças Windows existentes ou licenças Linux.

- Licenças Windows: Usar licenças Windows juntamente com imagens Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs Windows no Azure a um custo reduzido. Existem dois tipos de licenças:

- **Licença do Windows Server**. Permite 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/pt-br/pricing/hybrid-benefit/>`. O Benefício Híbrido do Azure reduz o custo de execução de VMs no Azure para a taxa de computação base, dispensando o custo de licenças extras do Windows Server da galeria do Azure.
- **Licença do Cliente Windows**. Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de Acesso de Cliente e Licenças de Gerenciamento.

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows_Server**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`.
- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows_Client**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`.

Alternativamente, você pode usar o SDK do PowerShell `Get-Provscheme` para fazer a verificação. Por exemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre este cmdlet, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`.

- Licenças Linux: Com as licenças Linux bring-your-own-subscription (BYOS), você não precisa pagar pelo software. A cobrança do BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:
  - **RHEL_BYOS**: Para usar o tipo RHEL_BYOS com sucesso, habilite o Red Hat Cloud Access em sua assinatura do Azure.
  - **SLES_BYOS**: As versões BYOS do SLES incluem suporte da SUSE.

  Você pode definir o valor de LicenseType para as opções do Linux em `New-ProvScheme` e `Set-ProvScheme`.

Exemplo de configuração de LicenseType para RHEL_BYOS em `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

Exemplo de configuração de LicenseType para SLES_BYOS em `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

Observação:

Se o valor `LicenseType` estiver vazio, os valores padrão serão Licença do Azure Windows Server ou Licença do Azure Linux, dependendo do valor de OsType.

Exemplo de como definir LicenseType como vazio:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
```

```
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

Consulte os seguintes documentos para entender os tipos de licença e seus benefícios:

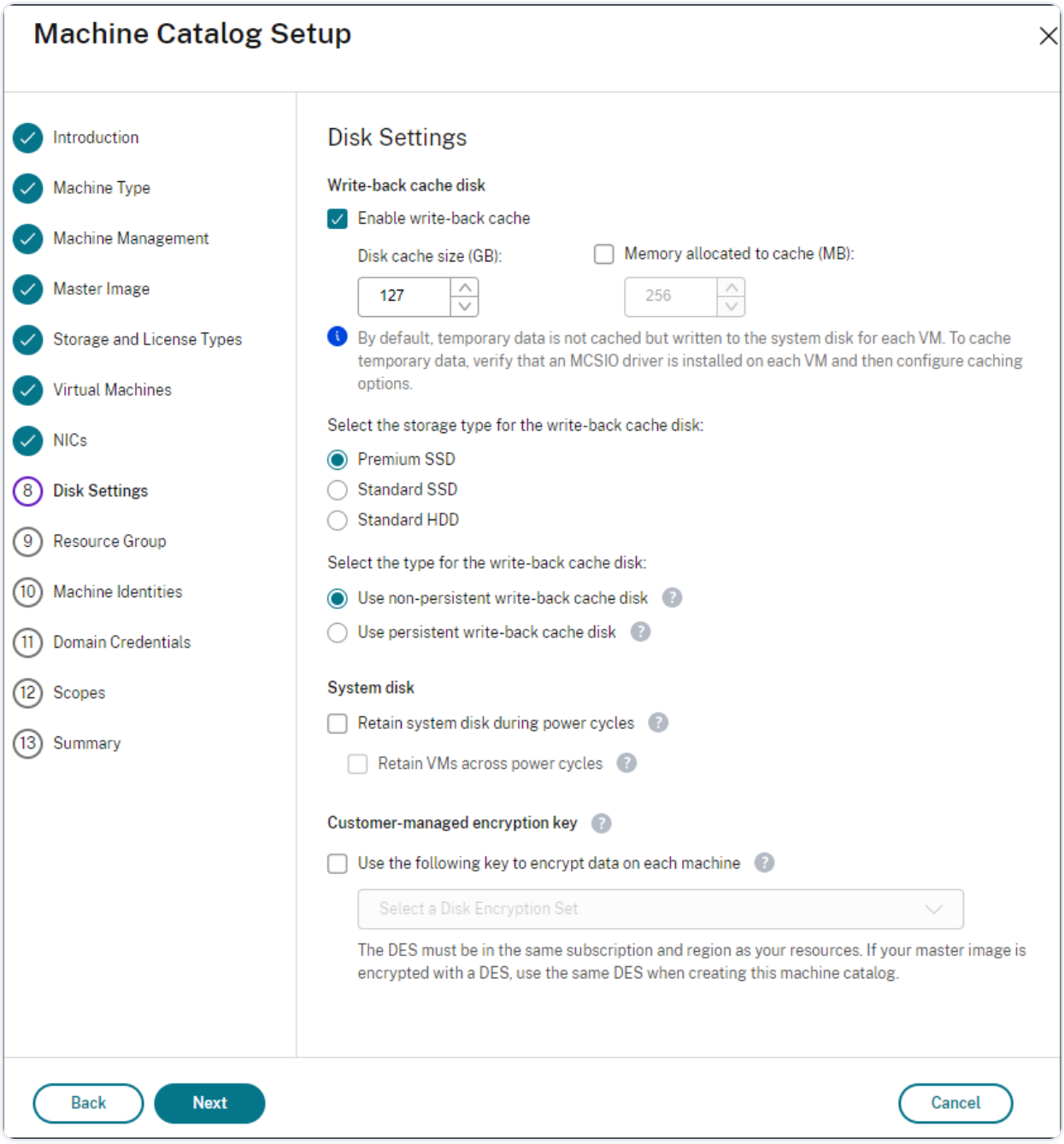
- `<https://docs.microsoft.com/pt-br/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/pt-br/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

A Galeria de Computação do Azure (anteriormente Galeria de Imagens Compartilhadas do Azure) é um repositório para gerenciar e compartilhar imagens. Ela permite que você disponibilize suas imagens em toda a sua organização. Recomendamos que você armazene uma imagem na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos de SO do VDA. Depois de selecionar **Colocar imagem preparada na Galeria de Computação do Azure**, a seção **Configurações da Galeria de Computação do Azure** aparece, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

- **Proporção de máquinas virtuais para réplicas de imagem**. Permite que você especifique 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. Para máquinas persistentes, esse número padrão é 1.000.
- **Contagem máxima de réplicas**. Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 100.

> **Observação:**
>
> Uma galeria é criada no ACG para armazenar a imagem. Esta galeria é acessível apenas ao MCS para criação de VM e não aparece na página **Selecionar uma imagem**.

- Na página **Máquinas Virtuais**, indique quantas VMs você deseja criar. Você deve especificar pelo menos uma 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 orientações no artigo Criar catálogos de máquinas.
- Na página **Configurações de Disco**, escolha se deseja habilitar o cache de write-back. Com o recurso de otimização de armazenamento do MCS ativado, você pode configurar as seguintes configurações ao criar um catálogo. Essas configurações se aplicam a ambientes Azure e GCP.



Após habilitar o cache de write-back, você pode fazer o seguinte:

- Configure o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
- Selecione o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:
  - SSD Premium
  - SSD Standard
  - HDD Standard
- Escolha se deseja que o disco de cache de write-back persista para as VMs provisionadas. Selecione **Habilitar cache de write-back** para disponibilizar as opções. Por padrão, **Usar disco de cache de write-back não persistente** é selecionado.
- Selecione o tipo para o disco de cache de write-back.
  - **Usar disco de cache de write-back não persistente**. Se selecionado, o disco de cache de write-back é excluído durante os ciclos de energia. Quaisquer dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache de write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Propriedades do Modelo**. Se o disco temporário for usado, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Sim (usando o disco temporário da VM)**. Caso contrário, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Não (não usando o disco temporário da VM)**.
  - **Usar disco de cache de write-back persistente**. Se selecionado, o disco de cache de write-back persiste para as VMs provisionadas. Habilitar a opção aumenta seus custos de armazenamento.
- Escolha se deseja reter VMs e discos de sistema para VDAs durante os ciclos de energia.

  Manter VM e disco do sistema durante ciclos de energia. Disponível quando você selecionou **Habilitar cache de write-back**. Por padrão, as VMs e os discos do sistema são excluídos no desligamento e recriados na inicialização. Se você deseja reduzir os tempos de reinicialização da VM, selecione esta opção. Lembre-se de que habilitar esta opção também aumenta os custos de armazenamento.

- Escolha se deseja habilitar **Economia de custos de armazenamento**. Se ativado, economize custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Padrão quando a VM for desligada. A VM retorna às suas configurações originais na reinicialização. A opção se aplica a discos de armazenamento e de cache de write-back. Alternativamente, você também pode usar o PowerShell. Consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

  > **Observação:**
  >
  > A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie futuras alterações de tipo de armazenamento. Para obter mais informações, consulte este artigo da Microsoft.

- Escolha se deseja criptografar dados nas máquinas provisionadas no catálogo. A criptografia do lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia no nível do disco gerenciado e proteger os dados nas máquinas do catálogo. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

- Na página **Grupo de Recursos**, escolha se deseja criar grupos de recursos ou usar grupos existentes.

  - Se você optar por criar grupos de recursos, selecione **Avançar**.
  - Se você optar por usar grupos de recursos existentes, selecione os grupos na lista **Grupos de Recursos de Provisionamento Disponíveis**. **Lembre-se**: Selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Uma mensagem aparece se você escolher poucos. Você pode querer selecionar mais do que o mínimo necessário se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que ele é criado.

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

- Na página **Identidades da Máquina**, escolha um tipo de identidade e configure identidades para as máquinas neste catálogo. Se você selecionar as VMs como **Unidas ao Azure Active Directory**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:

a. No campo **Tipo de identidade**, selecione **Unido ao Azure Active Directory**. A opção **Grupo de segurança do Azure AD (opcional)** aparece.

b. Clique em **Grupo de segurança do Azure AD: Criar novo**.

c. Insira um nome de grupo e depois clique em **Criar**.

d. Siga as instruções na tela para fazer login no Azure. Se o nome do grupo não existir no Azure, um ícone verde aparecerá. Caso contrário, uma mensagem de erro aparecerá solicitando que você insira um novo nome.

e. Insira o esquema de nomenclatura da conta de máquina para as VMs.

Após a criação do catálogo, o Citrix Virtual Apps and Desktops™ 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 neste catálogo são adicionadas automaticamente ao grupo de segurança.

Adicionar VMs com um esquema de nomenclatura diferente a este catálogo exige que você faça login no Azure. O Citrix Virtual Apps and Desktops pode então acessar o Azure e criar uma regra de associação dinâmica com base no novo esquema de nomenclatura.

Ao excluir este catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.

- As páginas **Credenciais de Domínio** e **Resumo** não contêm informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.

Conclua o assistente.

Condições para que o disco temporário do Azure seja elegível para disco de cache de write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem satisfeitas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.
- O tamanho da VM do Azure escolhido deve incluir um disco temporário.
- O disco do SO efêmero não precisa ser habilitado.
- Aceitar colocar o arquivo de cache de write-back no disco temporário do Azure.

- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco de cache de write-back + espaço reservado para arquivo de paginação + 1 GB de espaço de buffer).

Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back ao criar um catálogo de máquinas.

CENÁRIO	RESULTADO
Todas as condições para usar o disco temporário para cache de write-back são satisfeitas.	O arquivo WBC `mcsdif.vhdx` é colocado no disco temporário.
O disco temporário tem espaço insuficiente para uso do cache de write-back.	Um disco VHD `MCSWCDisk` é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.
O disco temporário tem espaço suficiente para uso do cache de write-back, mas `UseTempDiskForWBC` está definido como **false**.	Um disco VHD `MCSWCDisk` é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la no Web Studio e em comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Vá para o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a VM e a interface de rede. No menu **...** na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para provisionamento de catálogo. Verifique no arquivo JSON se as seções `parameters` e `variables` são:

   ```
   "parameters": {},

   "variables": {}
   ```

3. Clique em **Baixar** para salvar o modelo como arquivo JSON.

4. No portal do Azure, selecione **Especificações de modelo** e clique em **Importar modelo**.
5. Procure e importe o perfil da máquina (em JSON) salvo em seu computador.
6. Forneça o **Nome**, **Assinatura**, **Grupo de Recursos**, **Localização** e **Versão**. Clique em **Avançar: Editar Modelo**.
7. Crie **Revisar+Criar** e crie a especificação de modelo.
8. Na página **Especificações de Modelo**, verifique a especificação de modelo que você acabou de criar. Clique na especificação de modelo. No painel esquerdo, clique em **Versões**.
9. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, altere para a especificação de modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação de modelo.

Você pode obter informações sobre a especificação de modelo e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação de modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- Para obter informações sobre a versão da especificação de modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

Usar especificação de modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou comandos do PowerShell.

- Para o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio
- Para o PowerShell, consulte Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell

Criptografia do lado do servidor do Azure

O Citrix Virtual Apps and Desktops oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados do seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Criptografia do lado do servidor do Armazenamento em Disco do Azure.

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco é criptografado, você altera a chave atual no `DiskEncryptionSet`. Todos os recursos associados a esse `DiskEncryptionSet` mudam para serem criptografados com a nova chave.
- Quando você desativa ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja ativada novamente ou você atribua uma nova chave. Qualquer catálogo que use a chave não pode ser ligado, e você não pode adicionar VMs a ele.

Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente

Considere o seguinte ao usar este recurso:

- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Discos, instantâneos e imagens criptografados com chaves gerenciadas pelo cliente não podem ser movidos para outro grupo de recursos e assinatura.
- Consulte o site da Microsoft para obter informações sobre as limitações dos conjuntos de criptografia de disco por região.

> **Nota:**
>
> Consulte Início Rápido: Criar um Key Vault usando o portal do Azure para obter informações sobre como configurar a criptografia do lado do servidor do Azure.

Chave de criptografia gerenciada pelo cliente do Azure

Ao criar um catálogo de máquinas, você pode escolher se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia do lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas do catálogo. Um Conjunto de Criptografia de Disco (DES) representa uma chave gerenciada pelo cliente. Para usar esse recurso, você deve primeiro criar seu DES no Azure. Um DES está no seguinte formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos.

Consulte Criando um catálogo de máquinas usando chave gerenciada pelo cliente.

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS oferece suporte apenas ao fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma VM ou uma especificação de modelo como entrada para um perfil de máquina.

Esse método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta.

Restrições:

A criptografia de disco do Azure no host é:

- Não suportada para todos os tamanhos de máquina do Azure
- Incompatível com a criptografia de disco do Azure

Para criar um catálogo de máquinas com capacidade de criptografia no host:

1. Verifique se a assinatura tem o recurso de criptografia no host habilitado ou não. Para fazer isso, consulte `<https://learn.microsoft.com/pt-br/rest/api/resources/features/get?tabs=HTTP/>`. Se não estiver habilitado, você deve habilitar o recurso para a assinatura. Para obter informações sobre como habilitar o recurso para sua assinatura, consulte

`<https://learn.microsoft.com/pt-br/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`.

2. Verifique se um tamanho de VM específico do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute um dos seguintes:

```
PS XDHyp:\Connections\<your connection>\east
us.region\serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
```

3. Crie uma VM ou uma especificação de modelo, como entrada para o perfil da máquina, no portal do Azure com a criptografia no host 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 **Criptografia no host** é habilitada.
   - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `securityProfile`.

4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina, selecionando uma VM ou uma especificação de modelo.

   - Disco do SO / Disco de Dados: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma
   - Disco do SO Efêmero: É criptografado apenas por meio de chave gerenciada pela plataforma
   - Disco de Cache: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma

   Você pode criar o catálogo de máquinas usando o Web Studio ou executando comandos PowerShell.

Recuperar informações de criptografia no host de um perfil de máquina

Você pode recuperar as informações de criptografia no host de um perfil de máquina ao executar o comando PowerShell com o parâmetro `AdditionalData`. Se o parâmetro `EncryptionAtHost` for **True**, isso indica que a criptografia no host está habilitada para o perfil de máquina.

Por exemplo: Quando a entrada do perfil de máquina é uma VM, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

Por exemplo: Quando a entrada do perfil de máquina é uma especificação de modelo, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

Criptografia dupla em disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Quaisquer catálogos criados com esse recurso têm todos os discos criptografados no lado do servidor com chaves gerenciadas pela plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a Chave de Criptografia e os Conjuntos de Criptografia de Disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. Discos de SO e dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

Nota:

- Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e comandos PowerShell. Consulte Criar um catálogo de máquinas com criptografia dupla para comandos PowerShell.
- Você pode usar um fluxo de trabalho baseado em perfil não-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 o fluxo de trabalho baseado em perfil não-máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetId` armazenado.

- Se você usar um perfil de máquina, poderá usar uma VM ou especificação de modelo como entrada de perfil de máquina.

Limitações:

- A criptografia dupla não é suportada para Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desativar uma chave DiskEncryptionSet associada a um catálogo, as VMs do catálogo serão desativadas.
- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você pode criar apenas até 50 conjuntos de criptografia de disco por região por assinatura.

Grupos de recursos do Azure

Os grupos de recursos de provisionamento do Azure fornecem uma maneira de provisionar as VMs que fornecem aplicativos e desktops aos usuários. Você pode adicionar grupos de recursos do Azure vazios existentes ao criar um catálogo de máquinas MCS, ou ter novos grupos de recursos criados 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 um principal de serviço de escopo total para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar um principal de serviço de escopo restrito para criar um catálogo de máquinas, você deve fornecer um Grupo de Recursos do Azure vazio e pré-criado para o catálogo.

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você reutilize o disco de cache ou o disco temporário para armazenar o disco do SO para uma máquina virtual habilitada para Azure. Essa funcionalidade é útil para ambientes Azure que exigem um disco SSD de maior desempenho em

vez de um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte Criar um catálogo com discos efêmeros do Azure.

> **Nota:**
>
> Catálogos persistentes não suportam discos de SO efêmeros.

> Os discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Imagens Compartilhadas.

Armazenando um disco temporário de SO efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM ou em um disco de recurso. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não possui cache ou possui cache insuficiente. Essas VMs têm um disco temporário ou de recurso para armazenar um disco de SO efêmero, como `Ddv4`.

Considere o seguinte:

- Um disco efêmero é armazenado no disco de cache da VM ou no disco temporário (de recurso) da VM. O disco de cache é preferido em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco do SO.
- Para atualizações, uma nova imagem que é maior que o disco de cache, mas menor que o disco temporário, resulta na substituição do disco de SO efêmero pelo disco temporário da VM.

Disco efêmero do Azure e otimização de armazenamento do Machine Creation Services (MCS) (MCS I/O)

O disco de SO efêmero do Azure e o MCS I/O não podem ser ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Você não pode criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- Os parâmetros do PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) falham com mensagens de erro apropriadas se você os definir como **true** em `New-ProvScheme` ou `Set-ProvScheme`.
- Para catálogos de máquinas existentes criados com ambas as funcionalidades ativadas, você ainda pode:

- atualizar um catálogo de máquinas.
- adicionar ou excluir VMs.
- excluir um catálogo de máquinas.

Galeria de Computação do Azure

Use a Galeria de Computação do Azure (anteriormente Galeria de Imagens Compartilhadas do Azure) como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação de discos do SO, melhorando os tempos de inicialização e de lançamento de aplicativos para VMs não persistentes. A galeria de imagens compartilhadas contém os três elementos a seguir:

- *Galeria*: As imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de Imagem da Galeria*: Esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- *Versão da Imagem da Galeria*: Cada imagem em uma Galeria de Imagens Compartilhadas pode ter várias versões, e cada versão pode ter várias réplicas em diferentes regiões. Cada réplica é uma cópia completa da imagem publicada.

> **Nota:**
>
> A funcionalidade da Galeria de Imagens Compartilhadas é compatível apenas com discos gerenciados. Não está disponível para catálogos de máquinas legados.

> Para obter mais informações, consulte Visão geral da Galeria de Computação do Azure.

Para obter informações sobre como criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure com o PowerShell, consulte Criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que seu desktop virtual seja criptografado na memória e protegido em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto VM quanto a especificação de modelo ARM como entrada de perfil de máquina.

Considerações importantes para VMs confidenciais

As considerações importantes para tamanhos de VM suportados e criação de catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM suportados: As VMs Confidenciais suportam os seguintes tamanhos de VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Crie catálogos de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com VMs Confidenciais do Azure usando o Web Studio e comandos do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquinas com VMs Confidenciais do Azure. Você pode usar uma VM ou especificação de modelo como entrada de perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar ambas habilitadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:
    - **VMGuestStateOnly**: VM confidencial com apenas o estado do convidado da VM criptografado
    - **DiskWithVMGuestState**: VM confidencial com disco do SO e estado do convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Ambos os discos do SO, normal e efêmero, podem ser criptografados.
  - Você pode obter informações de VM confidenciais de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM, usando o parâmetro AdditionalData. Por exemplo:

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
```

Os campos de dados adicionais são:

- DiskSecurityType
- ConfidentialVMDiskEncryptionSetId
- DiskSecurityProfiles

Para obter a propriedade de computação confidencial de um tamanho de máquina, execute o seguinte comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

O campo de dados adicionais é `ConfidentialComputingType`.

- Você não pode alterar a imagem mestre ou o perfil da máquina de tipo de segurança confidencial para não confidencial, ou de não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

Preparar imagens mestre e perfis de máquina

Antes de criar um conjunto de VMs confidenciais, siga estas etapas para preparar uma imagem mestre e um perfil de máquina para elas:

1. No portal do Azure, crie uma VM confidencial com configurações específicas, como:
   - **Tipo de Segurança**: Máquinas virtuais confidenciais
   - **Criptografia de disco do SO confidencial**: Habilitado.
   - **Gerenciamento de chaves**: Criptografia de disco confidencial com uma chave gerenciada pela plataforma Para obter mais informações sobre como criar VMs confidenciais, consulte este artigo da Microsoft.
2. Prepare a imagem mestre na VM criada. Instale os aplicativos necessários e o VDA na VM criada.

   > **Nota:**
   >
   > A criação de VMs confidenciais usando VHD não é suportada. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil da máquina usando uma destas formas:

- Use a VM existente criada na etapa 1 se ela possuir as propriedades de máquina necessárias.
- Se você optar por uma especificação de modelo ARM como perfil da máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos de VM confidencial, como *SecurityEncryptionType* e *diskEncryptionSet* (para chave gerenciada pelo cliente). Para obter mais informações, consulte Criar uma especificação de modelo do Azure.

> **Nota:**
>
> - Certifique-se de que a imagem mestre e o perfil da máquina tenham o mesmo tipo de chave de segurança.
> - Para criar VMs confidenciais que exigem criptografia de disco do SO confidencial com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil da máquina sejam idênticos.

Criar VMs confidenciais usando o Web Studio ou comandos PowerShell

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Web Studio, siga as etapas descritas em Criar catálogos de máquinas. Tenha as seguintes considerações em mente:

- Na página **Imagem**, selecione uma imagem mestre e um perfil de máquina que você preparou para a criação da VM confidencial. A seleção do perfil da máquina é obrigatória e apenas perfis que correspondem ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.
- Na página **Máquinas Virtuais**, apenas os tamanhos de máquina que suportam VMs confidenciais aparecem para seleção.
- Na página **Configurações de Disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

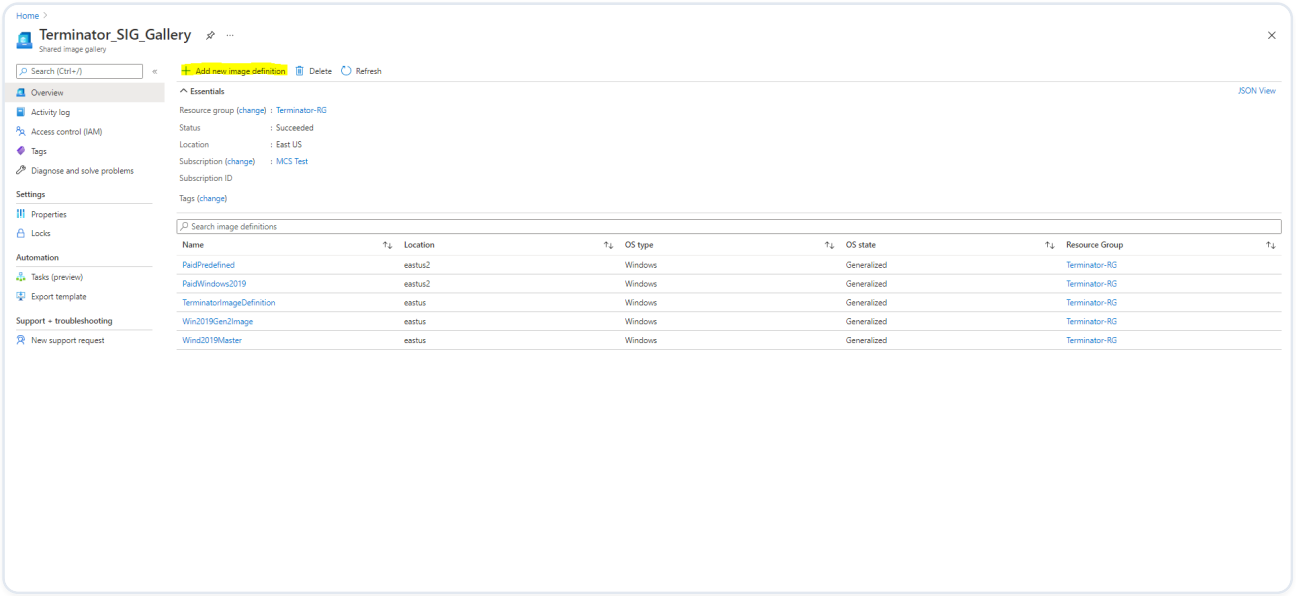
Azure Marketplace

O Citrix Virtual Apps and Desktops oferece suporte ao uso de uma imagem mestre no Azure que contém informações de plano para criar um catálogo de máquinas. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**
>
> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não anexam informações de plano. O recurso Citrix Virtual Apps and Desktops é para imagens pagas.

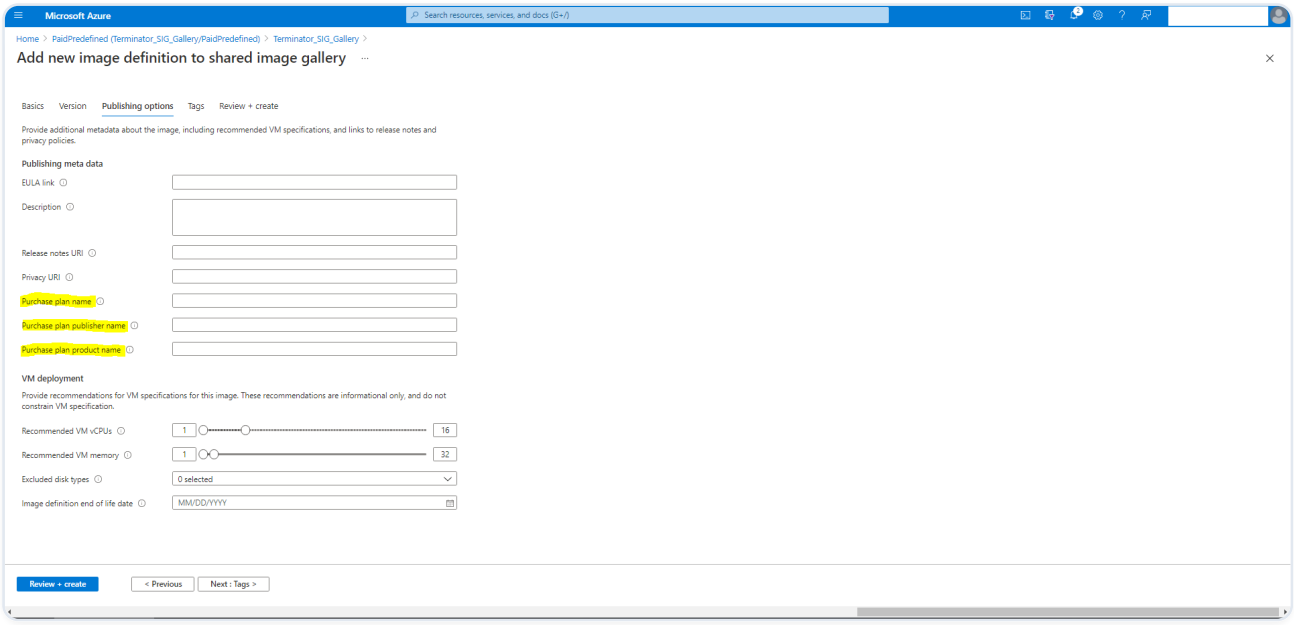
Certifique-se de que a imagem criada na Galeria de Imagens Compartilhadas contenha informações de plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Essas imagens podem ser usadas opcionalmente para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.

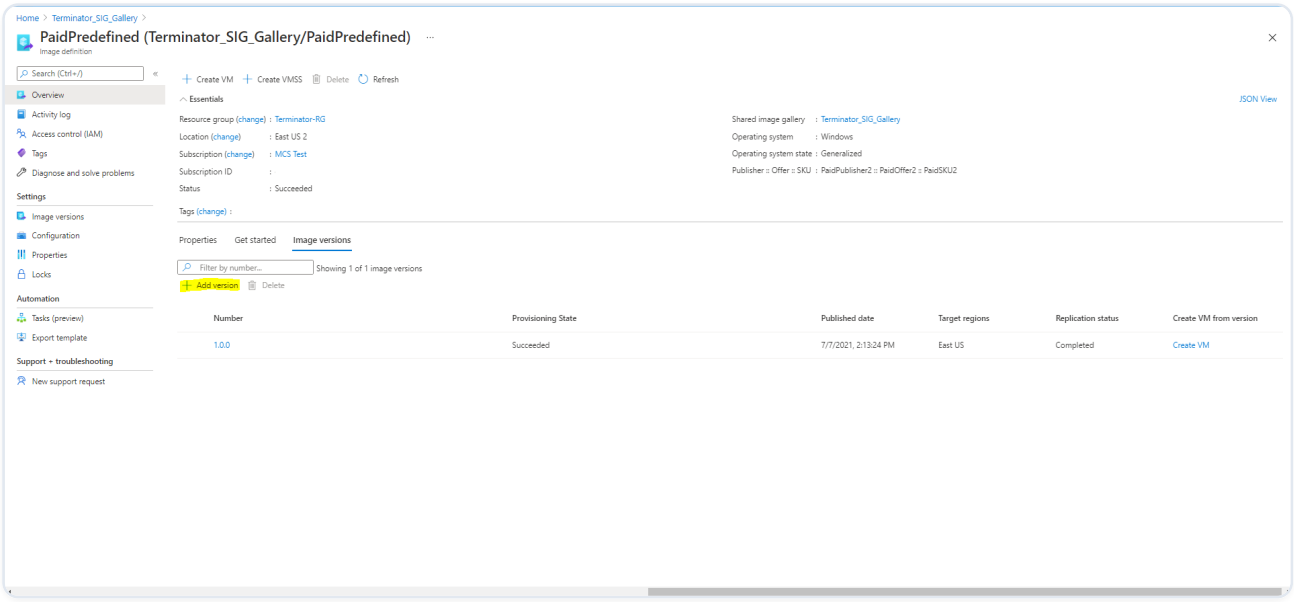


Na página **Opções de publicação**, verifique as informações do plano de compra.

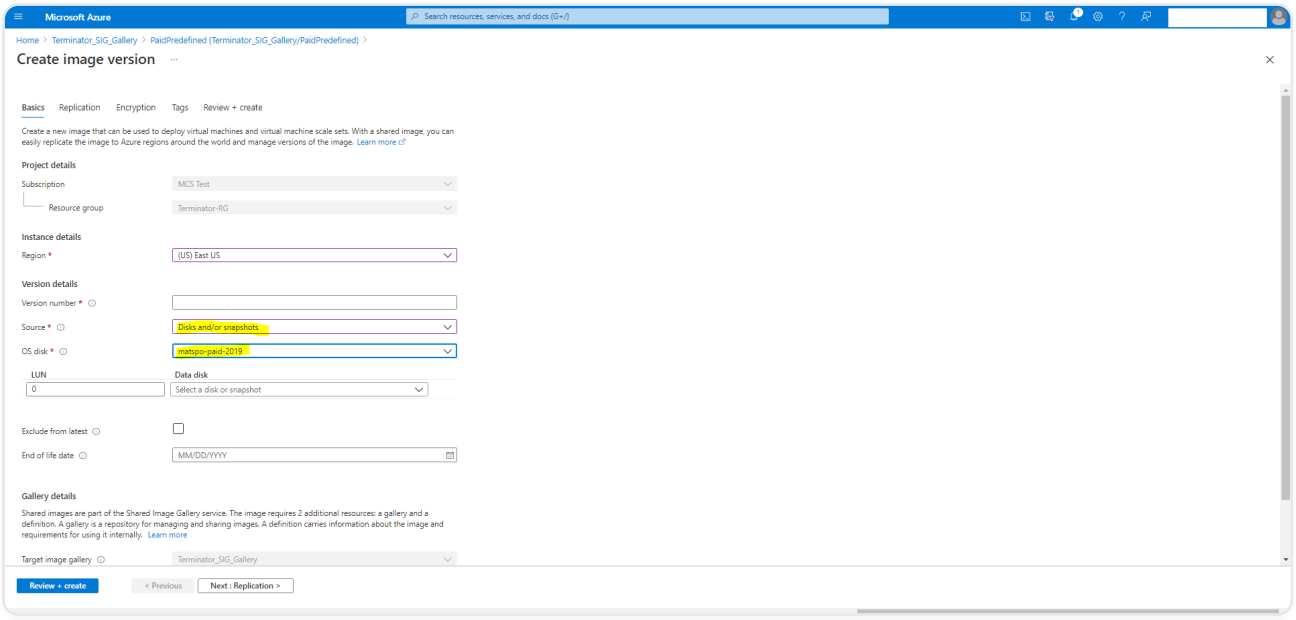
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. A falha ao preencher as informações do plano de compra pode fazer com que o processo de catálogo de máquinas falhe.



Após verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Esta é usada como a imagem mestre. Clique em **Adicionar versão**:



Na seção **Detalhes da versão**, selecione o instantâneo da imagem ou o disco gerenciado como a origem:



Virtualização aninhada

Se você configurar a VM mestre com virtualização aninhada habilitada, todas as VMs no catálogo de máquinas MCS criadas usando essa VM mestre terão a virtualização aninhada habilitada. Esse recurso é aplicável a VMs persistentes e não persistentes. Você pode atualizar um catálogo de máquinas MCS existente e VMs existentes para ter virtualização aninhada por meio da atualização da imagem.

Atualmente, apenas os tamanhos de VM Dv3 e Ev3 suportam virtualização aninhada.

Para obter informações sobre virtualização aninhada, consulte o blog da Microsoft Virtualização Aninhada no Azure.

Criar um catálogo de máquinas usando PowerShell

Esta seção detalha como você pode criar catálogos usando PowerShell:

- Criar um catálogo com disco de cache de write-back não persistente
- Criar um catálogo com disco de cache de write-back persistente
- Melhorar o desempenho de inicialização com MCSIO
- Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell
- Catálogos de máquinas com inicialização confiável
- Usar valores de propriedade de perfil de máquina
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente(#create-a-machine-catalog-with-customer-managed-encryption-key)
- Criar um catálogo de máquinas com criptografia dupla

- Criar um catálogo com discos efêmeros do Azure
- Hosts dedicados do Azure
- Criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure
- Configurar a Galeria de Imagens Compartilhadas
- Provisionar máquinas em Zonas de Disponibilidade especificadas
- Tipos de armazenamento
- Atualizar a configuração do arquivo de paginação
- Criar um catálogo usando VMs Spot do Azure(#create-a-catalog-using-azure-spot-vms)
- Configurar tamanhos de VM de backup
- Copiar tags em todos os recursos
- Provisionar VMs de catálogo com o Agente do Azure Monitor instalado

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 PowerShell `New-ProvScheme CustomProperties`. A propriedade personalizada `UseTempDiskForWBC` indica se você aceita usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como true ao executar `New-ProvScheme` se você quiser usar o disco temporário como disco de cache de write-back. Se esta propriedade não for especificada, o parâmetro será definido como **False** por padrão.

Por exemplo, usando o parâmetro `CustomProperties` para definir `UseTempDiskForWBC` como **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `
```

```
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

Observação:

Depois de confirmar o catálogo de máquinas para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar VHD posteriormente.

Criar um catálogo com disco de cache de write-back persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes de suportar `PersistWBC` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />
```

```
</CustomProperties>
```

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 usando o Web Studio.

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 usando o Web Studio.

Observação:

Se a propriedade `PersistWBC` for omitida, a propriedade assume o valor padrão **false** e o cache de write-back é excluído quando a máquina é desligada usando o Web Studio.

Por exemplo, usando o parâmetro `CustomProperties` para definir `PersistWBC` como true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

Importante:

A propriedade `PersistWBC` só pode ser definida usando o cmdlet PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como true:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache
```

```
-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Melhore o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

Para habilitar este recurso, defina a propriedade personalizada `PersistOSDisk` como `true`. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
```
```

```
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou comandos PowerShell.

Para o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio

Usando comandos do PowerShell:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie ou atualize um catálogo.

- Para criar um catálogo:

  a. Use o comando `New-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

  b. Conclua a criação do catálogo.

- Para atualizar um catálogo, use o comando `Set-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]
```

```
[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

Catálogos de máquinas com inicialização confiável

Para criar com sucesso um catálogo de máquinas com inicialização confiável, use:

- Um perfil de máquina com inicialização confiável
- Um tamanho de VM que suporta inicialização confiável
- Uma versão de VM do Windows que suporta inicialização confiável. Atualmente, Windows 10, Windows 11, Windows Server 2016, 2019 e 2022 suportam inicialização confiável.

Importante:

O MCS suporta a criação de um novo catálogo com VMs com inicialização confiável habilitada. No entanto, para atualizar um catálogo persistente existente e VMs existentes, você deve usar o portal do Azure. Você não pode atualizar a inicialização confiável de um catálogo não persistente. Para obter mais informações, consulte o documento da Microsoft Habilitar inicialização confiável em VMs existentes do Azure.

Para visualizar os itens de inventário da oferta Citrix Virtual Apps and Desktops e determinar se o tamanho da VM suporta inicialização confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
   - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM suporta inicialização confiável.
   - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não suporta inicialização confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que suportam inicialização confiável:

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

A seguir estão os exemplos que descrevem se o tamanho da VM suporta inicialização confiável depois de executar o comando Azure PowerShell.

- *Exemplo 1*: Se a VM do Azure suporta apenas Geração 1, essa VM não suporta inicialização confiável. Portanto, a capacidade `TrustedLaunchDisabled` não é exibida depois de executar o comando Azure PowerShell.
- *Exemplo 2*: Se a VM do Azure suportar apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` for **True**, o tamanho da VM da Geração 2 não é suportado para inicialização confiável.
- *Exemplo 3*: Se a VM do Azure suportar apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` não for exibida após a execução do comando PowerShell, o tamanho da VM da Geração 2 é suportado para inicialização confiável.

Para obter mais informações sobre inicialização confiável para máquinas virtuais do Azure, consulte o documento da Microsoft Inicialização confiável para máquinas virtuais do Azure.

Criar um catálogo de máquinas com inicialização confiável

1. Crie uma imagem mestre habilitada com inicialização confiável. Consulte a documentação da Microsoft Imagens de VM de inicialização confiável.
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de inicialização confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft Deploy a trusted launch VM.
3. Crie um catálogo de máquinas usando o Web Studio ou comandos PowerShell.
    - Se você quiser usar o Web Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Web Studio.
    - Se você quiser usar comandos PowerShell, use o comando `New-ProvScheme` com a VM ou a especificação do modelo como entrada de perfil de máquina. Para a lista completa de comandos para criar um catálogo, consulte Criando um catálogo.

      Exemplo de `New-ProvScheme` com VM como entrada de perfil de máquina:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
hine profile vm.vm>"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

Exemplo de `New-ProvScheme` com especificação de modelo como entrada de perfil de máquina:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

Erros ao criar catálogos de máquinas com inicialização confiável

Você recebe erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com inicialização confiável:

CENÁRIO	ERRO
Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado	`MachineProfileNotSupportedForUnmanagedCatalog`
Se você selecionar um perfil de máquina que suporte inicialização confiável ao criar um catálogo com disco não gerenciado como imagem mestre	`SecurityTypeNotSupportedForUnmanagedDisk`
Se você não selecionar um perfil de máquina ao criar um catálogo gerenciado com uma fonte de imagem mestre com inicialização confiável como tipo de segurança	`MachineProfileNotFoundForTrustedLaunchMasterImage`
Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
Se você selecionar um tamanho de VM que não suporte inicialização confiável, mas usar uma imagem mestre que suporte inicialização confiável ao criar um catálogo	`MachineSizeNotSupportTrustedLaunch`

Usar valores de propriedade do perfil de máquina

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

- Zona de disponibilidade
- ID do Grupo de Host Dedicado
- ID do Conjunto de Criptografia de Disco
- Tipo de SO
- Tipo de licença
- Tipo de armazenamento

Se essas propriedades personalizadas não forem definidas explicitamente, os valores das propriedades serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como perfil da máquina. Além disso, se `ServiceOffering` não for especificado, ele será definido a partir do perfil da máquina.

> **Nota:**
>
> Se algumas das propriedades estiverem ausentes do perfil da máquina e não forem definidas nas propriedades personalizadas, os valores padrão das propriedades serão aplicados onde for cabível.

> A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` têm todas as propriedades definidas ou os valores são derivados do MachineProfile.

- Cenários do New-ProvScheme
  - MachineProfile tem todas as propriedades e CustomProperties não estão definidas. Exemplo:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
    value>"/>
    ```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem apenas LicenseType e OsType.

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">

  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
  value>"/>

  </CustomProperties>
  ```

- Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  As propriedades personalizadas têm prioridade. Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Exemplo:
  - CustomProperties definem LicenseType e StorageAccountType
  - MachineProfile define LicenseType, OsType e Zones

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não é definido. Exemplo:
  - CustomProperties definem StorageType
  - MachineProfile especifica LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- Se o OsType não estiver nem em CustomProperties nem em MachineProfile, então:
  - O valor é lido da imagem mestre.
  - Se a imagem mestre for um disco não gerenciado, o OsType é definido como Windows. Exemplo:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

O valor da imagem mestre é gravado nas propriedades personalizadas, neste caso Linux.

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Cenários de Set-ProvScheme
  - Um catálogo existente com:
    - CustomProperties para `StorageAccountType` e OsType
    - Perfil da Máquina `mpA.vm` que define zonas
  - Atualizações:

- Perfil da Máquina mpB.vm que define StorageAccountType
- Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define LicenseType e OsType

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- Um catálogo existente com:
  - CustomProperties para S`torageAccountType` e OsType
  - Perfil da Máquina `mpA.vm` que define StorageAccountType e LicenseType
- Atualizações:
  - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define StorageAccountType e OsType.

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- Um catálogo existente com:
  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define Zonas
- Atualizações:
  - Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  - `ServiceOffering` não é especificado

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Provisionar VMs de catálogo com o Agente do Azure Monitor instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e agir sobre dados de telemetria de seus ambientes Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos de computação, como máquinas virtuais, e entrega os dados ao Azure Monitor. Atualmente, ele suporta a coleta de Logs de Eventos, Syslog e métricas de desempenho e os envia para as fontes de dados do Azure Monitor Metrics e Azure Monitor Logs.

Para habilitar o monitoramento identificando exclusivamente as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

Requisitos

- Permissões: Certifique-se de ter as permissões mínimas do Azure conforme especificado em Permissões do Azure necessárias e as seguintes permissões para usar o Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regra de Coleta de Dados: Configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar uma DCR, consulte Criar uma regra de coleta de dados. Uma DCR é específica da plataforma (Windows ou Linux). Certifique-se de criar uma

DCR de acordo com a plataforma necessária. O AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e fontes de dados, como Métricas do Azure Monitor e Logs do Azure Monitor.

- Espaço de Trabalho Padrão: Crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um, consulte Criar um espaço de trabalho do Log Analytics. Ao coletar logs e dados, as informações são armazenadas em um espaço de trabalho. Cada um possui 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, configure as fontes de dados e as soluções para armazenar seus dados nele.
- Extensão de monitoramento na lista de permissões: As extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões na lista de permissões definidas pela Citrix. Para visualizar a lista de extensões na lista de permissões, use o comando PoSH, `Get-ProvMetadataConfiguration`.
- Imagem Mestra: A Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso pode levar a arquivos residuais e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para provisionar VMs de catálogo com AMA habilitado:

1. Configurar um modelo de perfil de máquina.
    - Se você quiser usar uma VM como modelo de perfil de máquina:
        a. Crie uma VM no portal do Azure.
        b. Ligue a VM.
        c. Adicione a VM à regra de coleta de dados em **Recursos**. Isso invoca a instalação do agente na VM do modelo.

> **Observação:**
>
> Se você precisar criar um catálogo Linux, configure uma máquina Linux.

    - Se você quiser usar a especificação de modelo como um modelo de perfil de máquina:
        a. Configure uma especificação de modelo.

b. Adicione a seguinte extensão e associação de regra de coleta de dados à especificação de modelo gerada:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",
```

```
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. Crie ou atualize um catálogo de máquinas MCS existente.

   - Para criar um novo catálogo MCS:

     a. Selecione essa VM ou especificação de modelo como um perfil de máquina no Web Studio.

     b. Prossiga 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"
```

- Para atualizar VMs existentes com o modelo de perfil de máquina atualizado:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. Ligue as VMs do catálogo.
4. Vá para o portal do Azure e verifique se a extensão de monitoramento está instalada na VM e se a VM está aparecendo em Recursos da DCR. Após alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

Solução de problemas

Para obter informações sobre as diretrizes de solução de problemas para o Azure Monitor Agent, consulte o seguinte:

- https://learn.microsoft.com/pt-br/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/pt-br/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

As etapas detalhadas sobre como criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente são:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Digite `cd xdhyp:/`.
4. Digite `cd .\HostingUnits\(your hosting unit)`.
5. Digite `cd diskencryptionset.folder`.
6. Insira `dir` para obter a lista dos Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma string de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. Execute o comando New-ProvScheme: Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"
```

```
-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. Conclua a criação do catálogo de máquinas.

Criar um catálogo de máquinas com criptografia dupla

Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e comandos do PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Use o portal do Azure para habilitar a criptografia dupla em repouso para discos gerenciados.
2. Para procurar DiskEncryptionSets disponíveis em sua conexão de hospedagem:
   a. Abra uma janela do **PowerShell**.
   b. Execute os seguintes comandos PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`:
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (ex: azure-leste)
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Você pode usar um ID do `DiskEncryptionSet` para criar ou atualizar um catálogo usando propriedades personalizadas.
3. Se você quiser usar o fluxo de trabalho de perfil de máquina, crie uma VM ou especificação de modelo como entrada de perfil de máquina.
   - Se você quiser usar uma VM como entrada de perfil de máquina:

a. Crie uma VM no Portal do Azure.

b. navegar para **Discos>Gerenciamento de chaves** para criptografar a VM diretamente com qualquer `DiskEncryptionSetID`.

- Se você quiser usar uma especificação de modelo como entrada de perfil de máquina:

a. No modelo, em `properties>storageProfile>osDisk>managedDisk`, adicione o parâmetro `diskEncryptionSet` e adicione o ID do DES de criptografia dupla.

4. Crie o catálogo de máquinas.

- Se estiver usando o Web Studio, faça um dos seguintes, além das etapas em Criar catálogos de máquinas.

  - Se você não usa o fluxo de trabalho baseado em perfil de máquina, na página **Configurações de Disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue criando o catálogo.
  - Se estiver usando o fluxo de trabalho de perfil de máquina, na página **Imagem**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID de conjunto de criptografia de disco em suas propriedades.

  Todas as máquinas criadas no catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

- Se estiver usando comandos do PowerShell, faça um dos seguintes:

  - Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada `DiskEncryptionSetId` no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
```

```
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
```

```
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. Conclua a criação de um catálogo usando o SDK remoto do PowerShell. Para obter informações sobre como criar um catálogo usando o SDK remoto do PowerShell, 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 duplamente pela chave associada ao DES que você selecionou.

Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina).

- Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada DiskEncryptionSetId no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

Após o sucesso, todas as novas VMs que você adicionar ao seu catálogo serão criptografadas duplamente pela chave associada ao DES que você selecionou.

Verificar se o catálogo está criptografado duplamente

- No Web Studio:
  a. navegar para **Catálogos de Máquinas**.
  b. Selecione o catálogo que você deseja verificar. Clique na guia **Propriedades do Modelo** localizada perto da parte inferior da tela.
  c. Em **Detalhes do Azure**, verifique o ID do Conjunto de Criptografia de Disco em **Conjunto de Criptografia de Disco**. Se o ID DES do catálogo estiver em branco, o catálogo não está criptografado.
  d. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.
- Usando o comando PowerShell:
  a. Abra a janela do **PowerShell**.
  b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
  c. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. Recupere a propriedade personalizada ID do DES do catálogo de máquinas. Por exemplo:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

  e. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.

Criar um catálogo com discos efêmeros do Azure

Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **Observação:**

Se a propriedade personalizada `UseEphemeralOsDisk` for definida como **false** ou um valor não for especificado, todos os VDAs provisionados continuarão a usar um disco de SO provisionado.

A seguir, um exemplo de conjunto de propriedades personalizadas a serem usadas no esquema de provisionamento:

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },

            {

                "Name": "SharedImageGalleryReplicaRatio",

                "Value": "40"

            },

            {
```

```
            "Name": "SharedImageGalleryReplicaMaximum",
            "Value": "10"
        },
        {
            "Name": "LicenseType",
            "Value": "Windows_Server"
        },
        {
            "Name": "UseEphemeralOsDisk",
            "Value": "true"
        }
    ],
```

Configurar um disco efêmero para um catálogo

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**.

> **Observação:**
>
> Para usar este recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

Considerações importantes para discos efêmeros

Para provisionar discos de SO efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve suportar discos de SO efêmeros.
- O tamanho do cache ou do disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco do SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também estas questões ao:

- Criar o esquema de provisionamento.
- Modificando o esquema de provisionamento.
- Atualizando a imagem.

Hosts dedicados do Azure

Você pode usar o MCS para provisionar VMs em hosts dedicados do Azure. Antes de provisionar VMs em hosts dedicados do Azure:

- Criar um grupo de hosts.
- Criar hosts nesse grupo de hosts.
- Certifique-se de que há capacidade de host suficiente reservada para a criação de catálogos e máquinas virtuais.

Você pode criar um catálogo de máquinas com locação de host definida através do seguinte script PowerShell:

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade do catálogo e não pode ser alterado depois que o catálogo é criado. A locação dedicada não é atualmente suportada no Azure.
- Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`.
- O posicionamento automático do Azure é necessário. Essa funcionalidade faz uma solicitação para integrar a assinatura associada ao grupo de hosts. Para obter mais informações, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Se o posicionamento automático não estiver habilitado, o MCS gerará um erro durante a criação do catálogo.

Criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure

Ao selecionar uma imagem para usar na criação de um catálogo de máquinas, você pode selecionar imagens que criou na Galeria de Computação do Azure.

Para que essas imagens apareçam, você deve:

1. Configure um site do Citrix Virtual Apps and Desktops.
2. Conecte-se ao Azure Resource Manager.
3. No portal do Azure, crie um grupo de recursos. Para obter detalhes, consulte Criar uma Galeria de Computação do Azure usando o portal.
4. No grupo de recursos, crie uma Galeria de Computação do Azure.
5. Na Galeria de Computação do Azure, crie uma definição de imagem.

6. Na definição de imagem, crie uma versão de imagem.

Use os seguintes comandos do PowerShell para criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. Selecione uma definição de imagem e, em seguida, liste todas as versões de imagem dessa definição de imagem.

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

   Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurar a Galeria de Imagens Compartilhadas

Use o comando `New-ProvScheme` para criar um esquema de provisionamento com suporte à Galeria de Imagens Compartilhadas. 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 oferecer suporte ao recurso Galeria de Imagens Compartilhadas:

`UseSharedImageGallery`

- Define se a Galeria de Imagens Compartilhadas deve ser usada para armazenar as imagens publicadas. Se definido como **True**, a imagem é armazenada como uma imagem da Galeria de Imagens Compartilhadas; caso contrário, a imagem é armazenada como um instantâneo.
- Os valores válidos são **True** e **False**.
- Se a propriedade não for definida, o valor padrão é **False**.

`SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas da versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não for definida, os valores padrão são usados. O valor padrão para discos de SO persistentes é 1000 e o valor padrão para discos de SO não persistentes é 40.

`SharedImageGalleryReplicaMaximum`

- Define o número máximo de réplicas para cada versão da imagem da galeria.
- Se a propriedade não for definida, o valor padrão é 100.
- Se a propriedade não for definida, o valor padrão é 100.

> **Dica:**

> Ao usar a Galeria de Imagens Compartilhadas para armazenar uma imagem publicada para catálogos provisionados por MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na taxa de réplica e no máximo de réplicas. A contagem de réplicas é calculada dividindo 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, 81+ têm 5 réplicas.

Caso de uso: Atualizando a proporção e o máximo de réplicas da Galeria de Imagens Compartilhadas

O catálogo de máquinas existente usa a Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para atualizar as propriedades personalizadas para todas as máquinas existentes no catálogo e quaisquer máquinas futuras:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

Caso de Uso: Convertendo um catálogo de instantâneos para um catálogo da Galeria de Imagens Compartilhadas

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
```

```
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

Dica:

Os parâmetros `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` não são obrigatórios. Após a conclusão do comando `Set-ProvScheme`, a imagem da Galeria de Imagens Compartilhadas ainda não foi criada. Uma vez que o catálogo é configurado para usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. Reiniciar as máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Imagens Compartilhadas e todas as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente em algumas horas.

Caso de Uso: Convertendo um Catálogo da Galeria de Imagens Compartilhadas para um catálogo de instantâneos

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

Dica:

Ao contrário da atualização de um instantâneo para um catálogo da Galeria de Imagens Compartilhadas, os dados personalizados para cada máquina ainda não são atualizados para refletir as novas propriedades personalizadas. Execute o seguinte comando para ver as propriedades personalizadas originais da Galeria de Imagens Compartilhadas: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Após a conclusão do comando `Set-ProvScheme`, o instantâneo da imagem ainda não foi criado. Uma vez que o catálogo é configurado para não usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada como um instantâneo. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o instantâneo e todas as máquinas recém-provisionadas são criadas a partir do instantâneo. Reiniciar as máquinas as atualiza, momento em que os dados personalizados da máquina são atualizados para refletir que `UseSharedImageGallery` está definido como **False**. Os ativos antigos da Galeria de Imagens Compartilhadas (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 Azure. Você pode conseguir isso usando o PowerShell.

Nota:

Se nenhuma zona for especificada, o MCS permite que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribui aleatoriamente as máquinas entre elas.

Configurar Zonas de Disponibilidade via PowerShell

Usando o PowerShell, você pode visualizar os itens de inventário de oferta usando `Get-Item`. Por exemplo, para visualizar a oferta de serviço `Standard_B1ls` da *região Leste dos EUA*:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

Para visualizar as zonas, use o parâmetro `AdditionalData` para o item:

`$serviceOffering.AdditionalData`

Se as Zonas de Disponibilidade não forem especificadas, não haverá alteração na forma como as máquinas são provisionadas.

Para configurar Zonas de Disponibilidade via PowerShell, use a propriedade personalizada **Zones** disponível com a operação `New-ProvScheme`. A propriedade **Zones** define uma lista de Zonas de Disponibilidade para provisionar máquinas. Essas zonas podem incluir uma ou mais Zonas de Disponibilidade. Por exemplo, `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` para as Zonas 1 e 3.

Use o comando `Set-ProvScheme` para atualizar as zonas de um esquema de provisionamento.

Se uma zona inválida for fornecida, o esquema de provisionamento não será atualizado e uma mensagem de erro aparecerá fornecendo instruções sobre como corrigir o comando inválido.

> **Dica:**
>
> Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro relevante aparecerá.

Tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes Azure que usam MCS. Para VMs de destino, o MCS suporta:

- Disco do SO: SSD premium, SSD ou HDD
- Disco de cache de write-back: SSD premium, SSD ou HDD

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM suporta o tipo de armazenamento selecionado.
- Se sua configuração usa um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

> **Dica:**
>
> `StorageType` é configurado para um tipo de SO e conta de armazenamento. `WBCDiskStorageType` é configurado para o tipo de armazenamento de cache de write-

> back. Para um catálogo normal, `StorageType` é necessário. Se `WBCDiskStorageType` não estiver configurado, `StorageType` é usado como padrão para `WBCDiskStorageType`.

> Se WBCDiskStorageType não estiver configurado, então StorageType é usado como padrão para WBCDiskStorageType

Configurar tipos de armazenamento

Para configurar tipos de armazenamento para VM, use o parâmetro `StorageType` em `New-ProvScheme`. Defina o valor do parâmetro `StorageType` para um dos tipos de armazenamento suportados.

A seguir, um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

Habilitar armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica seu disco gerenciado do Azure de forma síncrona em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser configurado usando propriedades personalizadas existentes ou através do modelo **MachineProfile**. O armazenamento ZRS também é suportado com o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow`

e `-DurationInMinutes -1`, e você pode alterar uma máquina existente de armazenamento LRS para ZRS.

Limitações:

- Suportado apenas para discos gerenciados
- Suportado apenas com unidades de estado sólido (SSD) premium e padrão
- Não compatível com `StorageTypeAtShutdown`
- Disponível apenas em certas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em escala. Portanto, para a primeira inicialização, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

DEFINIR O ARMAZENAMENTO COM REDUNDÂNCIA DE ZONA COMO O TIPO DE ARMAZENAMENTO DE DISCO

Você pode selecionar o armazenamento com redundância de zona durante a criação inicial do catálogo, ou pode atualizar seu tipo de armazenamento em um catálogo existente.

SELECIONAR ARMAZENAMENTO COM REDUNDÂNCIA DE ZONA USANDO COMANDOS DO POWERSHELL

Ao criar um novo catálogo no Azure usando o comando PowerShell `New-ProvScheme`, use `Standard_ZRS` como valor em `StorageAccountType`. Por exemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso de ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: A propriedade personalizada StorageTypeAtShutdown não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta exceção ocorre se você tentar usar o Armazenamento ZRS em uma Região do Azure que não oferece suporte a ZRS
- **ZrsRequiresManagedDisks**: Você pode usar o armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento de disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Observação:**
>
> Durante a criação do catálogo, o disco do SO do perfil da máquina `StorageType` é usado se as propriedades personalizadas não estiverem definidas.

Capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina ao criar um catálogo de máquinas, atualizar um catálogo de máquinas existente e atualizar VMs existentes.

Você pode criar uma VM ou especificação de modelo como uma fonte de perfil de máquina.

Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação do modelo.
    - Conta de armazenamento
    - Espaço de trabalho do Log Analytics
    - Namespace do hub de eventos com o preço da camada padrão
2. Criar fonte de perfil de máquina.
3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize VMs existentes.

Configurar IDs necessárias no Azure

Configure um dos seguintes no Azure:

- Conta de armazenamento
- Espaço de trabalho do Log Analytics
- Namespace do Hub de Eventos com o preço da camada Standard

CONFIGURAR UMA CONTA DE ARMAZENAMENTO

Crie uma conta de armazenamento padrão no Azure. Na especificação do modelo, forneça o resourceId completo para a conta de armazenamento como o `storageAccountId`.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, os dados podem ser encontrados no contêiner `insights-metrics-pt1m`.

CONFIGURAR UM ESPAÇO DE TRABALHO DO LOG ANALYTICS

Crie um espaço de trabalho do Log Analytics. Na especificação do modelo, forneça o resourceId completo para o espaço de trabalho do Log Analytics como o workspaceId.

Depois que as VMs são configuradas para registrar dados no espaço de trabalho, os dados podem ser consultados em Logs no Azure. Você pode executar o seguinte comando no Azure em Logs para mostrar uma contagem de todas as métricas registradas por um recurso:

```
AzureMetrics | summarize Count=count() by ResourceId
```

CONFIGURAR UM HUB DE EVENTOS

Faça o seguinte para configurar um hub de eventos no portal do Azure:

1. Crie um namespace do hub de eventos com o preço da camada padrão.
2. Crie um hub de eventos sob o namespace.
3. navegar para **Captura** sob o hub de eventos. Ative o botão para capturar com o tipo de saída Avro.
4. Crie um novo contêiner em uma conta de armazenamento existente para capturar os logs.
5. Na especificação do modelo, especifique o `eventHubAuthorizationRuleId` no seguinte formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique o nome do hub de eventos.

Depois que as VMs são configuradas para registrar dados no hub de eventos, os dados são capturados no contêiner de armazenamento configurado.

Criar uma origem de perfil de máquina

Você pode criar uma VM ou especificação de modelo como uma origem de perfil de máquina.

CRIAR UM PERFIL DE MÁQUINA BASEADO EM VM COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você quiser criar uma VM como seu perfil de máquina, então primeiro configure as configurações de diagnóstico na própria VM do modelo. Você pode consultar as instruções detalhadas fornecidas na documentação da Microsoft Configurações de diagnóstico no Azure Monitor.

Você pode executar os seguintes comandos para verificar se agora há configurações de diagnóstico associadas à VM ou NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

CRIAR UM PERFIL DE MÁQUINA BASEADO EM ESPECIFICAÇÃO DE MODELO COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você quiser usar uma VM que já tenha as configurações de diagnóstico habilitadas e exportá-la para uma especificação de modelo ARM, essas configurações não serão incluídas automaticamente no modelo. Você deve adicionar ou modificar manualmente as configurações de diagnóstico dentro do modelo ARM.

No entanto, se você quiser uma VM como seu perfil de máquina, o MCS garante que as configurações de diagnóstico críticas sejam capturadas com precisão e aplicadas aos recursos dentro do seu catálogo MCS.

1. Crie uma especificação de modelo padrão que defina uma VM e NIC(s).
2. Adicione recursos adicionais para implantar as configurações de diagnóstico de acordo com a especificação: Microsoft.Insights diagnosticSettings. Para o escopo, faça referência a uma VM ou NIC que esteja no modelo pelo nome com um ID parcial. Por exemplo, para criar configurações de diagnóstico anexadas a uma VM chamada test-VM na especificação do modelo, especifique o escopo como:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use a especificação do modelo como uma origem de perfil de máquina.

Criar ou atualizar um catálogo com configurações de diagnóstico

Depois de criar uma origem de perfil de máquina, agora você pode criar um catálogo de máquinas usando o comando `New-ProvScheme`, atualizar um catálogo de máquinas existente usando o comando `Set-ProvScheme` e atualizar VMs existentes usando o comando `Request-ProvVMUpdate`.

Determinação do local do arquivo de paginação

O local do arquivo de paginação é determinado de acordo com o seguinte cenário:

Nota:

O local padrão do arquivo de paginação é o disco do SO.

CENÁRIO	LOCAL
A configuração do arquivo de paginação é especificada nas propriedades personalizadas	Conforme especificado nas propriedades personalizadas
Disco de SO efêmero ou hibernação está habilitado	Disco do SO
A VM tem um disco temporário	Disco temporário
E/S do MCS está habilitada	Disco WBC

Cenários de configuração do arquivo de paginação

A tabela a seguir descreve alguns dos possíveis cenários de configuração do arquivo de paginação durante a preparação da imagem e a atualização do esquema de provisionamento:

DURANTE	CENÁRIO	RESULTADO
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco temporário, enquanto o tamanho da VM que você especifica no	O arquivo de paginação é colocado no SO

DURANTE	CENÁRIO	RESULTADO
	esquema de provisionamento não tem disco temporário	
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco do SO, enquanto o tamanho da VM que você especifica no esquema de provisionamento tem um disco temporário	O arquivo de paginação é colocado no disco temporário
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco temporário e habilita o disco do SO efêmero no esquema de provisionamento	O arquivo de paginação é colocado no disco do SO
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento quando a versão do VDA é anterior a 2311	Modifica a configuração do arquivo de paginação com um aviso
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento quando a versão do VDA é 2311 ou posterior	Determina o local do arquivo de paginação conforme Determinação do local do arquivo de paginação

Especificar configuração do arquivo de paginação

Usando comandos PowerShell, você pode especificar as configurações do arquivo de paginação, incluindo o local e o tamanho. Isso substitui as configurações do arquivo de paginação determinadas pelo MCS conforme Determinação do local do arquivo de paginação. Você pode fazer isso executando o seguinte comando `New-ProvScheme` durante a criação do catálogo de máquinas.

Considerações importantes

Considere o seguinte antes de prosseguir com a criação do catálogo:

- Você deve fornecer todas as propriedades personalizadas ('PageFileDiskDriveLetterOverride', 'InitialPageFileSizeInMB' e 'MaxPageFileSizeInMB') no comando `New-ProvScheme` ou nenhuma delas.
- Este recurso não é suportado através do Citrix Studio.
- O tamanho inicial do arquivo de paginação deve estar entre 16 MB e 16777216 MB.
- O tamanho máximo do arquivo de paginação deve ser maior ou igual ao tamanho inicial do arquivo de paginação e menor que 16777216 MB.
- Você pode definir o tamanho inicial e o tamanho máximo do arquivo de paginação como zero ao mesmo tempo.

Nota:

Você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas de um catálogo existente, sem atualizar a imagem mestre. Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell. Para obter mais informações, consulte Modificar configurações do arquivo de paginação.

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
```

```
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

Modificar configurações do arquivo de paginação

Você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas a um catálogo existente sem atualizar a imagem mestre. Atualmente, este recurso é aplicável apenas a ambientes Azure.

Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell.

A seguir estão as várias configurações de arquivo de paginação que você pode modificar no ambiente Azure:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`

- `MaxPageFileSizeInMB`

Modificar as configurações do arquivo de paginação de um catálogo existente

Para modificar as configurações do arquivo de paginação de um catálogo de máquinas existente, execute o comando `Set-ProvScheme`. Neste caso, as atualizações são aplicadas apenas às novas VMs adicionadas ao catálogo. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

Nota:

> Se você habilitar o cache de write-back e tentar definir o `PageFileDiskDriveLetterOverride` para `C:` usando o comando PowerShell, o driver de E/S do MCS redireciona automaticamente o arquivo de paginação para uma unidade de disco correta e não `C:`.

Criar um catálogo usando VMs Spot do Azure

As VMs Spot do Azure permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa de custos. No entanto, a capacidade de alocar uma VM Spot do Azure depende da capacidade e dos preços atuais. Portanto, o Azure pode despejar sua VM em execução, falhar ao criar a VM ou falhar ao ligar a VM de acordo com a Política de despejo. Portanto, as VMs Spot do Azure são boas para algumas aplicações e desktops não críticos. Para obter mais informações, consulte Usar Máquinas Virtuais Spot do Azure.

Limitações

- Nem todos os tamanhos de VM são suportados para VMs Spot do Azure. Para obter mais informações, consulte Limitações.

  Você pode executar o seguinte comando PowerShell para verificar se um tamanho de VM suporta VMs Spot ou não. Se um tamanho de VM suportar VM Spot, então `SupportsSpotVM` é **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- Atualmente, as VMs Spot do Azure não suportam hibernação.

Requisito

Ao criar a origem do perfil da máquina (VM ou especificação de modelo) para o catálogo de VMs Spot do Azure, você deve selecionar Instância Spot do Azure (se estiver usando VM) ou definir `priority` como `Spot` (se estiver usando especificação de modelo).

Etapas para criar um catálogo usando VMs Spot do Azure

1. Crie uma origem de perfil de máquina (VM ou modelo de inicialização).
   - Para criar uma VM usando o portal do Azure, consulte Implantar Máquinas Virtuais Spot do Azure usando o portal do Azure.

- Para criar uma especificação de modelo, adicione as seguintes propriedades em **resources > type: Microsoft.Compute/virtualMachines > properties** na especificação de modelo. Por exemplo:

```
"priority": "Spot",

"evictionPolicy": "Deallocate",

"billingProfile": {

"maxPrice": 0.01

}
```

Nota:

- A política de remoção pode ser **Deallocate** ou **Delete**.
  - Para VMs não persistentes, o MCS sempre define a política de remoção como **Delete**. Se a VM for removida, ela será excluída junto com quaisquer discos não persistentes (por exemplo, disco do SO). Quaisquer discos persistentes (por exemplo, disco de identidade) não são excluídos. No entanto, um disco do SO é persistente se o tipo de catálogo for persistente ou se a propriedade personalizada `PersistOsDisk` for definida como True. Da mesma forma, um disco WBC é persistente se a propriedade personalizada `PersistWbc` for definida como **True**.
  - Para VMs persistentes, o MCS sempre define a política de remoção como Deallocate. Se a VM for removida, ela será desalocada. Nenhuma alteração é feita nos discos.
- O preço máximo é o preço que você está disposto a pagar por hora. Se você estiver usando **Somente Capacidade**, então este é **-1**. O preço máximo pode ser apenas nulo, -1 ou um decimal maior que zero. Para obter mais informações, consulte Preços.

2. Você pode executar o seguinte comando PowerShell para verificar se um perfil de máquina está habilitado para Azure Spot VM ou não. Se o parâmetro `SpotEnabled` for **True** e

`SpotEvictionPolicy` estiver definido como **Deallocate** ou **Delete**, então o perfil de máquina estará habilitado para Azure Spot VM. Por exemplo,

- Se a origem do perfil da máquina for uma VM, execute o seguinte comando:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
delete.vm"). AdditionalData
```

- Se a origem do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
templatespec.templatespec\14.0.0-spot-
delete.templatespecversion").AdditionalData
```

3. Crie um catálogo de máquinas usando um perfil de máquina com o comando PowerShell `New-ProvScheme`.

Você pode atualizar um catálogo usando o comando `Set-ProvScheme`. Você também pode atualizar VMs existentes usando o comando PowerShell `Set-ProvVmUpdateTimeWindow`. O perfil da máquina é atualizado no próximo ligar.

Remoções em uma VM Spot do Azure em execução

Se a capacidade de computação estiver indisponível ou o preço por hora for superior ao preço máximo configurado, o Azure removerá uma VM Spot em execução. Por padrão, você não é notificado de uma remoção. A VM simplesmente congela e é removida. A Microsoft recomenda usar Eventos Agendados para monitorar remoções. Consulte Monitorar continuamente para remoção. Você também pode executar scripts de dentro de uma VM para receber uma notificação antes da remoção. Por exemplo, a Microsoft tem um script de sondagem em Python ScheduledEvents.cs.

Solução de problemas

- Você pode ver as propriedades da VM Spot em customMachineData da VM provisionada usando o comando `Get-ProvVM`. Se o campo de prioridade estiver definido como **Spot**, então o Spot está em uso.
- Você pode verificar se uma VM está usando Spot no Portal do Azure:

a. Encontre a VM no Portal do Azure.
b. Vá para a página **Visão geral**.
c. Role para baixo até o final e localize a seção **Azure Spot**.
    - Se o Spot não estiver em uso, este campo estará vazio.
    - Se o Spot estiver em uso, os campos **Azure Spot** e **Política de remoção do Azure Spot** estarão definidos.

1. Você pode verificar o perfil de faturamento ou o preço máximo por hora para a VM na página de Configuração.

Configurar tamanhos de VM de backup

As nuvens públicas podem, às vezes, ficar sem capacidade para um tamanho de VM específico. Além disso, se você usar VMs Spot do Azure, as VMs serão despejadas a qualquer momento com base nas necessidades de capacidade do Azure. Em tal caso de capacidade insuficiente no Azure ou falha na inicialização de uma VM Spot, o MCS recorre aos tamanhos de VM de backup. Você pode fornecer uma lista de tamanhos de VM de backup usando uma propriedade personalizada `BackupVmConfiguration` ao criar ou atualizar um catálogo de máquinas MCS. O MCS tenta recorrer aos tamanhos de VM de backup na ordem fornecida por você na lista.

Quando o MCS usa uma configuração de backup específica para a VM, ele continua a usar essa configuração até o próximo desligamento. Na próxima inicialização, o MCS tenta inicializar a configuração primária da VM. Em caso de falha, o MCS tenta novamente inicializar uma configuração de tamanho de VM de backup conforme a lista.

Este recurso é compatível com:

- um catálogo que usa um perfil de máquina
- catálogos de máquinas MCS persistentes e não persistentes
- ambientes Azure atualmente

Considerações importantes

- Você pode fornecer mais de um tamanho de VM de backup na lista.
- A lista deve ser única.
- Você pode adicionar a propriedade de tipo de instância para cada uma das VMs na lista. O tipo é **Spot** ou **Regular**. Se o tipo não for especificado, o MCS considera a VM como **Regular**.

- Você pode alterar a lista de tamanhos de VM de backup de um catálogo existente usando os comandos PowerShell `Set-ProvScheme`.
- Você pode atualizar as VMs existentes criadas a partir do esquema de provisionamento associado ao catálogo usando o comando `Set-ProvVMUpdateTimeWindow`.
- Você pode configurar a lista de tamanho de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Se o comando `Set-ProvVm` for usado em uma VM, a VM continuará a usar a lista de tamanho de VM de backup definida nessa VM específica, mesmo que a lista no esquema de provisionamento seja atualizada posteriormente. Você pode usar `Set-ProvVM` com `-RevertToProvSchemeConfiguration` para fazer com que a VM use a lista de backup no esquema de provisionamento.

Criar um catálogo com tamanhos de VM de backup

> **Nota:**
>
> Para resolver o problema de congelamento da interface do usuário do Studio, substitua todas as aspas simples por `"` ao executar os comandos do PowerShell.

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
4. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
5. Crie um esquema de provisionamento com o perfil da máquina. Consulte Como configurar a configuração de backup.
6. Atualize o BrokerCatalog com o Id exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

Atualizar um catálogo existente

Você pode atualizar um esquema de provisionamento usando o comando `Set-ProvScheme`. Consulte Como configurar a configuração de backup.

Atualizar VMs existentes

Você pode atualizar VMs existentes em um catálogo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`. O comando atualiza as VMs criadas a partir do esquema de provisionamento associado ao catálogo no próximo ligar dentro da janela de tempo fornecida. Por exemplo:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Observação:**
>
> `StartsNow` indica a hora de início agendada. `DurationInMinutes` é a janela de tempo do agendamento.

> Você pode configurar a lista de tamanho de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Por exemplo:

1. Execute o comando `Set-ProvVM` para configurar a lista de tamanhos de VM de backup para uma VM MCS existente selecionada. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. Execute o comando `Set-ProvVMUpdateTimeWindow` para aplicar as atualizações. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

Copiar tags em todos os recursos

Você pode copiar tags especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do SO, disco de identidade e disco de cache de write-back) de uma nova VM ou de uma VM existente em um catálogo de máquinas. A origem do perfil da máquina pode ser uma VM ou uma especificação de modelo ARM.

Nota:

Você deve adicionar a política nas tags (consulte Atribuir definições de política para conformidade de tags) ou adicionar as tags em uma origem de perfil de máquina para reter as tags nos recursos.

Pré-requisitos

Crie a origem do perfil da máquina (VM ou especificação de modelo ARM) para ter tags na VM, discos e NICs dessa VM.

- Se você deseja ter uma VM como entrada de perfil de máquina, aplique tags na VM e em todos os recursos no portal do Azure. Consulte Aplicar tags com o portal do Azure.
- Se você deseja ter uma especificação de modelo ARM como entrada de perfil de máquina, adicione o seguinte bloco de tags em cada recurso.

```
 "tags": {

"TagC": "Value3"

},
```

Nota:

Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

Copiar tags para os recursos de uma VM em um novo catálogo de máquinas

1. Crie um catálogo não persistente ou persistente com uma VM ou especificação de modelo ARM como entrada de perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

Nota:

Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs que você deseja que as VMs usem.

Modificar tags nos recursos de uma VM existente

1. Crie um perfil de máquina com as tags em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. Desligue a VM na qual você deseja aplicar as atualizações.

4. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. Ligue a VM.
6. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes.

Nota:

Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs fornecidas no `Set-ProvScheme`.

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft Azure

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure Resource Manager
- Criar catálogos de máquinas

Criar um catálogo do Microsoft System Center Virtual Machine Manager

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

Observação:

Antes de criar um catálogo VMM, você precisa concluir a criação de uma conexão com o VMM. Consulte Conexão com o Microsoft System Center Virtual Machine Manager.

Criar uma VM mestre

1. Instale um VDA na VM mestre e selecione a opção para otimizar a área de trabalho para melhorar o desempenho.
2. Tire um instantâneo da VM mestre para usar como backup.
3. Crie áreas de trabalho virtuais.

MCS em compartilhamentos de arquivos SMB 3

Para catálogos de máquinas criados com MCS em compartilhamentos de arquivos SMB 3 para armazenamento de VM, certifique-se de que as credenciais atendam aos seguintes requisitos. Esses requisitos garantem que as chamadas da Biblioteca de Comunicações do Hypervisor (HCL) do Controller se conectem com sucesso ao armazenamento SMB:

- As credenciais de usuário do VMM devem incluir acesso total de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante eventos do ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Ao usar o armazenamento SMB, habilite o Provedor de Suporte de Segurança de Credencial de Autenticação (CredSSP) do Controller para máquinas Hyper-V individuais. Use este processo para VMM 2012 SP1 com Hyper-V no Windows Server 2012. Para obter mais informações, consulte CTX137465.

A HCL usa `CredSSP` para abrir uma conexão com a máquina Hyper-V. Esse recurso passa credenciais de usuário criptografadas por Kerberos para a máquina Hyper-V. Os comandos do **PowerShell** na sessão na máquina Hyper-V remota são executados com as credenciais fornecidas. Neste caso, as credenciais do usuário VMM, para que os comandos de comunicação para o armazenamento funcionem corretamente.

As seguintes tarefas usam scripts PowerShell que se originam na HCL e são então enviados para a máquina Hyper-V para atuar no armazenamento SMB 3.0.

- **Consolidar imagem mestre**: Uma imagem mestre cria um esquema de provisionamento MCS (catálogo de máquinas). Ela clona e nivela a VM mestre pronta para criar VMs a partir do novo disco criado (e remove a dependência da VM mestre original).

  ConvertVirtualHardDisk no namespace root\\virtualization\\v2

  Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **Criar disco de diferença:** Cria um disco de diferença a partir da imagem mestre gerada pela consolidação da imagem mestre. O disco de diferença é então anexado a uma nova VM.

  CreateVirtualHardDisk no namespace root\\virtualization\\v2

  Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **Carregar discos de identidade:** A HCL não pode carregar diretamente o disco de identidade para o armazenamento SMB. Portanto, a máquina Hyper-V deve carregar e copiar o disco de identidade para o armazenamento. Como a máquina Hyper-V não pode ler o disco do Controller, a HCL deve primeiro copiar o disco de identidade através da máquina Hyper-V da seguinte forma.

  a. O HCL carrega a Identidade para a máquina Hyper-V através do compartilhamento do administrador.
  b. A máquina Hyper-V copia o disco para o armazenamento SMB através de um script PowerShell executado na sessão remota do PowerShell. Uma pasta é criada na máquina Hyper-V e as permissões nessa pasta são bloqueadas apenas para o usuário VMM (através da conexão remota do PowerShell).
  c. O HCL exclui o arquivo do compartilhamento do administrador.
  d. Quando a HCL termina de carregar o disco de identidade para a máquina Hyper-V, a sessão remota do PowerShell copia os discos de identidade para o armazenamento SMB. Em seguida, ela os exclui da máquina Hyper-V.

  A pasta do disco de identidade é recriada se for excluída para que esteja disponível para reutilização.

- **Baixar discos de identidade:** Assim como nos uploads, os discos de identidade passam pela máquina Hyper-V para a HCL. O processo a seguir cria uma pasta que tem apenas permissões de usuário VMM no servidor Hyper-V, caso ela não exista.

  a. A máquina Hyper-V copia o disco do armazenamento SMB para o armazenamento local do Hyper-V através de um script PowerShell. Este script é executado na sessão remota do PowerShell V3.

  b. O HCL lê o disco do compartilhamento do administrador da máquina Hyper-V para a memória.

  c. O HCL exclui o arquivo do compartilhamento do administrador.

Criar catálogo com um perfil de máquina

Você pode usar um perfil de máquina para criar e atualizar um catálogo de máquinas MCS em ambientes do System Center Virtual Machine Manager (SCVMM). Você pode habilitar o vTPM. Você também pode adicionar tags personalizadas de uma VM de perfil de máquina às VMs provisionadas.

Considerações importantes

- A imagem mestre só pode ser um instantâneo e não uma VM.
- Você só pode usar a VM como a origem do perfil de máquina.
- Você pode configurar o VTPM a partir do console do Hyper-V e não a partir do console do SCVMM.
- Se a imagem mestre tiver o vTPM habilitado, você deverá habilitar o vTPM na origem do perfil de máquina.
- O vTPM é suportado apenas em máquinas de Geração 2.
- Os seguintes parâmetros sobrescrevem os valores capturados em um perfil de máquina se fornecidos separadamente:
  - VMCpuCount
  - VMMemoryMB
  - Armazenamento em disco
- As tags personalizadas são herdadas apenas do perfil da máquina e não da imagem mestre. A tag `CitrixProvisioningSchemeId` é adicionada por padrão à VM. Se você não quiser incluir a tag `CitrixProvisioningSchemeId`, adicione o parâmetro `-NoVmTagging` ao criar uma unidade de hospedagem. Exemplo:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- Você pode atualizar um catálogo existente usando o comando `Set-ProvScheme`.

Criar um catálogo de máquinas usando um perfil de máquina

1. Crie uma VM para ser uma fonte de perfil de máquina. Para obter mais informações, consulte Provisionar máquinas virtuais na malha VMM. Você não pode alterar a **Geração** depois de selecionada. Você pode fazer o seguinte no SCVMM:
    - Para habilitar o vTPM:
        a. Depois de criar a VM, faça login no host Hyper-V e encontre sua VM em **Gerenciador do Hyper-V**.
        b. Clique com o botão direito do mouse na VM e vá para **Configurações**.
        c. Em **Segurança**, selecione a caixa de seleção **Habilitar Módulo de Plataforma Confiável**.
2. Abra uma janela do **PowerShell**.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
5. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
6. Crie um esquema de provisionamento com o perfil da máquina. Por exemplo:
```

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. Atualiza o catálogo do Broker com o ID exclusivo do esquema de provisionamento.
8. Crie e adicione VMs ao catálogo.

Atualizar um catálogo existente

Você pode atualizar um catálogo existente usando o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

Remover uma VM

Você pode optar por remover uma VM de um catálogo, mas não excluir a VM do SCVMM. Neste caso, a tag `CitrixProvisioningSchemeId` é removida apenas da VM. As tags personalizadas não são excluídas da VM. Você pode remover uma VM usando o Web Studio ou comandos do PowerShell.

REMOVER UMA VM USANDO O WEB STUDIO

1. Selecione e clique com o botão direito na VM.
2. Clique em **Excluir**.
3. Selecione **Remover as máquinas virtuais do catálogo, mas não excluir as máquinas virtuais**.

USANDO COMANDOS POWERSHELL

`Remove-ProvVM` com o parâmetro `ForgetVM`. Para obter mais informações, consulte:

- Remover tags
- Excluir máquinas sem acesso ao hypervisor

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega

- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas

Criar um catálogo Nutanix

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização Nutanix.

> **Nota:**
>
> Antes de criar um catálogo Nutanix, você precisa concluir a criação de uma conexão com o Nutanix. Consulte Conexão com Nutanix.

Criar um catálogo de máquinas usando um snapshot do Nutanix

O snapshot selecionado é o modelo usado para criar as VMs no catálogo. Antes de criar o catálogo, crie imagens e snapshots no Nutanix. Para obter mais informações, consulte a documentação do Nutanix.

No assistente de criação de catálogo:

- As páginas **Sistema Operacional** e **Gerenciamento de Máquinas** não contêm informações específicas do Nutanix.
- A página **Container** ou **Cluster and Container** é exclusiva do Nutanix.

  Se você implantar máquinas usando o Nutanix AHV XI como recursos, verá a página **Contêiner**. 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 e Contêiner**. Selecione qual cluster usar para a implantação de VMs e, em seguida, um contêiner.

- Na página **Imagem**, selecione o snapshot da imagem. Os nomes dos snapshots do Acropolis devem ser prefixados com "XD_" para serem usados no Citrix Virtual Apps and Desktops. Use o console do Acropolis para renomear seus snapshots, se necessário. Se você renomear os snapshots, reinicie o assistente de criação de catálogo para ver uma lista atualizada.
- Na página **Virtual Machines**, indique o número de CPUs virtuais e o número de núcleos por vCPU.
- Na página **Placas de Rede**, selecione o tipo de NIC para filtrar as redes associadas. Existem dois tipos de NIC: **VLAN** e **OVERLAY**. Selecione uma ou mais NICs que a imagem mestre contém 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 conexão de host Nutanix (especificamente, plug-in Nutanix AHV 2.7.1), o tamanho do disco rígido das VMs provisionadas é exibido incorretamente no Web Studio. O tamanho exibido é muito menor (1 GB) do que o tamanho real do armazenamento (50 GB). O tamanho do disco rígido é exibido corretamente no console do Nutanix.

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Nutanix
- Conexão com a nuvem Nutanix e soluções de parceiros
- Criar catálogos de máquinas

Criar um catálogo VMware

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

Observação:

Antes de criar um catálogo VMware, você precisa concluir a criação de uma conexão com o VMware. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/connections/connection-vmware-virtualization-environments.html).

Criar uma VM mestre

Use uma VM mestre para fornecer desktops e aplicativos de usuário em um catálogo de máquinas. No seu hipervisor:

1. Instale um VDA na VM mestre, selecionando a opção de otimizar o desktop, o que melhora o desempenho.
2. Tire um snapshot da VM mestre para usar como backup.

Observação:

Você pode usar o MCS para provisionar VMs no ambiente vSAN 8.0.

Criar um catálogo de máquinas usando um perfil de máquina

Você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A origem da entrada do perfil de máquina é um modelo VMware. O perfil de máquina captura as propriedades de hardware de um modelo VMware e as aplica às VMs recém-provisionadas no catálogo.

Observação:

- A entrada da imagem mestre (snapshot) e a entrada do perfil de máquina (modelo VMware) devem estar ambas com vTPM ativado ou ambas com vTPM desativado. Esta regra se aplica a `New-ProvScheme` e `Set-ProvScheme`.
- Se a imagem mestre estiver com vTPM ativado, o modelo VMware só poderá vir da mesma origem de VM que a imagem mestre.
- A política de armazenamento criptografado suporta apenas clone completo.
- Os catálogos baseados em perfil de máquina utilizam o modelo VMware fornecido para coletar informações do controlador de armazenamento, contando com os discos virtuais

> anexados. O modelo deve incluir um disco virtual que é necessário para recuperar as informações do controlador de armazenamento usadas para configurar discos virtuais para as máquinas virtuais.

> O modelo VMware no perfil de máquina deve existir durante o ciclo de vida do catálogo para permitir o provisionamento de VMs para o catálogo. Sem um modelo VMware, você não pode provisionar novas VMs. Quando um modelo VMware é excluído, você deve fornecer um novo modelo usando o comando `Set-ProvScheme`.

- O MCS captura propriedades de um modelo VMware. Você pode criar um novo modelo VMware referenciando propriedades armazenadas de um modelo VMware usando o comando Get-Provscheme.
- Alternativamente, se o catálogo de máquinas e as VMs provisionadas existirem, uma máquina provisionada por MCS também pode ser usada para criar um novo modelo VMware.

Com base em diferentes sistemas operacionais, você pode criar um catálogo de máquinas com diferentes configurações:

- Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Portanto, o modelo VMware, que é uma fonte de perfil de máquina, deve ter o vTPM anexado a ele.
- Se o Windows 10 estiver instalado na imagem mestre sem vTPM anexado, você pode criar um catálogo de máquinas com um modelo VMware sem vTPM como fonte para o perfil da máquina.

Existe outra configuração onde você pode criar um catálogo de máquinas usando o modo de disco de cópia completa com o modelo de perfil de máquina aplicado com política de armazenamento criptografado.

Para criar um catálogo de máquinas usando comandos PowerShell com perfil de máquina como entrada:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute os seguintes comandos:
    - Para criar um catálogo de máquinas com modelo VMware com vTPM anexado como fonte para entrada de perfil de máquina e imagem mestre com Windows 11 instalado:

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"
```

```
-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas com modelo VMware sem vTPM como fonte para perfil de máquina e imagem mestre com Windows 10 instalado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
```

```
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas usando o modo de disco de cópia completa com o modelo de perfil de máquina aplicado com política de armazenamento criptografado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"
```

```
-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()
```

```
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

Para atualizar um perfil de máquina, use o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

Verificar várias NICs

Você recebe várias mensagens de erro durante as verificações pré-voo para várias NICs ao usar um perfil de máquina e o parâmetro `NetworkMapping` nos comandos `New-ProvScheme` e `Set-ProvScheme`.

A lista de verificação pré-voo para várias NICs é a seguinte:

- Apenas a contagem de NICs do modelo de perfil de máquina é usada e validada. A rede para a qual essas NICs apontam não é usada ou validada em relação às redes da unidade de hospedagem.
- Se a contagem de NICs no modelo de perfil de máquina for maior que o número de redes na unidade de hospedagem, você receberá uma mensagem de erro.
- Se a contagem de NICs no modelo de perfil de máquina for zero, você receberá uma mensagem de erro. Quando a contagem de NICs no modelo de perfil de máquina for um, então:
  - Se nenhum mapeamento de rede for especificado no comando `New-ProvScheme` ou `Set-ProvScheme`, e a rede da unidade de hospedagem for única, então a rede da unidade de hospedagem será usada.
  - Se o mapeamento de rede for especificado, então o mapeamento de rede especificado será usado se for válido.
- Quando a contagem de NICs no modelo de perfil da máquina for maior que 1, ou a contagem de redes da unidade de hospedagem for maior que 1, então:

- É necessário um mapeamento de rede válido no comando, e ele deve fornecer mapeamento para cada NIC (ou seja, a contagem de NetworkMapping deve ser a mesma que a contagem de NICs do perfil da máquina).
- Múltiplas NICs não podem ser mapeadas para a mesma rede na unidade de hospedagem.
- A contagem de `NetworkMapping` e a contagem de NICs do perfil da máquina devem ser menores ou iguais à contagem de redes da unidade de hospedagem.
- `NetworkMapping` deve ser fornecido para cada ID de 0 a n-1, onde n é o número de adaptadores de rede no modelo de perfil da máquina.

Solução de problemas

Se a criação do catálogo falhar, consulte CTX294978.

Próximos passos

- Se este for o primeiro catálogo criado, o Web Studio o guiará para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo VMware

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Criar catálogos de máquinas

Criar catálogos de diferentes tipos de associação

Criar catálogos unidos ao Azure Active Directory Híbrido

> **Observação:**

> Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência a Azure Active Directory, Azure AD ou AAD agora se refere a Microsoft Entra ID.

> Este artigo descreve como criar catálogos unidos ao Azure Active Directory (AD) Híbrido.

Você pode criar catálogos unidos ao Azure AD usando o Web Studio ou o PowerShell.

Para obter informações sobre requisitos, limitações e considerações, consulte Unido ao Azure Active Directory Híbrido.

Usar o Web Studio

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar catálogos unidos ao Azure AD híbrido, siga as orientações gerais desse artigo, observando os detalhes específicos dos catálogos unidos ao Azure AD híbrido.

No assistente de criação de catálogo:

- Na página **Identidades da Máquina**, selecione **Unido ao Azure Active Directory Híbrido**. As máquinas criadas são de propriedade de uma organização e são conectadas com uma conta do Active Directory Domain Services que pertence a essa organização. Elas existem na nuvem e no local.

> **Observação:**
>
> Se você selecionar **Unido ao Azure Active Directory Híbrido** como o tipo de identidade, cada máquina no catálogo deve ter uma conta de computador AD correspondente.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações no Web Studio. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

A diferença entre catálogos unidos ao AD local e catálogos unidos ao Azure AD híbrido reside na criação do pool de identidades e das contas de máquina.

Para criar um pool de identidades junto com as contas para catálogos unidos ao 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-
d2f2-49d2-ab12-bae5bbd0df05"
```

```
New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

Observação:

`$password` é a senha correspondente para uma conta de usuário AD com Permissões de Gravação.

Todos os outros comandos usados para criar catálogos unidos ao Azure AD híbrido são os mesmos que para catálogos tradicionais unidos ao AD local.

Visualizar o status do processo de união ao Azure AD híbrido

No Web Studio, o status do processo de junção híbrida do Azure AD é visível quando as máquinas unidas ao Azure AD híbrido em um grupo de entrega estão em estado ligado. Para visualizar o status, use Pesquisar para identificar essas máquinas e, em seguida, para cada uma, verifique **Identidade da Máquina** na guia **Detalhes** no painel inferior. As seguintes informações podem aparecer em **Identidade da Máquina**:

- Unido ao Azure AD híbrido
- Ainda não unido ao Azure AD

Observação:

- Você pode experimentar um atraso na junção híbrida do Azure AD quando a máquina é ligada inicialmente. Isso é causado pelo intervalo de sincronização padrão da identidade da máquina (30 minutos do Azure AD Connect). A máquina estará no estado de junção híbrida do Azure AD somente depois que as identidades da máquina forem sincronizadas com o Azure AD por meio do Azure AD Connect.
- Se as máquinas falharem em estar no estado de junção híbrida do Azure AD, elas não serão registradas no Delivery Controller. O status de registro delas aparece como **Inicialização**.

> Além disso, usando o Web Studio, você pode descobrir por que as máquinas estão indisponíveis. Para fazer isso, clique em uma máquina no nó **Pesquisar**, verifique **Registro** na guia **Detalhes** no painel inferior e, em seguida, leia a dica de ferramenta para obter informações adicionais.

Solução de problemas

Se as máquinas falharem em ser unidas ao 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, **Ainda não unido ao 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 OU configurada para ser sincronizada com o Azure AD. Contas de máquina sem o atributo **userCertificate** não são sincronizadas com o Azure AD, mesmo que estejam na OU 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 após a criação da conta da máquina. Caso contrário, execute manualmente o comando `Start-ADSyncSyncCycle -PolicyType Delta` no console do PowerShell da máquina Azure AD Connect para acionar uma sincronização imediata.

- Verifique se o par de chaves do dispositivo gerenciado pelo Citrix para junção híbrida do Azure AD 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. Caso contrário, as possíveis razões são:

  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `HybridAzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
  - A máquina não foi provisionada usando o mesmo esquema de provisionamento do catálogo de máquinas.
  - A máquina não está unida ao domínio local. A junção ao domínio local é um pré-requisito para a junção híbrida do Azure AD.

- Verifique as mensagens de diagnóstico executando o comando `dsregcmd /status /debug` na máquina provisionada pelo MCS.
  - Se a junção híbrida do Azure AD for bem-sucedida, **AzureAdJoined** e **DomainJoined** serão **YES** na saída da linha de comando.
  - Caso contrário, consulte a documentação da Microsoft para solucionar os problemas: `<https://docs.microsoft.com/pt-br/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`.
  - Se você receber a mensagem de erro **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, execute o seguinte comando PowerShell para reparar o certificado do usuário:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    Para obter mais informações sobre o problema do certificado do usuário, consulte CTX566696.

Criar catálogos não associados a domínio

Este artigo descreve como criar catálogos não associados a domínio usando o Citrix Virtual Apps and Desktops.

Para obter informações sobre requisitos, limitações e considerações, consulte Não associado a domínio.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recurso
   - navegar para a UI de administração do Citrix Cloud™ > menu hambúrguer superior esquerdo > **Locais de Recursos**.
   - Clique em **+ Local de Recurso**.
   - Insira um nome para o novo local de recurso e clique em **Salvar**.
2. Crie uma conexão de hospedagem. Consulte a seção Criar e gerenciar conexões para obter detalhes.

Usando o Citrix Virtual Apps and Desktops, você pode criar catálogos baseados em grupos de trabalho ou máquinas não associadas a domínio. A criação de máquinas não associadas a

domínio depende de como o pool de identidades da conta é criado. O pool de identidades da conta é o mecanismo usado pelo MCS para criar e rastrear nomes de máquinas durante o provisionamento do catálogo.

Atualmente, você pode criar catálogos não associados a domínio apenas usando os comandos do PowerShell.

Usar PowerShell

Você pode criar um pool de identidades para catálogos não associados a domínio usando o SDK do PowerShell Remoto.

Use os parâmetros do PowerShell, **WorkgroupMachine** e **IdentityType**, para criar um pool de identidades para catálogos não associados a domínio. Os parâmetros eliminam a necessidade de especificar todos os parâmetros específicos do AD, incluindo as credenciais de administrador de domínio:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

Todos os outros comandos usados para criar catálogos não associados a domínio são os mesmos que para os catálogos tradicionais associados ao Active Directory local.

Gerenciar catálogos de máquinas

> **Nota:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Você pode adicionar ou remover máquinas de um catálogo de máquinas, renomear, alterar a descrição ou gerenciar as contas de computador do Active Directory de um catálogo.

A manutenção de catálogos também pode incluir a garantia de que cada máquina tenha as atualizações mais recentes do sistema operacional. Incluindo atualizações de antivírus, atualizações de sistema operacional ou alterações de configuração.

- Catálogos que contêm máquinas aleatórias agrupadas criadas usando o Machine Creation Services™ (MCS) mantêm as máquinas atualizando a imagem mestre usada no catálogo e, em seguida, atualizando as máquinas. Esse método permite que você atualize eficientemente um grande número de máquinas de usuário.
- Para catálogos que contêm máquinas estáticas, permanentemente atribuídas, e para catálogos de máquinas de Acesso Remoto a PC, você gerencia as atualizações das máquinas dos usuários fora do Web Studio. Execute esta tarefa individualmente ou coletivamente usando ferramentas de distribuição de software de terceiros.

Para obter informações sobre como criar e gerenciar conexões com hipervisores de host, consulte Conexões e recursos.

> **Nota:**
>
> O MCS não oferece suporte ao Windows 10 IoT Core e ao Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

Sobre instâncias persistentes

Ao atualizar um catálogo MCS criado usando instâncias persistentes ou dedicadas, todas as novas máquinas criadas para o catálogo usam a imagem atualizada. As instâncias pré-existentes continuam a usar a instância original. O processo de atualização de uma imagem é feito da mesma forma para qualquer outro tipo de catálogo. Considere o seguinte:

- Com catálogos de disco persistentes, as máquinas pré-existentes não são atualizadas para a nova imagem, mas quaisquer novas máquinas adicionadas ao catálogo usam a nova imagem.
- Para catálogos de disco não persistentes, a imagem da máquina é atualizada na próxima vez que a máquina for redefinida.
- Com catálogos de máquinas persistentes, a atualização da imagem também atualiza as instâncias do catálogo que a utilizam.
- Para catálogos que não persistem, se você quiser imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

Gerenciar catálogos de máquinas

Você pode gerenciar um catálogo de máquinas de duas maneiras:

- Usando o Web Studio
- Usando o PowerShell

Usar o Web Studio

Esta seção detalha como você pode gerenciar catálogos usando o Web Studio:

- Gerenciar catálogos de máquinas
    - Introdução
    - Sobre instâncias persistentes
- Gerenciar catálogos de máquinas
- Usar o Web Studio
- Exibir detalhes do catálogo
    - Adicionar máquinas a um catálogo
    - Excluir máquinas de um catálogo
- Editar um catálogo
- Renomear um catálogo
- Mover um catálogo para uma zona diferente(#move-a-catalog-to-a-different-zone)
- Excluir um catálogo
- Gerenciar contas de computador do Active Directory em um catálogo
- Atualizar um catálogo(#update-a-catalog)
    - Atualizar ou criar uma imagem mestre(#update-or-create-a-master-image)
    - Alterar a imagem mestre(#change-the-master-image)
    - Reverter a imagem mestre(#roll-back-the-master-image)
- Alterar o nível funcional ou desfazer a alteração
- Clonar um catálogo
- Organizar catálogos usando pastas
    - Criar uma pasta de catálogo(#create-a-catalog-folder)

    - Mover um catálogo(#move-a-catalog)
    - Gerenciar pastas de catálogo(#manage-catalog-folders)
- Tentar novamente a criação do catálogo
- Registrar VDAs provisionados não-MCS usando tokens (Pré-visualização)(#enroll-non-mcs-provisioned-vdas-using-tokens-preview)
- Usar PowerShell(#use-powershell)
- Recuperar avisos e erros associados a um catálogo
- Adicionar descrições a uma imagem
- Redefinir disco do SO
- Alterar a configuração de rede para um esquema de provisionamento existente(#change-the-network-setting-for-an-existing-provisioning-scheme)
- Gerenciar versões de um catálogo de máquinas
- Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina
- Reparar as informações de identidade de contas de computador ativas
    - Condições(#conditions)
    - Redefinir disco de identidade(#reset-identity-disk)
- Alterar a configuração de cache em um catálogo de máquinas existente(#change-cache-configuration-on-an-existing-machine-catalog)
    - Requisitos(#requirements)
    - Alterar a configuração do cache
- Suporte à atualização do VDA via acesso a compartilhamento de arquivos local
    - Cmdlets do PowerShell
    - Pré-requisitos
    - Como definir permissões de compartilhamento de arquivos
    - Atualizações do VDA de um compartilhamento de arquivos local
- Solucionar problemas
- Onde ir em seguida

Exibir detalhes do catálogo

1. Use a função de pesquisa para localizar um catálogo de máquinas específico. Consulte Pesquisar instâncias para obter instruções.
2. Nos resultados da pesquisa, selecione um catálogo conforme necessário.
3. Consulte a tabela a seguir para obter descrições das colunas do catálogo.
4. Clique em uma guia no painel de detalhes inferior para obter mais informações sobre este catálogo.

COLUNA	DESCRIÇÃO
Catálogo de Máquinas	O nome e o tipo de alocação do catálogo. Os tipos de alocação incluem: • Aleatório: As máquinas no catálogo são alocadas a um usuário aleatoriamente. • Permanente: As máquinas no catálogo são alocadas a um usuário permanentemente.
Tipo de Máquina	O tipo de sessão suportado das máquinas no catálogo. Os valores possíveis incluem: • Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: Descartar. • Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: No disco local

COLUNA	DESCRIÇÃO
	• Tipo de SO: SO de sessão única (Acesso Remoto a PC) • Tipo de SO: SO de sessão única (Virtual); Dados do usuário: Descartar • Tipo de SO: SO de sessão única (Virtual); Dados do usuário: No disco local
Contagem de Máquinas	A contagem de máquinas no catálogo e o método de provisionamento. Os métodos de provisionamento possíveis incluem: Serviços de criação de máquinas (máquina MCS), Manual e Serviços de provisionamento Citrix™.
Contagem Alocada	O número de máquinas no catálogo atribuídas a um grupo de entrega.
Pasta	O local do catálogo na árvore de **Catálogos de Máquinas**. Ele exibe o nome da pasta em que o catálogo está (incluindo a barra invertida final), ou `-` se o catálogo estiver no nível raiz.
Atualização do VDA	Estado da Atualização do VDA. Os valores possíveis incluem: Não configurado,

COLUNA	DESCRIÇÃO
	Agendado, Disponível e Atualizado.
Status da Imagem	O status de atualização da imagem do catálogo. Aplicável apenas a catálogos de máquinas não persistentes. Os valores possíveis incluem: Totalmente atualizado, Parcialmente atualizado, Atualizações pendentes, Preparando

Adicionar máquinas a um catálogo

Antes de começar:

- Certifique-se de que o host de virtualização tenha processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- Certifique-se de ter contas de computador do Active Directory não utilizadas suficientes. Se você estiver usando contas existentes, o número de máquinas que você pode adicionar é limitado pelo número de contas disponíveis.
- Se você usar o Web Studio para criar contas de computador do Active Directory para as máquinas adicionais, você deve ter a permissão de administrador de domínio apropriada.

Para adicionar máquinas a um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar máquinas** na barra de ações.
4. Selecione o número de máquinas virtuais a serem adicionadas.
5. Se houver contas do Active Directory existentes insuficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas. Especifique um esquema de nomenclatura de conta, usando sinais de cerquilha para indicar onde números ou letras sequenciais aparecem. Não use uma barra (/) em um nome de UO. Um nome não pode começar com um número. 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.

6. Se você usar contas do Active Directory existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo .csv contendo nomes de contas. Certifique-se de que há contas suficientes para todas as máquinas que você está adicionando. O Web Studio gerencia essas contas. Permita que o Web Studio redefina as senhas de todas as contas, ou especifique a senha da conta, que deve ser a mesma para todas as contas.

As máquinas são criadas como um processo em segundo plano e podem levar muito tempo ao criar muitas máquinas. A criação de máquinas continua mesmo se você fechar o Web Studio.

Excluir máquinas de um catálogo

Depois de excluir uma máquina de um catálogo de máquinas, os usuários não poderão mais acessá-la, portanto, antes de excluir uma máquina, certifique-se de que:

- Os dados do usuário foram copiados ou não são mais necessários.
- Todos os usuários estão desconectados. Ativar o modo de manutenção impede que novas conexões sejam feitas a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Exibir Máquinas** na barra de ações.
4. Selecione uma ou mais máquinas e, em seguida, selecione **Excluir** na barra de ações.

Escolha se deseja excluir as máquinas que estão sendo removidas. Se você optar por excluir as máquinas, indique se as contas do Active Directory para essas máquinas são mantidas, desabilitadas ou excluídas.

Editar um catálogo

1. Na página **Descrição**, altere a descrição do catálogo.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Editar Catálogo de Máquinas** na barra de ações.
4. Na página **Escopos**, altere os escopos.

5. Na página **NIC**, execute as seguintes ações:

   - Para alterar o mapeamento de sub-rede de uma NIC, selecione uma rede no campo **Rede Associada**.
   - Para adicionar um mapeamento de sub-rede, selecione **Adicionar NIC**, selecione uma rede no campo **Rede Associada** e clique em **Salvar**.

   Somente as sub-redes presentes no host associado ao catálogo aparecem no campo **Rede Associada**.

   Você só pode adicionar NIC a catálogos de máquinas do Azure sem perfis de máquina.

   > **Nota:**
   >
   > - Para catálogos de máquinas AWS, você não pode mapear a mesma sub-rede para mais de uma NIC.
   > - Para catálogos de máquinas com perfis de máquina, o número de NICs no catálogo deve ser igual ao número de NICs no perfil de máquina.
   > - Este recurso não é compatível com hipervisores IBM Cloud.
   > - Este recurso é suportado apenas para Nutanix Prism Element no caso de hipervisores Nutanix.

6. Você pode ver outras páginas 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 que você faz se aplicam apenas às máquinas que você adicionar ao catálogo posteriormente. As máquinas existentes permanecem inalteradas.

   - Na página **Máquinas Virtuais**, altere o tamanho da máquina e as zonas de disponibilidade onde você deseja criar máquinas.

     > **Nota:**
     >
     > - Somente os tamanhos de máquina compatíveis com o catálogo são exibidos.

    - Se necessário, selecione **Mostrar apenas tamanhos de máquina usados em outros catálogos de máquinas** para filtrar a lista de tamanhos de máquina.

- Na página **Perfil da Máquina**, escolha se deseja usar ou alterar um perfil de máquina.
- (Visível apenas quando o catálogo está configurado com um host de grupo dedicado) Na página **Grupo de host dedicado**, escolha se deseja alterar um grupo de host.
- Na página **Tipos de Armazenamento e Licença**, escolha se deseja alterar o tipo de armazenamento, o tipo de licença e as configurações da Galeria de Computadores do Azure (disponível apenas quando **Colocar imagem preparada na Galeria do Azure** estiver em uso).

Nota:

Se a configuração recém-selecionada não suportar o tamanho atual da máquina, uma caixa de diálogo de aviso aparecerá, informando que a alteração da configuração redefine a configuração de tamanho da máquina. Se você optar por continuar, um ponto vermelho aparecerá ao lado do menu **Máquinas Virtuais**, solicitando que você selecione um novo tamanho de máquina.

- Na página **Tipo de Licença**, escolha se deseja alterar a configuração de licença do Windows ou licença do Linux.

Para catálogos de Acesso Remoto a PC, as seguintes páginas estão visíveis:

- Na página **Gerenciamento de Energia**, altere as configurações de gerenciamento de energia e selecione uma conexão de gerenciamento de energia.
- Na página **Unidades Organizacionais**, adicione ou remova UOs do Active Directory.

7. Clique em **Aplicar** para aplicar as alterações feitas e clique em **Salvar** para sair.

Renomear um catálogo

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Renomear Catálogo de Máquinas** na barra de ações.

4. Insira o novo nome.

Mover um catálogo para uma zona diferente

Se sua implantação tiver mais de uma zona, você poderá mover um catálogo de uma zona para outra.

Mover um catálogo para uma zona diferente, que não seja o hipervisor que contém as VMs nesse catálogo, afeta o desempenho.

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Mover** na barra de ações.
4. Selecione a zona para a qual você deseja mover o catálogo.

Excluir um catálogo

Antes de excluir um catálogo, certifique-se de que:

- Todos os usuários são desconectados e você não executa nenhuma sessão desconectada.
- O modo de manutenção está ativado para todas as máquinas no catálogo para que novas conexões não possam ser feitas.
- Todas as máquinas no catálogo estão desligadas.
- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Excluir Catálogo de Máquinas** na barra de ações.
4. Indique se as máquinas no catálogo são excluídas. Se você optar por excluir as máquinas, indique se as contas de computador do Active Directory para essas máquinas são retidas, desabilitadas ou excluídas.

Gerenciar contas de computador do Active Directory em um catálogo

Para gerenciar contas do Active Directory em um catálogo de máquinas, você pode:

- Libere contas de máquina não utilizadas removendo contas de computador do Active Directory de catálogos de SO de sessão única e de SO de várias sessões. Essas contas podem então ser usadas para outras máquinas.
- Adicionar contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam no lugar. Não use uma barra (/) em um nome de OU.

Para gerenciar contas do Active Directory:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Gerenciar contas AD** na barra de ações.
4. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas das contas: redefina todas elas ou insira uma senha que se aplique a todas as contas.

   Você pode redefinir senhas se não souber as senhas atuais da conta; você deve ter permissão para realizar uma redefinição de senha. Ao inserir uma senha, a senha é alterada nas contas à medida que são importadas. Ao excluir uma conta, escolha se a conta no Active Directory é mantida, desabilitada ou excluída.

Indique se as contas do Active Directory são retidas, desabilitadas ou excluídas ao remover máquinas de um catálogo ou excluir um catálogo.

Atualizar um catálogo

Recomendamos que você salve cópias ou instantâneos de imagens mestre antes de atualizar as máquinas no catálogo. O banco de dados mantém um registro histórico das imagens mestre usadas com cada catálogo de máquinas. Reverta as máquinas em um catálogo para usar a versão anterior da imagem mestre. Execute esta tarefa se os usuários encontrarem problemas com as atualizações que você implantou em seus desktops. Isso minimiza o tempo de inatividade do usuário. Não exclua, mova ou renomeie imagens mestre. Você não pode reverter um catálogo para usá-las.

Depois que uma máquina é atualizada, ela reinicia automaticamente.

Atualizar ou criar uma imagem mestre

Antes de atualizar o catálogo de máquinas, atualize uma imagem mestre existente ou crie uma em seu hipervisor host.

1. Em seu hipervisor, tire um instantâneo da VM atual e dê ao instantâneo um nome significativo. Este instantâneo pode ser usado para reverter (restaurar) máquinas no catálogo, se necessário.
2. Se necessário, ligue a imagem mestre e faça login.
3. Instale atualizações ou faça as alterações necessárias na imagem mestre.
4. Desligue a VM.
5. Tire um instantâneo da VM. Dê a ele um nome significativo que seja reconhecido quando o catálogo for atualizado no Web Studio. Embora o Web Studio possa criar um instantâneo, a Citrix recomenda que você o crie usando o console de gerenciamento do hipervisor. Em seguida, selecione esse instantâneo no Web Studio. Esse processo permite que você forneça um nome e uma descrição significativos, em vez de um nome gerado automaticamente. Para imagens mestre de GPU, você pode alterar a imagem mestre apenas através do console XenServer®.

Alterar a imagem mestre

Para preparar e implantar a atualização em todas as máquinas em um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Alterar Imagem Mestre** na barra de ações.
4. Na página **Imagem**, selecione o host e a imagem que você deseja implantar.

> **Dica:**
>
> Para um catálogo criado por MCS, você pode anotar sua imagem adicionando uma nota para a imagem. Uma nota pode conter até 500 caracteres. Cada vez que você altera a imagem mestre, uma entrada relacionada à nota é criada, independentemente de você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como nula (-). Para visualizar o histórico de notas da imagem, selecione o catálogo, clique em **Propriedades do Modelo** no painel inferior e, em seguida, clique em **Exibir histórico de notas**.

5. Na página **Estratégia de Implantação**, escolha quando as máquinas no catálogo de máquinas são atualizadas com a nova imagem mestre: no próximo desligamento ou imediatamente.

> **Observação:**
>
> A página **Estratégia de Implantação** não está disponível para VMs persistentes porque a implantação é aplicável apenas a VMs não persistentes.

6. Verifique as informações na página **Resumo** e clique em **Concluir**. Cada máquina reinicia automaticamente após ser atualizada.

Para acompanhar o progresso da atualização, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Ao atualizar um catálogo usando o SDK do PowerShell diretamente, em vez do Web Studio, especifique um modelo de hipervisor (**VMTemplates**). Use-o como uma alternativa a uma imagem ou a um instantâneo de uma imagem.

Estratégia de implantação:

A atualização de imagens no próximo desligamento afetará imediatamente todas as máquinas que não estão em uso no momento, ou seja, máquinas que não possuem uma sessão de usuário ativa. Um sistema em uso recebe a atualização quando a sessão ativa atual termina. Considere o seguinte:

- Novas sessões não podem ser iniciadas até que a atualização seja concluída nas máquinas aplicáveis.
- Para máquinas de SO de sessão única, as máquinas são atualizadas imediatamente quando a máquina não está em uso ou quando os usuários não estão logados.
- Para um SO multi-sessão com máquinas filhas, as reinicializações não ocorrem automaticamente. Para aplicar a imagem mestre atualizada, reinicie as máquinas usando o Studio, PowerShell ou Workspace. A reinicialização a partir das máquinas ou do hipervisor não aplica a atualização.

> **Dica:**
>
> Limite o número de máquinas sendo reiniciadas usando as configurações avançadas para uma conexão de host. Use essas configurações para modificar as ações tomadas para um determinado catálogo; as configurações avançadas variam dependendo do hipervisor.

Reverter a imagem mestre

Depois de implantar uma imagem mestre atualizada ou nova, você pode revertê-la. Esse processo pode ser necessário se ocorrerem problemas com as máquinas recém-atualizadas. Ao reverter, as máquinas no catálogo são revertidas para a última imagem funcional. Quaisquer novos recursos que exijam a imagem mais recente não estarão mais disponíveis. Assim como na implantação, a reversão de uma máquina inclui uma reinicialização.

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione o catálogo e, em seguida, selecione **Reverter Imagem Mestra** na barra de ações.
4. Especifique quando aplicar a imagem mestre anterior às máquinas, conforme descrito na seção anterior para a operação de implantação.

A reversão é aplicada apenas às máquinas que precisam ser revertidas. Máquinas que não são atualizadas com a imagem mestre nova ou atualizada não recebem mensagens de notificação e não são forçadas a fazer logoff.

Para acompanhar o progresso da reversão, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

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. A Citrix recomenda atualizar todos os VDAs para a versão mais recente para permitir o acesso a todos os recursos mais recentes.

Antes de alterar o nível funcional para um catálogo de máquinas:

- Inicie as máquinas atualizadas para que elas se registrem no Controller. Esse processo permite que o Web Studio determine que as máquinas no catálogo precisam de atualização.

Para alterar o nível funcional de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Catálogos de Máquinas** no painel esquerdo.
3. Selecione o catálogo. A guia **Detalhes** no painel inferior exibe as informações da versão.
4. Selecione **Alterar Nível Funcional**. Se o Web Studio detectar que o catálogo precisa ser atualizado, ele exibirá uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser atualizadas, uma mensagem explicará o motivo. Para garantir que todas as

máquinas funcionem corretamente, a Citrix recomenda que você resolva os problemas da máquina antes de clicar em **Alterar** para prosseguir.

Após a conclusão da alteração do catálogo, você pode reverter as máquinas para suas versões VDA anteriores selecionando o catálogo e, em seguida, selecionando **Desfazer Alteração de Nível Funcional** na barra de ações.

Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Você não pode alterar as configurações associadas ao sistema operacional e ao gerenciamento de máquinas. O catálogo clonado herda essas configurações do original.
- A clonagem de um catálogo pode levar algum tempo para ser concluída. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.
- O catálogo clonado herda o nome do original e tem o sufixo `Copy`. Você pode alterar o nome. Consulte Renomear um catálogo.
- Após a conclusão da clonagem, certifique-se de atribuir o catálogo clonado a um grupo de entrega.

1. Faça login no Web Studio e, em seguida, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Clonar** na barra de ações.
3. Na janela **Clonar Catálogo de Máquinas Selecionado**, visualize as configurações do catálogo clonado e configure as configurações conforme aplicável. Selecione **Avançar** para prosseguir para a próxima página.
4. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para iniciar a clonagem.
5. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.

Organizar catálogos usando pastas

Você pode criar pastas para organizar catálogos para facilitar o acesso. Por exemplo, você pode organizar catálogos por tipo de imagem ou por estrutura organizacional.

Criar uma pasta de catálogo

Antes de começar, planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis de profundidade (excluindo a pasta raiz padrão).

- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós no Web Studio (como os nós **Catálogos de Máquinas** e **Aplicativos**) compartilham uma árvore de pastas no backend. Para evitar conflitos de nomes com outros nós ao renomear ou mover pastas, recomendamos que você dê nomes diferentes para pastas de primeiro nível em nós diferentes.

Para criar uma pasta de catálogo, siga estas etapas:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra de **Ações**.
3. Digite um nome para a nova pasta e clique em **Concluído**.

> **Dica:**
>
> Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Visualize catálogos por pasta. Você também pode ativar **Visualizar tudo** acima da hierarquia de pastas para visualizar todos os catálogos de uma vez.
3. Clique com o botão direito em um catálogo e selecione **Mover Catálogo de Máquinas**.
4. Selecione a pasta para a qual você deseja mover o catálogo e clique em **Concluído**.

> **Dica:**
>
> Você pode arrastar um catálogo para uma pasta.

Gerenciar pastas de catálogo

Você pode excluir, renomear e mover pastas de catálogo.

Você pode excluir uma pasta somente se ela e suas subpastas não contiverem catálogos.

Para gerenciar uma pasta, siga as etapas abaixo:

1. Selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

Tentar novamente a criação do catálogo

> **Nota:**
>
> Este recurso se aplica apenas a catálogos MCS.
>
> Os catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, vá para a guia **Solucionar problemas** de cada catálogo. Antes de tentar novamente a criação do catálogo, esteja ciente das seguintes considerações:

- Verifique primeiro as informações de solução de problemas e resolva os problemas. As informações descrevem os problemas encontrados e fornecem recomendações para resolvê-los.
- Você não pode alterar as configurações associadas a Sistema operacional e gerenciamento de máquina. O catálogo herda essas configurações do original.
- A criação pode levar algum tempo para ser concluída. Se necessário, selecione **Ocultar progresso** para executar a criação em segundo plano.

Para tentar novamente a criação de um catálogo, faça o seguinte:

1. No Web Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo e vá para a guia **Solucionar problemas**.
3. Clique no hiperlink de repetição para tentar novamente a criação do catálogo.
4. No assistente que aparece, altere as configurações onde for necessário. Se não houver necessidade de fazer alterações, você pode ir diretamente para a página **Resumo**.

5. Depois de terminar, selecione **Concluir** para iniciar a criação.

Registrar VDAs provisionados sem MCS usando tokens (Pré-visualização)

Agora você pode gerar e gerenciar tokens de registro para VDAs provisionados sem MCS. Essa implementação permite o registro de VDA via WebSocket sem provisionar os VDAs com MCS. Esse recurso também oferece suporte a Linux Virtual Delivery Agent, Citrix Virtual Delivery Agent para macOS e VDAs não ingressados no domínio com Citrix Virtual Apps and Desktops.

Antes de começar

1. Configure seu site. Para obter mais informações, consulte Criar um site.
2. Instale certificados TLS nos Delivery Controllers. Para obter mais informações, consulte Instalar certificados de servidor TLS nos Controllers.
3. Instale a CA raiz e a CA intermediária no VDA para confiar no Delivery Controller.
4. Habilite a conexão WebSocket no Delivery Controller. Execute o seguinte comando em cada Delivery Controller presente em seu site:

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **Observação:**
>
> Certifique-se de reiniciar os Delivery Controllers após habilitar o WebSocket.

Gerar tokens de inscrição

Depois de decidir habilitar a inscrição baseada em token para máquinas provisionadas não-Citrix, você deve primeiro gerar tokens por catálogo de máquina e, em seguida, compartilhá-los com os administradores de instalação do VDA.

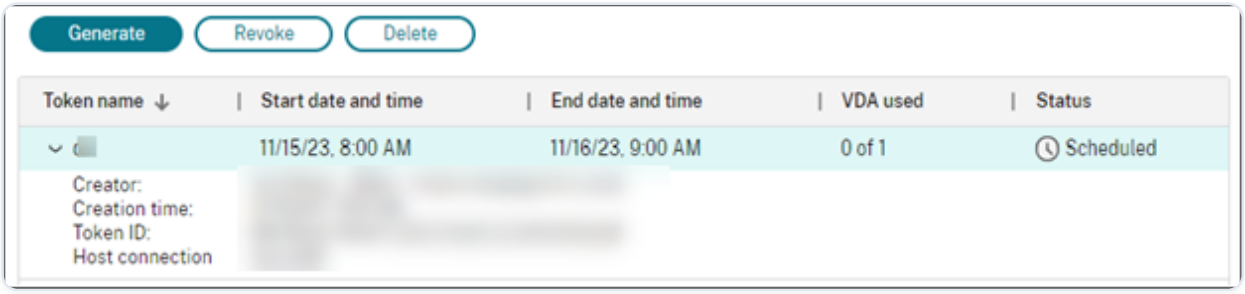
Um token de registro apresenta:

- Intervalo de registro: 1–100 máquinas VDA
- Período de validade: até 14 dias

Para gerar um token para um catálogo usando o Web Studio, siga estas etapas:

1. Em **Web Studio > Catálogos de Máquinas**, localize um catálogo não provisionado por MCS, que tenha **Método de provisionamento: Manual** exibido na coluna **Contagem de Máquinas**.
2. Clique com o botão direito do mouse no catálogo e selecione **Gerenciar Tokens de Registro**.
3. Na página **Gerar token de registro** que aparece, forneça as seguintes informações do token:
   - Digite um nome para o token.
   - Insira seu período de validade. O período não deve ser superior a 14 dias. O token é válido apenas para o período especificado.
   - (Opcional) Selecione uma conexão de host para o gerenciamento de energia de VDAs registrados com o token. As opções incluem todas as conexões de host na zona deste catálogo.
   - Insira os limites de uso do token (entre 1 e 100).
4. Clique em **Gerar**.
5. Na janela **Token gerado com sucesso** que aparece, copie o token e salve-o em um local seguro, ou clique em **Baixar** para fazer o download para a pasta **Downloads**.

   Um registro de token aparece na lista de tokens.



6. Compartilhe o token com os administradores de instalação do VDA.

   Para obter mais informações sobre como instalar o VDA e um token nas máquinas, consulte Instalar VDAs.

Gerenciar tokens

Você tem duas opções para revogar um token e torná-lo indisponível para o registro do VDA:

- Revogar: Revoga o token, mas o mantém na lista para fins de registro.
- Excluir: Revoga o token e o exclui da lista.

> **Observação:**

> Tokens expirados são excluídos automaticamente em 14 dias.

Registrar máquinas em catálogos usando a ferramenta de registro VDA WebSocket

A ferramenta de registro de VDA WebSocket facilita o registro baseado em token para máquinas VDA. Esta ferramenta ajuda você a converter uma conexão em uma conexão WebSocket adicionando o VDA ao catálogo de máquinas usando o token de registro.

> **Observação:**
>
> Esta ferramenta foi projetada para registrar máquinas VDA que não foram registradas em nenhum catálogo de máquinas.

> Siga as instruções para executar a ferramenta de registro:

1. Faça login no VDA.
2. Localize a ferramenta `EnrollMachine.exe`, em `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Execute a ferramenta com os parâmetros de entrada apropriados. Por exemplo, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

A tabela a seguir descreve os parâmetros de entrada da ferramenta de registro:

NOME DO PARÂMETRO	OBRIGATÓRIO	DESCRIÇÃO	EXEMPLO
`-websocket_token_stdin`	Sim	Lê o token de registro.	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		Lê o token de registro diretamente do parâmetro da linha de comando.	`.\EnrollMachine.exe -websocket_token_string:<token>`

NOME DO PARÂMETRO	OBRIGATÓRIO	DESCRIÇÃO	EXEMPLO
`-websocket_token_file:[token-file-path]`		Lê o token de registro do caminho fornecido.	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	Não	Mostra os logs da ferramenta de registro.	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	Não	Mostra um breve texto de ajuda.	`.\EnrollMachine.exe -help`

Após a inscrição bem-sucedida, você receberá uma mensagem de sucesso na ferramenta e nos logs. Certifique-se de fazer login no Web Studio para verificar se a máquina VDA foi adicionada ao catálogo e se o status da máquina está registrado.

Solução de problemas

Por padrão, você pode encontrar os logs da ferramenta de registro em:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

Se você especificou um caminho diferente para os logs, pode usar `log:[log-file-path]` para recuperar seus logs.

A tabela a seguir lista os códigos retornados pela ferramenta de registro:

CÓDIGO	STRING	DESCRIÇÃO
0	Sucesso	O VDA foi adicionado com sucesso ao catálogo de máquinas.

CÓDIGO	STRING	DESCRIÇÃO
-1	ArgumentoInválido	O parâmetro de entrada no token de registro é inválido.
-2	BrokerAgentNãoEncontrado	O serviço do agente do broker não foi encontrado.
-3	TokenInválido	O token inserido é inválido.
-4	ClaimsObrigatóriosDoTokenAusentes	As declarações (claims) obrigatórias para o token estão ausentes, por exemplo, CustomerId ou URIs de Registro.
-5	ErroInterno	Ocorreu um erro geral.
-6	TempoEsgotado	A tarefa expirou.
-7	FalhaAoDeterminarStatusADDaMáquina	O serviço que retorna o status de ingresso da máquina no AD falhou.
-8	MáquinaADFalhouAoEncontrarSid	O serviço que retorna o Sid da máquina AD falhou.
-9	FalhaNaSolicitaçãoDeInscrição	A solicitação falhou devido a um erro HTTP.
-10	RespostaDeInscriçãoComCamposObrigatóriosAusentes	A resposta da ferramenta de inscrição está faltando o parâmetro `VirtualSiteId`.
-11	PermissãoInsuficiente	Você não tem a permissão necessária para executar a tarefa.
-12	FalhaAoDeterminarStatusDeAdesãoAadDaMáquina	O serviço que verifica o status de adesão ao AD da máquina retorna um erro.

CÓDIGO	STRING	DESCRIÇÃO
-13	AadMáquinaFalhouAoEncontrarDeviceId	O parâmetro adicional `AAD device id` adicionado pelo sistema está vazio.
-14	AadDeviceIdNãoVálido	O parâmetro adicional `AAD device id` adicionado pelo sistema não é um guid válido.
-15	NenhumEndereçoMacVálido	Endereço MAC inválido.
-16	FailedToGetComputerHostNameForVdaInstanceName	Falha ao obter o nome do host do computador para definir o parâmetro adicional `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Falha ao abrir a chave de registro do VDA para gravar a lista de Delivery Controllers.
-18	O token com falha atingiu a contagem máxima	O token com falha atingiu a contagem máxima.

Usar PowerShell

Esta seção detalha como você pode gerenciar catálogos usando o PowerShell:

- Recuperar avisos e erros associados a um catálogo
- Adicionar descrições a uma imagem
- Redefinir disco do SO
- Alterar a configuração de rede para um esquema de provisionamento existente
- Gerenciar versões de um catálogo de máquinas
- Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina
- Reparar as informações de identidade de contas de computador ativas
- Alterar a configuração de cache em um catálogo de máquinas existente
- Suporte à atualização de VDA via acesso a compartilhamento de arquivo local

Recuperar avisos e erros associados a um catálogo

Você pode obter erros e avisos históricos para entender os problemas com seu catálogo de máquinas MCS e corrigi-los.

Usando comandos PowerShell, você pode:

- Obter uma lista de erros ou avisos
- Alterar o estado do aviso de **Novo** para **Reconhecido**
- Excluir os erros ou avisos

Para executar os comandos PowerShell:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

Para obter uma lista de erros e avisos:

Execute o comando `Get-ProvOperationEvent`.

- Sem parâmetros: Obtém todos os erros e avisos
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Obtém todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `EventId`: Obtém um erro ou aviso específico que corresponde a este ID de evento
- Com o parâmetro `Filter`: Obtém erros ou avisos por filtro personalizado

Para alterar o estado de erros ou avisos de **Novo** para **Reconhecido**:

Execute o comando `Confirm-ProvOperationEvent`.

- Com o parâmetro `EventId`: Define o estado de um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como saída do comando `Get-ProvOperationEvent`
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Define o estado de todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Define o estado de todos os erros e avisos como **Reconhecido**

Para excluir os erros ou avisos:

Execute o comando `Remove-ProvOperationEvent`.

- Com o parâmetro `EventId`: Remove um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como saída do comando `Get-ProvOperationEvent`.
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Remove todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Remove todos os erros e avisos

Para obter mais informações, consulte Citrix PowerShell SDK.

Excluir máquinas sem acesso ao hipervisor

Ao excluir uma VM ou um esquema de provisionamento, o MCS precisa remover tags da VM e, às vezes, também do disco base, para que os recursos incluídos nas opções de exclusão não sejam mais rastreados ou identificados pelo MCS. No entanto, alguns desses recursos são acessíveis apenas através do hipervisor. Use a opção `PurgeDBOnly` no PowerShell `Remove-ProvVM` para excluir objetos de recurso de VM, como VM, disco base, imagem no ACG e assim por diante, do banco de dados, mesmo quando não há acesso ao hipervisor.

Esta opção está habilitada em:

- todos os hipervisores suportados
- VMs persistentes e não persistentes

Limitações

Você não pode usar os comandos -PurgeDBOnly e -ForgetVM ao mesmo tempo.

Usar o comando PurgeDBOnly

Ao executar o comando PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`, a operação de exclusão pode falhar nos seguintes cenários:

- A conexão do host está em modo de manutenção
- Credenciais inválidas
- Falha na autenticação
- Operação não autorizada
- O hipervisor está inacessível

> **Nota:**

> Remove-provVM -ForgetVM tem como alvo apenas VMs persistentes. Se uma das VMs na lista não for persistente, a operação falhará.

> Quando a operação falha porque o hipervisor está inacessível, o seguinte prompt aparece:

`Try to use -PurgeDBOnly option to clean DDC database.`.

Use a opção `-PurgeDBOnly` no comando PowerShell `Remove-ProvVM` para excluir referências de uma VM do banco de dados MCS. Por exemplo,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

Adicionar descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagem para catálogos de máquinas. Use esse recurso para adicionar uma descrição ao criar um catálogo ou ao atualizar uma imagem mestre existente para um catálogo. Você também pode exibir informações para cada imagem mestre no catálogo. Use os seguintes comandos para adicionar ou visualizar descrições de imagem:

- Para adicionar uma nota ao criar um catálogo de máquinas com uma imagem mestre, use o parâmetro `MasterImageNote` no comando `NewProvScheme`. Por exemplo:

  ```
  C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
  <name> -IdentityPoolName <name> -MasterImageVM

  XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
  -MasterImageNote "Note"
  ```

- Para atualizar a imagem mestre associada a um catálogo de máquinas, use o parâmetro `MasterImageNote` no comando `Publish-ProvMasterVMImage`. Por exemplo:

  ```
  C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
  -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
  name>.vm\base.snapshot -MasterImageNote "Note"
  ```

- Para exibir as informações de cada imagem, use o comando Get-ProvSchemeMasterVMImageHistory. Por exemplo:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

Para acompanhar o progresso da reversão, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em certos cenários, incluindo os seguintes. (A opção **Reverter Imagem Mestra** não está visível).

- Você não tem permissão para reverter.
- O catálogo não foi criado usando o MCS.
- O catálogo foi criado usando uma imagem do disco do SO.
- O snapshot usado para criar o catálogo foi corrompido.
- As alterações do usuário nas máquinas do catálogo não persistem.
- As máquinas no catálogo estão em execução.

Redefinir disco do SO

Use o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado pelo MCS. Atualmente, este recurso é aplicável a ambientes de virtualização AWS, Azure, XenServer, Google Cloud, SCVMM e VMware.

Para executar o comando PowerShell com sucesso, certifique-se de que:

- As VMs de destino estão em um catálogo MCS persistente.
- O catálogo de máquinas MCS está funcionando corretamente.
- Isso implica que o esquema de provisionamento e o host existem, e o esquema de provisionamento tem entradas corretas.
- O hipervisor não está em modo de manutenção.
- As VMs de destino estão desligadas e em modo de manutenção.

Execute as seguintes etapas para redefinir o disco do SO:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando PowerShell `Reset-ProvVMDisk` de uma das seguintes maneiras:

- Especifique a lista de VMs como uma lista separada por vírgulas, e execute a redefinição em cada VM:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
-OS
```

- Especifique a lista de VMs como uma saída do comando `Get-ProvVM`, e execute a redefinição em cada VM:

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
-OS
```

- Especifique uma única VM pelo nome:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- Crie tarefas de redefinição separadas para cada uma das VMs retornadas pelo comando `Get-ProvVM`. Isso é menos eficiente porque cada tarefa executará as mesmas verificações redundantes, como verificação de capacidade do hipervisor, verificação de conexão para cada VM.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. Um prompt de confirmação aparece listando as VMs a serem redefinidas, juntamente com uma mensagem de aviso de que é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma outra ação será executada.

> **Nota:**
>
> Não retire as VMs do modo de manutenção nem as ligue até a conclusão do processo de redefinição.

> Você pode executar o comando PowerShell `-WhatIf` para imprimir a ação que ele executaria e sair sem realizar a ação.

Você também pode ignorar o prompt de confirmação usando um dos seguintes métodos:

- Forneça o parâmetro `-Force`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- Forneça o parâmetro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- Antes de executar o `Reset-ProvVMDisk`, altere `$ConfirmPreference` para **None**:

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. Execute `Get-ProvTask` para obter o status das tarefas retornadas pelo comando `Reset-ProvVMDisk`.

Alterar a configuração de rede para um esquema de provisionamento existente

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.

Observação:

Este recurso é compatível com Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versões posteriores.

Para alterar a configuração de rede para um esquema de provisionamento existente, faça o seguinte:

1. Na janela do PowerShell, execute o comando `asnp citrix*` para carregar os módulos do PowerShell.
2. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para acessar o caminho de rede que você deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

   ```
   $NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
   0.network"}
   ```

4. Execute `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`.
5. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar a nova configuração de rede para o esquema de provisionamento existente.

Gerenciar versões de um catálogo de máquinas

Quando um catálogo de máquinas MCS é atualizado com o comando `Set-ProvScheme`, a configuração atual é salva como uma versão. Você pode então gerenciar as várias versões do catálogo de máquinas usando comandos PowerShell. Você pode:

- Consulte a lista de versões de um catálogo de máquinas
- Use qualquer versão anterior para atualizar o catálogo de máquinas
- Exclua manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas
- Altere o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99)

Uma versão inclui as seguintes informações de um catálogo de máquinas:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Execute os seguintes comandos (fornecidos como exemplos) para gerenciar as várias versões de um catálogo de máquinas.

- Para ver os detalhes de configuração das várias versões de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Para ver os detalhes de configuração de uma versão específica de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para ver o número total de versões associadas a um catálogo de máquinas:

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- Para usar qualquer versão anterior para atualizar o catálogo de máquinas:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para excluir manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- Para definir o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99). Essa configuração é aplicada a todos os catálogos. Por exemplo, neste caso, um máximo de 15 versões será retido para todos os catálogos provisionados pelo MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

Se o número de versões atingir o número máximo de versões, uma nova versão não poderá ser criada se versões mais antigas estiverem em uso por qualquer uma das VMs no catálogo de máquinas. Nesse caso, faça uma das seguintes ações:

- Aumente o limite do número máximo de versões a serem retidas pelo catálogo de máquinas.

- Atualize algumas VMs que estão em versões mais antigas para que essas versões mais antigas não sejam mais referenciadas por nenhuma VM e possam ser excluídas.

Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina

Você pode usar uma VM, especificação de modelo (no caso do Azure) ou modelo de inicialização (no caso da AWS) 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. Novas VMs adicionadas ao catálogo assumem os valores de propriedade do perfil da máquina, a menos que sejam substituídos por uma propriedade personalizada explícita.

> **Observação:**
>
> Um catálogo de máquinas existente baseado em perfil de máquina não pode ser alterado para um catálogo de máquinas não baseado em perfil de máquina.

Para fazer isso:

1. Crie um catálogo de máquinas persistente ou não persistente com VMs e sem um perfil de máquina.
2. Abra a janela do **PowerShell**.
3. Execute o comando `Set-ProvScheme` para aplicar os valores de propriedade do perfil da máquina às novas VMs adicionadas ao catálogo de máquinas. Por exemplo:
   - No caso do Azure:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - No caso da AWS:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

Reparar as informações de identidade de contas de computador ativas

Você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

> **Nota:**
>
> Atualmente, o recurso é compatível com ambientes de virtualização AWS, GCP, Azure, XenServer e VMware.

Condições

Certifique-se do seguinte para redefinir o disco de identidade com êxito:

- Desligue e defina a VM para o modo de manutenção
- Não inclua o parâmetro -OS no comando PowerShell

Redefinir disco de identidade

Para redefinir o disco de identidade:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Redefina as informações de identidade.
   - Para redefinir apenas a senha da máquina e as chaves de confiança, execute o seguinte comando:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     A descrição dos parâmetros usados no comando é a seguinte:

     - IdentityAccountName: O nome da conta de identidade que deve ser reparada.
     - PrivilegedUserName: Conta de usuário que tem permissão de gravação no provedor de identidade (AD ou AzureAD).

- PrivilegedUserPassword: Senha para PrivilegedUserName.
- Target: Destino para a ação de reparo. Pode ser IdentityInfo para reparar a senha da conta/chave de confiança, e UserCertificate para reparar os atributos do certificado do usuário de identidades de máquina unidas ao Hybrid AzureAD.

- Para redefinir toda a configuração do disco de identidade, execute os seguintes comandos na seguinte ordem:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- Para recriar completamente o disco de identidade:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. Digite **y** para confirmar a ação. Você também pode pular o prompt de confirmação usando o parâmetro `-Force`. Por exemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. Execute `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` para verificar a configuração atualizada do disco de identidade. Os atributos do disco de identidade (por exemplo, `IdentityDiskId`) devem ser atualizados. O `StorageId` e o `IdentityDiskIndex` não devem ser alterados.

Alterar a configuração de cache em um catálogo de máquinas existente

Após criar um catálogo não persistente com MCSIO habilitado, você pode usar o comando Set-ProvScheme para modificar os seguintes parâmetros:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Este recurso é atualmente aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO ativado

Requisitos

Os requisitos para modificar a configuração do cache são:

- Atualize para a versão mais recente do VDA (2308 ou posterior).
- Habilite o parâmetro `UseWriteBackCache` para o catálogo de máquinas existente. Use `New-ProvScheme` para criar um catálogo de máquinas com `UseWriteBackCache` habilitado. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

Alterar a configuração do cache

Execute o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

Observação:

- O valor de `WriteBackCacheDiskSize` deve ser maior que zero, pois é necessário pelo menos 1 GB de armazenamento em disco de cache.
- O valor de `WriteBackCacheMemorySize` deve ser menor que o tamanho da memória do catálogo de máquinas.
- Essas alterações afetam apenas as novas VMs adicionadas ao catálogo após a alteração. As VMs existentes não são afetadas por essas alterações.

Suporte à atualização de VDA via Acesso a Compartilhamento de Arquivos Local

Especifique o local do instalador do VDA por meio de cmdlets do PowerShell, o que reduz seu esforço de fornecer regras de rede para permitir que cada VDA vá e busque o novo instalador do VDA do Citrix Managed Azure CDN.

Cmdlets do PowerShell

Dois novos parâmetros opcionais adicionados aos cmdlets **New-VusCatalogSchedule** e **New-VusMachineUpgrade** que permitem usar instaladores de um compartilhamento de arquivos local

- **VdaWorkstationPackageUri** - para especificar o caminho UNC para o instalador VDA do SO da estação de trabalho
- **VdaServerPackageUri** - para especificar o caminho UNC para o instalador VDA do SO do servidor

Pré-requisitos

- Instalador do Agente VUS que vem com o VDA 2311
- Agente de Atualização VDA para a versão 7.40.0.35 ou posterior (usando o instalador VDA versão 2311 ou posterior)
- SDK do PowerShell Remoto do Virtual Apps and Desktops versão 7.40 ou mais recente (lançado em Jan 10, 2024 ou posterior)

Como Definir Permissões de Compartilhamento de Arquivos

Os compartilhamentos de rede que contêm pacotes de instalação VDA devem ter acesso de leitura para o serviço do Agente de Atualização VDA, que é executado como Sistema Local (principal NT AUTHORITY\SYSTEM).

- **Permissão de compartilhamento de arquivos ingressado no domínio**

Quando a máquina VDA está ingressada no domínio, a conta **Sistema Local** (o VUA é executado como Sistema Local) usa credenciais de computador ao acessar compartilhamentos de rede.

A permissão de menor privilégio pode ser definida concedendo acesso de **Leitura** aos Computadores do Domínio.

a. Escolha as pessoas em sua rede com quem você deseja compartilhar o arquivo.
b. Clique em **Configurações de Compartilhamento Avançadas** e ative o **Compartilhamento de Arquivos e Impressoras**.

- **Permissão de compartilhamento de arquivos não ingressado no domínio**

Quando a máquina VDA não está ingressada no domínio, a conta **Sistema Local** (o VUA é executado como Sistema Local) usa **LOGON ANÔNIMO** ao acessar compartilhamentos de rede.

a. Selecione uma pasta compartilhada.
b. Desative a proteção por senha.
    a. Vá para **Propriedades** da Pasta.
    b. Selecione **Central de Rede e Compartilhamento**.
    c. Desative o **Compartilhamento Protegido por Senha**.
c. Clique em **Compartilhamento Avançado** para conceder uma permissão de compartilhamento.
    a. Selecione **Permissões**.
    b. Conceda uma permissão de compartilhamento de **Leitura** para **ANONYMOUS LOGON**.
d. Selecione a **Guia Segurança** para conceder permissões de pasta
    a. Clique em **Editar** para adicionar permissões à pasta compartilhada
    b. Selecione a pasta compartilhada para conceder permissões de pasta a **ANONYMOUS LOGON**.
e. Clique em **Avançado** para ativar o **Compartilhamento de Arquivos e Impressoras**.
f. Adicione o nome da pasta compartilhada à **Política de Segurança de Acesso à Rede**.

> **Observação:**
>
> Reinicie sua máquina para que a alteração entre em vigor imediatamente.

Atualizações do VDA a partir de um Compartilhamento de Arquivos Local

1. Baixe o instalador do VDA e coloque-o no arquivo compartilhado.

> **Observação:**
>
> Com o Virtual Upgrade Service, você pode selecionar entre a trilha Current Release ou a trilha LTSR.
>
> **Por Exemplo:** Se o catálogo de máquinas estiver definido como Current Release, que é 2311, e a versão do VDA for 2305, você deve atualizar o VDA para a versão 2311.

   a. navegar para a página de **Downloads** em nosso site.
   b. Selecione **Citrix Virtual Apps and Desktops** como o produto.
   c. Selecione **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
   d. Selecione o instalador do VDA na seção expansível **Components that are on product ISO but also packaged separately**.

2. Selecione o instalador do VDA relevante com base no tipo de catálogo.

   - Baixe o **instalador VDA do SO multi-sessão** se o tipo de catálogo for **multi-sessão**
   - Baixe o **instalador VDA do SO de sessão única** se o tipo de catálogo for **sessão única**
   - Baixe o **instalador VDA de Serviços Principais do SO de sessão única** se o tipo de catálogo for **Acesso Remoto a PC**

> **Observação:**
>
> A versão do instalador de compartilhamento de arquivos deve corresponder **exatamente** à versão do instalador mais recente publicada pelo VUS na nuvem.

Solução de problemas

- Para máquinas com status "Power State Unknown", consulte CTX131267 para obter orientação.
- Para corrigir VMs que exibem continuamente um estado de energia desconhecido, consulte Como corrigir VMs que exibem continuamente um estado de energia desconhecido.

Onde ir em seguida

Para obter informações sobre como gerenciar catálogos de serviços de nuvem específicos, consulte:

- Gerenciar um catálogo AWS
- Gerenciar um catálogo do XenServer
- Gerenciar um catálogo do Google Cloud Platform
- Gerenciar um catálogo do Microsoft Azure
- Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager
- Gerenciar um catálogo do VMware

Gerenciar um catálogo AWS

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem AWS.

> **Observação:**
>
> Antes de gerenciar um catálogo AWS, você precisa terminar de criar um catálogo AWS. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-aws.html).

Remover tags

Ao criar um catálogo ou uma VM, as tags criadas pelo MCS são criadas nos seguintes recursos:

- Máquina virtual
- Volume do disco raiz
- Volume do disco de identidade

- NIC
- Imagem do disco raiz (AMI)
- Modelo de inicialização
- Snapshot da AMI ou do disco raiz

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix® e remover as tags criadas pelo MCS. Você pode usar:

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

Este recurso é aplicável apenas a VMs persistentes.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Desbloqueie a VM antes de remover as VMs. Por exemplo:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. Execute um dos seguintes comandos para remover VMs, catálogo de máquinas e tags criadas pelo MCS 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
     ```

   - Execute `Remove-ProvScheme` para remover o catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas. Por exemplo:

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. Verifique se a VM foi removida do Delivery Controller™, mas não do hipervisor.

a. Execute `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. Isso não deve retornar nada.

b. Vá para o console AWS EC2. Você deve ver as VMs, no entanto, as tags 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 do AWS EC2 se os seguintes recursos foram removidos.

- Imagem do disco raiz (AMI)
- Modelo de inicialização
- Snapshot da AMI ou do disco raiz

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"Name": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagem	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOME DO RECURSO	TAG
NIC	"Descrição": "XD NIC"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"Name": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Recurso Citrix": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "RecursoOperacionalCitrix": ""
PrepVM	"Nome": "Preparação - Nome do Catálogo - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Recurso Citrix": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
Instantâneo publicado	"XdConfig": "XdProvisioned=true"
	Se não for um snapshot para Volume Worker AMI, então "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOME DO RECURSO	TAG
Modelo	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
VM no catálogo	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
AMI de trabalho de volume	"XdConfig": "XdProvisioned=true"
Bootstrapper do worker de volume	"Nome": "XenDesktop® Temp"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOME DO RECURSO	TAG
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
Instância do worker de volume	"Nome": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"XdConfig": "XdProvisioned=true"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com AWS
- Criar catálogos de máquinas
- Criar um catálogo AWS
- Gerenciar catálogos de máquinas

Gerenciar um catálogo XenServer®

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização XenServer.

> **Nota:**
>
> Antes de gerenciar um catálogo XenServer, você precisa terminar de criar um catálogo XenServer. Consulte Criar um catálogo XenServer.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	TAG
Disco base publicado e sua cópia em cada rede ou armazenamento local	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOME DO RECURSO	TAG
Disco de ID	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM de preparação	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM no catálogo	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco WBC	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com XenServer
- Criar catálogos de máquinas
- Criar um catálogo do XenServer
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Google Cloud Platform

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos de ambientes de nuvem do Google.

> **Observação:**
>
> Antes de gerenciar um catálogo do Google Cloud Platform, você precisa concluir a criação de um catálogo do Google Cloud Platform. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html).

Gerenciar catálogo de máquinas

Para adicionar máquinas a um catálogo, atualizar máquinas e reverter uma atualização, consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html).

Gerenciamento de energia

O Citrix DaaS™ permite o gerenciamento de energia de máquinas do Google Cloud. Use o nó **Pesquisar** no painel esquerdo para localizar a máquina que você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Excluir
- Iniciar
- Reiniciar
- Reinicialização Forçada
- Desligar
- Desligamento Forçado
- Adicionar ao Grupo de Entrega
- Gerenciar Tags
- Ativar Modo de Manutenção

Você também pode gerenciar a energia das máquinas do Google Cloud usando o Autoscale. Para fazer isso, adicione as máquinas do Google Cloud a um Grupo de Entrega e, em seguida, habilite o Autoscale para esse Grupo de Entrega. Para obter mais informações sobre o Autoscale, consulte (/pt-br/citrix-daas/manage-deployment/autoscale.html).

Atualizar máquinas provisionadas usando PowerShell

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, agora você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas existente, persistente ou não persistente. 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
   ```

2. Atualize o esquema de provisionamento. Por exemplo,

   ```
   `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
   "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
   ```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. Atualizar máquinas existentes.

   - Para atualizar todas as máquinas existentes:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar uma lista de máquinas específicas:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar máquinas com base na saída de `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. Reinicie as máquinas. Na próxima inicialização, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Alterar propriedades personalizadas relacionadas ao disco de um catálogo existente

Você pode alterar as seguintes propriedades personalizadas relacionadas ao disco de um catálogo existente e de VMs existentes do catálogo:

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

Observação:

- A propriedade `StorageType` é para o disco do SO
- A propriedade `PersistOsDisk` pode ser definida apenas para catálogos não persistentes com cache de write-back ativado

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

Para fazer isso, use os comandos PowerShell `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute `Get-ProvVM -VMName <VM name>` para obter as propriedades personalizadas.
4. Altere a string de propriedades personalizadas:
   a. Copie as propriedades personalizadas para um Bloco de Notas e altere as propriedades personalizadas.
   b. Na janela do **PowerShell**, cole as propriedades personalizadas modificadas do Bloco de Notas e atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. Atualize o catálogo existente. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. Atualize as VMs existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. Reinicie as VMs. Na próxima inicialização, as alterações de propriedade personalizadas são aplicadas às VMs existentes.

Proteger exclusão acidental de máquina

O Citrix DaaS permite proteger os recursos do MCS no Google Cloud para evitar exclusões acidentais. Configure a VM provisionada definindo o sinalizador `deletionProtection` como TRUE.

Por padrão, as VMs provisionadas através do MCS ou do plug-in do Google Cloud são criadas com a Proteção de Instância ativada. A implementação é aplicável a catálogos persistentes e não persistentes. Os catálogos não persistentes são atualizados quando as instâncias são recriadas a partir do modelo. Para máquinas persistentes existentes, você pode definir o sinalizador no console do Google Cloud. Para obter mais informações sobre como definir o sinalizador, consulte o site de Documentação do Google. Novas máquinas adicionadas a catálogos persistentes são criadas com `deletionProtection` ativado.

Se você tentar excluir uma instância de VM para a qual definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você tiver a permissão `compute.instances.setDeletionProtection` ou for atribuído à função IAM de **Administrador de Computação**, 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. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"CitrixResource": "interno"

NOME DO RECURSO	TAG
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagem	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Instantâneo publicado	"CitrixResource": "interno"
Bucket de armazenamento	"Citrixresource": "interno"
Modelo	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM no catálogo	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". O plug-in também adiciona este rótulo para VMs provisionadas pelo MCS: "citrix-provisioning-scheme-id": "provSchemeId". Você pode usar este rótulo para filtrar por catálogo no console do GCP.
Disco WBC	"CitrixResource": "interno"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Observação:

Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas
- Criar um catálogo Google Cloud Platform
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Microsoft Azure

Nota:

Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência a Azure Active Directory, Azure AD ou AAD agora se refere a Microsoft Entra ID.

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

Nota:

Antes de gerenciar um catálogo do Microsoft Azure, você precisa concluir a criação de um catálogo do Microsoft Azure. Consulte Criar um catálogo do Microsoft Azure.

Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada

Você pode economizar custos de armazenamento alterando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade personalizada `StorageTypeAtShutdown`.

O tipo de armazenamento do disco muda para um nível inferior (conforme especificado na propriedade personalizada `StorageTypeAtShutdown`) quando você desliga a VM. Depois de ligar a VM, o tipo de armazenamento volta ao original (conforme especificado na propriedade personalizada `StorageType` ou na propriedade personalizada `WBCDiskStorageType`).

> **Importante:**
>
> O disco não existe até que a VM seja ligada pelo menos uma vez. Portanto, você não pode alterar o tipo de armazenamento ao ligar a VM pela primeira vez.

Requisitos

- Aplicável a um disco gerenciado. Isso implica que você define a propriedade personalizada `UseManagedDisks` como true.
- Aplicável a um catálogo persistente e não persistente com um disco de SO persistente. Isso implica que você define a propriedade personalizada `persistOsDisk` como true.
- Aplicável a um catálogo não persistente com um disco WBC persistente. Isso implica que você define a propriedade personalizada `persistWBC` como true.

Restrição

- De acordo com a Microsoft, você só pode alterar o tipo de disco duas vezes por dia. Consulte o documento da Microsoft. De acordo com a Citrix, a atualização `StorageType` ocorre sempre que há uma ação de Iniciar ou Desalocar para a VM. Portanto, limite o número de ações de energia por VM a duas por dia. Por exemplo, uma ação de energia pela manhã para iniciar a VM e uma à noite para desalocar a VM.

Alterar o tipo de armazenamento para um nível inferior

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

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 falha.

Exemplo de configuração de propriedades personalizadas ao criar um catálogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

Exemplo de configuração de propriedades personalizadas ao criar um catálogo não persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

Nota:

Ao usar um perfil de máquina, a propriedade personalizada tem precedência sobre a propriedade definida em `MachineProfile`.

2. Desligue a VM e verifique o tipo de armazenamento da VM no portal do Azure. O tipo de armazenamento do disco muda para um nível inferior, conforme especificado na propriedade personalizada `StorageTypeAtShutdown`.

3. Ligue a VM. O tipo de armazenamento do disco volta para o tipo de armazenamento mencionado em:
    - propriedade personalizada `StorageType` para disco do SO
    - propriedade personalizada `WBCDiskStorageType` para disco WBC somente se você especificá-lo em `CustomProperties`. Caso contrário, ele volta para o tipo de armazenamento mencionado em `StorageType`.

Aplicar `StorageTypeAtShutdown` a um catálogo existente

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

Use `Set-ProvScheme` para adicionar uma VM a um catálogo existente. O recurso se aplica a novas VMs adicionadas após a execução de `Set-ProvScheme`. As máquinas existentes não são afetadas.

Exemplo de como definir propriedades personalizadas ao adicionar uma VM a um catálogo existente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
```

```
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

Altere o tipo de armazenamento de VMs existentes para um nível inferior no desligamento

Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

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 alterar o tipo de armazenamento de máquinas existentes em um catálogo para um nível inferior quando as VMs são desligadas:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Altere a string de propriedades personalizadas.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. Atualize o esquema de provisionamento do catálogo existente. A atualização se aplica a novas VMs adicionadas após a execução de `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. Atualize as VMs existentes para habilitar `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. Na próxima vez que você ligar as máquinas, a propriedade `StorageTypeAtShutdown` das máquinas será atualizada. O tipo de armazenamento muda no próximo desligamento.
8. Execute o seguinte comando para visualizar o valor `StorageTypeAtShutdown` para cada VM em um catálogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, você pode aplicar o esquema de provisionamento atual a uma máquina persistente ou não persistente existente ou a um conjunto de máquinas. Você também pode agendar um período de tempo para as atualizações de configuração das máquinas provisionadas pelo MCS existentes. Qualquer inicialização ou reinicialização durante o período de tempo agendado aplica uma atualização de esquema de provisionamento agendada a uma máquina. Atualmente, no Azure, você pode atualizar `ServiceOffering`, `MachineProfile` e as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Nota:

- Você só pode atualizar as propriedades personalizadas `StorageType`, `WBCDiskStorageType` e `IdentityDiskStorageType` para um catálogo usando disco gerenciado em ambientes Azure.
- Se você executar `Set-ProvVMUpdateTimeWindow` duas vezes, o comando mais recente terá efeito.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento (nome do catálogo de máquinas)

Depois de fazer as seguintes alterações no esquema de provisionamento, a instância da VM é recriada para catálogos persistentes no Azure:

- Alterar o `MachineProfile`
- Remover `LicenseType`
- Remover `DedicatedHostGroupId`

Nota:

O disco do SO das máquinas existentes, juntamente com todos os seus dados, permanece como está e uma nova VM é anexada ao disco.

> Antes de atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. Atualize o esquema de provisionamento. Por exemplo,

   - Com a VM como entrada de perfil de máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
group>.resourcegroup\<virtual-machine>.vm"
```

   - Com a especificação de modelo como entrada de perfil de máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

   - Apenas com a oferta de serviço:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

Para solicitar atualizações para máquinas existentes que serão aplicadas na próxima reinicialização:

1. Execute os seguintes comandos para atualizar as máquinas existentes e fazer com que as atualizações sejam aplicadas na próxima reinicialização.
   - Para atualizar todas as máquinas existentes. Por exemplo,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar uma lista de máquinas específicas. Por exemplo,

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar máquinas com base na saída de Get-ProvVM. Por exemplo,

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

Nota:

- `StartsNow` indica que a hora de início agendada é a hora atual.
- `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Reinicie as máquinas. No próximo ligamento, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Para agendar uma VM para atualizar para as configurações de provisionamento mais recentes na próxima vez que ela iniciar na janela de tempo agendada:

1. Execute os seguintes comandos:

   - Para agendar uma atualização com a hora de início como a hora atual

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

   - Para agendar uma atualização em um fim de semana

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

Nota:

- `VMName` é opcional. Se não for especificado, a atualização é agendada para todo o catálogo.
- Em vez de `StartTimeInUTC`, use `StartsNow` para indicar que a hora de início do agendamento é a hora atual.
- `DurationInMinutes` é opcional. O padrão é 120 minutos. Um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Verifique o status da atualização.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. Ligue a VM. Se você ligar a máquina após o período agendado, a atualização da configuração não será aplicada. Se você ligar a máquina dentro do período agendado,
    - Se a máquina estiver desligada e
        - se você não ligar a máquina, a atualização de configuração não será aplicada
        - se você ligar a máquina, a atualização de configuração será aplicada
    - Se a máquina estiver ligada e
        - você não reinicia a máquina, a atualização de configuração não é aplicada
        - você reinicia a máquina, a atualização de configuração é aplicada

Para cancelar a atualização da configuração:

Você também pode cancelar uma atualização de configuração de uma única VM, de várias VMs ou de um catálogo inteiro. Para cancelar uma atualização de configuração:

1. Execute `Clear-ProvVMUpdateTimeWindow`. Por exemplo:
    - Para cancelar a atualização da configuração agendada para uma única VM:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
    -VMName “vm1”
    ```

    - Para cancelar a atualização da configuração agendada para várias VMs:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
    -VMName "vm1","vm2"
    ```

    Nota:

    As VMs devem ser do mesmo catálogo.

Atualizar propriedades de VMs individuais

Você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistente usando o comando PowerShell `Set-ProvVM`. No entanto, as atualizações não são aplicadas imediatamente. Você deve definir a janela de tempo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow` para que as atualizações sejam aplicadas.

Esta implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, este recurso é aplicável apenas ao ambiente Azure.

Atualmente, as propriedades que você pode atualizar são:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Usando este recurso, você pode:

- Atualizar as propriedades de uma VM
- Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas
- Reverter as atualizações de configuração aplicadas a uma VM

Antes de atualizar as propriedades de uma VM:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Verifique a configuração do catálogo de máquinas existente. Por exemplo:

   ```
   Get-ProvScheme -ProvisioningSchemeName AzureCatalog
   ```

4. Verifique a configuração da VM na qual você deseja aplicar as atualizações. Por exemplo:

   ```
   Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
   ```

Atualizar propriedades de uma VM

Faça o seguinte para atualizar as propriedades em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.

2. Atualize as propriedades da VM. Por exemplo, se você quiser atualizar a propriedade personalizada do tipo de armazenamento (`StorageType`) da VM, execute o seguinte:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

   Você pode atualizar as propriedades de duas VMs em um catálogo de máquinas simultaneamente. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

   Observação:

   As atualizações não são aplicadas imediatamente.

3. Obtenha a lista de propriedades que devem ser atualizadas e a versão da configuração. Por exemplo:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

   Verifique o valor da propriedade de `Version` e as propriedades a serem atualizadas (neste caso, `StorageType`).

4. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização ainda não foi aplicada. A VM ainda está na configuração antiga.

5. Solicite a atualização agendada. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

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

> **Observação:**
>
> Qualquer atualização pendente do esquema de provisionamento também é aplicada.

6. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização agora foi aplicada. A VM agora tem a nova configuração.

8. Para aplicar mais atualizações de configuração na VM, desligue a VM e repita os passos.

Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas

Faça o seguinte para manter as propriedades atualizadas em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.
2. Atualize o catálogo de máquinas. Por exemplo, se você quiser alterar o tamanho da VM (`ServiceOffering`) e o tipo de armazenamento (`StorageType`), execute o seguinte:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. Obtenha os detalhes de configuração do catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

O `ProvisioningSchemeVersion` agora é incrementado em um. O tamanho da VM e o tipo de armazenamento também são atualizados.

4. Atualize as propriedades da VM. Por exemplo, forneça um perfil de máquina para a VM.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

Observação:

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
```

Observação:

Quaisquer atualizações na VM substituirão as atualizações feitas no catálogo de máquinas.

6. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

A VM mantém seu tamanho de VM atualizado conforme derivado do perfil da máquina. Os valores de tag especificados no perfil da máquina também são aplicados à VM. No entanto, o tipo de armazenamento é derivado do esquema de provisionamento mais recente.

8. Obtenha a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

O `ProvisioningSchemeVersion` e o `ProvVMConfigurationVersion` agora mostram a versão mais recente.

Reverter as atualizações de configuração aplicadas a uma VM

1. Após aplicar as atualizações a uma VM, desligue a VM.
2. Execute o seguinte comando para remover as atualizações aplicadas na VM. Por exemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Verifique a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

O valor `ProvVMConfigurationVersion` agora é a versão de configuração do catálogo de máquinas.

Alterar criptografia de disco

Você pode alterar a criptografia de disco em ambientes de virtualização do Azure e fazer o seguinte:

- Crie um catálogo de máquinas MCS com conjunto de criptografia de disco (DES) que seja diferente do DES da imagem mestre usando o comando `New-ProvScheme`. Por exemplo:

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- Altere o tipo de criptografia de disco de uma chave DES para outra chave DES de um catálogo de máquinas MCS existente e VMs existentes usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Depois de reiniciar as VMs, você poderá ver a chave DES atualizada. Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Atualize um catálogo de máquinas MCS e uma VM que não estava anteriormente habilitada para CMEK para ter criptografia de chave de criptografia gerenciada pelo cliente (CMEK) (DES), criptografia de disco no host ou criptografia dupla usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Para obter informações sobre os diferentes tipos de criptografia, consulte Criptografia do lado do servidor do Azure, Criptografia de disco do Azure no host e Criptografia dupla em disco gerenciado.
- Atualize um catálogo de máquinas MCS e VMs existentes para não serem criptografados, que foram criptografados anteriormente usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Habilitar criptografia de disco com endpoint privado (um catálogo de máquinas MCS que usou uma conexão de host habilitada com `ProxyHypervisorTrafficThroughConnector`). Para obter informações sobre como habilitar a criptografia de disco com endpoints privados, consulte Habilitar criptografia de disco com endpoint privado.

Habilitar criptografia de disco com ponto de extremidade privado

De acordo com a limitação do Azure, atualmente, você não pode ter criptografia do lado do servidor com chaves gerenciadas pelo cliente para pontos de extremidade privados. No entanto, você pode atualizar um catálogo de máquinas MCS existente e VMs com pontos de extremidade privados para serem criptografados com a chave DES.

ATUALIZAR UM CATÁLOGO DE MÁQUINAS EXISTENTE COM PONTOS DE EXTREMIDADE PRIVADOS

As etapas detalhadas para atualizar um catálogo de máquinas existente com pontos de extremidade privados são as seguintes:

1. Crie um catálogo sem criptografia de disco através de `ProxyHypervisorTrafficThroughConnector`.
2. Execute `Set-ProvScheme` para atualizar o catálogo com `DiskEncryptionSetId`.

> **Nota:**
>
> `DiskEcryptionSetId` pode ser configurado através de `CustomProperties` ou `MachineProfile`. Quando definido em `CustomProperties` e `MachineProfile`, as propriedades definidas em `CustomProperties` são aplicadas.

> Exemplo ao usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
```

```
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

Exemplo ao usar MachineProfile: Use uma VM com criptografia de disco ativada ou uma especificação de modelo com configurações de criptografia de disco:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

Alternativamente, você pode atualizar um perfil de máquina usando o Web Studio.

3. Execute `Set-ProvVMUpdateTimeWindow` para atualizar as VMs de catálogo existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. Após reiniciar as VMs, você pode ver a criptografia de disco atualizada nos discos da VM no portal do Azure.
5. Execute `Set-ProvScheme` para desativar a criptografia de disco antes de adicionar novas VMs de catálogo.

> **Nota:**
>
> Esta etapa é necessária porque você está atualizando um catálogo de endpoint privado. Se você não realizar esta etapa, receberá erros ao tentar adicionar novas VMs ao catálogo.
>
> Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. Adicione novas VMs ao catálogo.

ATUALIZAR VMS DE CATÁLOGO INDIVIDUAIS

As etapas detalhadas para atualizar VMs de catálogo individuais são as seguintes:

1. Crie um catálogo sem criptografia de disco através de `ProxyHypervisorTrafficThroughConnector`.
2. Execute `Set-ProvVM` para atualizar a VM do catálogo com `DiskEncryptionSetId`.

> **Nota:**
>
> O `DiskEcryptionSetId` pode ser configurado por meio de `CustomProperties` ou `MachineProfile`.
>
> Exemplo ao usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'
```

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

Exemplo ao usar MachineProfile:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. Execute `Set-ProvVMUpdateTimeWindow` para atualizar as VMs do catálogo existente. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. Depois de reiniciar as VMs, você pode ver a criptografia de disco atualizada nos discos das VMs no portal do Azure.
5. Adicione novas VMs ao catálogo.

Recuperar informações para VMs do Azure, snapshots, disco do SO e definição de imagem da galeria

Você pode exibir informações para uma VM do Azure, incluindo disco e tipo de SO, snapshot e definição de imagem da galeria. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Use esta funcionalidade para visualizar e selecionar uma imagem Linux ou Windows. Uma propriedade do PowerShell, `TemplateIsWindowsTemplate`, foi adicionada ao parâmetro `AdditionDatafield`. Este campo contém informações específicas do Azure: tipo de VM, disco do SO, informações da imagem da galeria e informações do tipo de SO. Definir `TemplateIsWindowsTemplate` como **True** indica que o tipo de SO é Windows; definir `TemplateIsWindowsTemplate` como **False** indica que o tipo de SO é Linux.

> **Dica:**

> As informações exibidas pela propriedade PowerShell `TemplateIsWindowsTemplate` são derivadas da API do Azure. Às vezes, este campo pode estar vazio. Por exemplo, um

snapshot de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de SO não pode ser recuperado de um snapshot.

Por exemplo, defina o parâmetro `AdditionData` da VM do Azure como **True** para o tipo de SO Windows usando o PowerShell:

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	TAG
Disco de ID	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

NOME DO RECURSO	TAG
Imagem	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
NIC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Disco do SO	"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"
Grupo de recursos	"CitrixResource" : "Internal"
	CitrixSchemaVersion: 2.0
	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Conta de armazenamento	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
VM no catálogo	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

NOME DO RECURSO	TAG
Disco WBC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

Nota:

Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Remover tags

Ao criar um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Grupo de recursos
- Máquina virtual
- Disco do SO
- Disco de identidade
- Interface de rede
- Conta de armazenamento

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix e remover tags. Você pode usar:

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

Este recurso é aplicável apenas a VMs persistentes.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.

3. Execute `Remove-ProvVM` para excluir VMs do banco de dados Citrix e tags de VMs. Por exemplo:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. Execute `Remove-ProvScheme` para excluir o catálogo de máquinas do banco de dados Citrix e tags dos catálogos de máquinas. Por exemplo:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
```

> **Nota:**
>
> Depois de usar o parâmetro `ForgetVM` em `Remove-ProvScheme`, o MCS exclui todos os instantâneos, incluindo o instantâneo do disco base, se o esquema de provisionamento estiver presente em um grupo de recursos próprio (BYORG) ou em um grupo de recursos gerenciado pela Citrix.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure
- Criar catálogos de máquinas
- Criar um catálogo do Microsoft Azure
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

> **Observação:**

> Antes de gerenciar um catálogo VMM, você precisa concluir a criação de um catálogo VMM. Consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	TAG
VM de Preparação	String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True"
VM no catálogo	String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas
- Criar um catálogo Microsoft System Center Virtual Machine Manager
- Gerenciar catálogos de máquinas

Gerenciar um catálogo VMware

(/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage.html) descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

> **Observação:**

> Antes de gerenciar um catálogo VMware, você precisa terminar de criar um catálogo VMware. Consulte (/pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html).

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 sob este novo ID de pasta. Se esta propriedade não for especificada em `CustomProperties`, as VMs serão criadas na pasta onde a imagem mestre está localizada.

Execute as seguintes etapas para atualizar o ID da pasta de um catálogo de máquinas.

1. Abra um navegador da Web e insira o URL para o **vSphere Web Client**.
2. Insira as credenciais e clique em **Login**.
3. Crie uma pasta de posicionamento de VM no **vSphere Web Client**.
4. Abra uma janela do PowerShell.
5. Execute **asnp citrix®*** para carregar os módulos PowerShell específicos da Citrix.
6. Especifique o `FolderID` no `CustomProperties` de `Set-ProvScheme`. Neste exemplo, o valor do ID da pasta é `group-v2406`.

   ```
   Set-ProvScheme -ProvisioningSchemeUid
   "50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
   "<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
   machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
   instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
   Value=""group-v2406"" /></CustomProperties>"
   ```

7. Adicione uma VM ao catálogo de máquinas usando o Studio.
8. Verifique a nova VM no vSphere Web Client. A nova VM é criada na nova pasta.

Encontrar o ID da pasta no vSphere

Acesse o Managed Object Browser (MOB) em qualquer sistema de servidor ESXi ou vCenter para encontrar o ID da pasta das VMs.

O MOB é um aplicativo de servidor baseado na web disponível embutido em todos os sistemas de servidor ESX/ESXi e vCenter. Este utilitário vSphere permite visualizar informações detalhadas sobre objetos como VMs, datastores e pools de recursos.

1. Abra um navegador da web e digite `http://x.x.x.x/mob`, onde x.x.x.x é o endereço IP do vCenter Server ou host ESX/ESXi. Por exemplo, `<https://10.60.4.70/mob>`.
2. Na página **Home** do MOB, clique no valor da propriedade **content**.
3. Clique no valor de **rootFolder**.
4. Clique no valor de **childEntity**.
5. Clique no valor de **vmFolder**.
6. Você pode encontrar o ID da pasta no valor de **childEntity**.

Migração de armazenamento de VMs

Você pode mover o armazenamento em disco de VMs existentes de um armazenamento antigo para um novo armazenamento. Durante a migração, o MCS retém os recursos da VM, como gerenciamento de energia, redefinição do disco do SO e assim por diante. Você também pode adicionar novas VMs ao catálogo de máquinas usando o novo armazenamento em disco. Para fazer isso, use o comando PowerShell `Move-ProvVMDisk`.

Atualmente, você só pode migrar VMs persistentes de clone completo.

O novo armazenamento deve satisfazer as seguintes condições:

- Deve estar dentro do mesmo cluster do armazenamento antigo.
- O host no qual a VM está sendo executada deve ter acesso aos datastores antigo e novo.

Você pode realizar as seguintes tarefas:

- Migrar o armazenamento em disco
- Descontinuar o armazenamento antigo

Migrar o armazenamento em disco

Para migrar o armazenamento em disco:

1. Adicione um novo armazenamento a uma unidade de hospedagem existente. Altere o armazenamento antigo para **Substituído**. Você pode fazer isso usando o Web Studio ou comandos do PowerShell.
    - Se estiver usando o Web Studio, consulte Editar armazenamento.

- Se estiver usando comandos do PowerShell:
  - Execute `Add-Hyphostingunitstorage` para adicionar o novo armazenamento à unidade de hospedagem existente.
  - Execute `Set-Hyphostingunitstorage` com **Superseded** como true para desabilitar a criação de novas VMs no armazenamento antigo.

2. Desligue as VMs e ative o **Modo de Manutenção**.
3. Mova o armazenamento em disco das VMs para o novo armazenamento e atualize as informações de armazenamento. Por exemplo:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. Obtenha o ID da tarefa da migração. Por exemplo:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. Verifique o status da migração.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: Fornece a lista de VMs com migração de disco bem-sucedida, incluindo as VMs que já foram migradas para o novo armazenamento.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: Fornece a lista de VMs com migração falha.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: Fornece a lista de VMs cuja migração ainda não começou.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: Fornece as propriedades atualizadas da VM após a migração. Verifique as propriedades como `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` e `LastBootTime`.

Após migrar os discos de VMs criadas pelo MCS com snapshot, você pode ver o aviso **Consolidation is required in the VSphere Client**. Para consolidar e evitar perda de dados:

1. Faça um backup da VM VMware. Por exemplo, transfira todos os arquivos da VM para outra pasta em um datastore.
2. Depois de ver o aviso, clique em **Consolidate** e, em seguida, clique em **OK** para confirmar a consolidação.

Descontinuar o armazenamento antigo

Para descontinuar o armazenamento antigo após a migração de disco das VMs:

1. Obtenha as informações sobre os discos base e a contagem de máquinas em cada armazenamento de disco da unidade de hospedagem. Por exemplo:

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

   $result

   $result.ProvResourceInStorage | Format-List -Property *
   ```

   Após uma migração bem-sucedida, o MCS remove automaticamente o disco base obsoleto e não há máquinas no armazenamento antigo. Portanto, após executar o comando, certifique-se de que não há máquinas e disco base no armazenamento antigo.
2. Execute `Remove-Hyphostingunitstorage` para remover completamente o armazenamento antigo da unidade de hospedagem. Você também pode usar o Web Studio para remover o armazenamento antigo.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
VM de Preparação	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"
VM no catálogo	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Criar catálogos de máquinas
- Criar um catálogo VMware
- Gerenciar catálogos de máquinas

Gerenciamento de Energia

Com o Citrix Virtual Apps and Desktops™, você pode gerenciar o consumo de energia de VMs provisionadas por MCS em vários hipervisores e serviços de nuvem compatíveis. A operação de gerenciamento de energia oferece a você:

- Experiência ideal do usuário
- Gerenciamento de custos e economia de energia

As ações de energia disponíveis são:

- Iniciar
- Desligar
- Reiniciar
- Suspender
- Retomar
- Forçar reinício
- Desligamento forçado

> **Observação:**
>
> - Para uma VM não persistente, o ciclo de energia (desligar/iniciar e reiniciar) resulta na redefinição do disco do SO.
> - As capacidades e comportamentos das ações de energia variam dependendo de hipervisores ou serviços de nuvem.

> O artigo aborda os principais recursos de gerenciamento de energia associados a certos hipervisores compatíveis.

- Gerenciar o consumo de energia de VMs AWS
- Gerenciar o consumo de energia de VMs Azure

Gerenciar energia de VMs AWS

Para obter informações sobre as permissões necessárias, consulte Permissões AWS necessárias.

Hibernação de Instância

O processo de hibernação armazena o estado em memória da instância, juntamente com seus endereços IP privados e elásticos, permitindo que ela retome exatamente de onde parou.

Quando uma instância é instruída a hibernar, ela grava o estado em memória em um arquivo no volume EBS raiz e, em seguida, se desliga. Um volume Amazon EBS é um dispositivo de armazenamento durável, em nível de bloco, que você pode anexar às suas instâncias. Depois de anexar um volume a uma instância, você pode usá-lo como usaria um disco rígido físico. Criptografe o volume EBS raiz da instância. A criptografia garante a proteção adequada para dados confidenciais quando são copiados da memória para o volume EBS. Para obter informações sobre a criptografia EBS, consulte Criptografia Amazon EBS.

A seguir estão as limitações da hibernação de instância suportada:

- Memória da instância (RAM) de apenas até 150 GB é suportada
- O modo de inicialização UEFI não é suportado
- Os SSDs de uso geral e os SSDs de IOPS provisionadas são suportados apenas como tipos de volume EBS.

Criar VMs com suporte a hibernação

Para criar VMs com suporte a hibernação:

1. Crie uma conexão de host. Consulte Conexão com a AWS.
2. Inicie uma instância com o root EBS criptografado e a propriedade **Stop-Hibernate** habilitada. Para obter mais informações sobre como iniciar a instância, criptografar o volume EBS raiz e habilitar a hibernação, consulte `<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`. Use esta instância como uma imagem mestre para criar uma AMI.
3. Prepare a imagem mestre:

a. Instale um VDA na imagem mestre. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe. Para obter mais informações sobre como instalar um VDA, consulte Instalar VDAs.

b. Una a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas.

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 AWS no Web Studio, consulte **Aplicando propriedades da instância AWS e marcando recursos operacionais no Web Studio**.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

Para obter informações sobre como criar um catálogo de máquinas usando comandos PowerShell, consulte `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>`.

As VMs que podem ser hibernadas são criadas se:

- Você selecionar uma AMI criada a partir de uma imagem mestre que tenha a propriedade **Stop-Hibernate** habilitada.
- A VM mestre estiver unida ao domínio e tiver o VDA instalado.

- Você seleciona o tamanho correto da VM (oferta de serviço) que pode manipular a hibernação.

O comando **New-ProvScheme** falha com uma mensagem de erro apropriada se:

- A VM mestre está habilitada para hibernação, mas a oferta de serviço não é capaz de lidar com a hibernação.
- Se a VM mestre não estiver ingressada no domínio e não tiver nenhum VDA instalado.

Status de hibernação de ofertas de serviço e AMI

Para obter o status de hibernação das ofertas de serviço e AMI (modelos), execute os seguintes comandos:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

Atualizar oferta de serviço de um esquema de provisionamento existente com suporte a hibernação

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

O sistema exibe uma mensagem de exceção se a oferta de serviço não for compatível.

Criar catálogo de máquinas com suporte a hibernação

Ao criar catálogos de máquinas, você pode usar um perfil de máquina que suporte hibernação.

1. No assistente de criação de catálogo, siga as instruções até a seleção do perfil da máquina.
2. Na página **Modelo de Máquina**, clique em **Selecionar um perfil de máquina** e selecione um perfil de máquina.
3. Na página **Máquina Virtual**, clique no ícone **Editar** e selecione uma VM.

> **Nota:**

> Se o perfil da máquina estiver habilitado para hibernação, o sistema exibirá apenas as VMs que podem ser hibernadas.

4. Siga as instruções na tela para concluir todas as configurações. A página **Resumo** exibe o status de hibernação do catálogo.

> **Nota:**
>
> Ao editar o catálogo de máquinas, quando você altera o perfil da máquina para um habilitado para hibernação, será solicitado que você reconfigure suas VMs de acordo.

Atualizar catálogo de máquinas que suporta hibernação

Se você tentar atualizar um catálogo de máquinas existente com um catálogo de máquinas que não suporta hibernação, a atualização falhará com uma mensagem de erro apropriada.

Gerenciamento de energia de VMs hibernadas

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs hibernadas:

1. Suspender a VM do estado de execução.
2. Retomar a VM do estado suspenso.
3. Reiniciar a VM do estado suspenso.

Gerenciar energia de VMs do Azure

Para obter informações sobre as permissões necessárias, consulte Permissões do Azure necessárias.

Provisionamento sob demanda do Azure

Com o provisionamento sob demanda do Azure, as VMs são criadas apenas quando o Citrix Virtual Apps and Desktops™ inicia uma ação de ligar, após a conclusão do provisionamento.

Ao usar o MCS para criar catálogos de máquinas no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz seus custos de armazenamento
- Oferece criação de catálogo mais rápida

Ao criar um catálogo MCS, o portal do Azure exibe os grupos de segurança de rede, interfaces de rede, imagens base e discos de identidade nos grupos de recursos.

O portal do Azure não mostra uma VM até que o Citrix Virtual Apps and Desktops inicie uma ação de ligar para ela. Existem dois tipos de máquinas com as seguintes diferenças:

- Para uma máquina agrupada, o disco do sistema operacional e o cache de write-back existem apenas quando a VM existe. Ao desligar uma máquina agrupada no console, a VM não fica visível no portal do Azure. Há uma economia significativa de custos de armazenamento se você desligar as máquinas rotineiramente (por exemplo, fora do horário de trabalho).
- Para uma máquina dedicada, o disco do sistema operacional é criado na primeira vez que a VM é ligada. A VM no portal do Azure permanece em armazenamento até que a identidade da máquina seja excluída. Ao desligar uma máquina dedicada no console, a VM ainda fica visível no portal do Azure.

Nota:

O suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos “legados”) foi descontinuado. Portanto, recrie as VMs de catálogo legadas do Azure. Os catálogos são então provisionados sob demanda, o que economiza custos de armazenamento.

Preservar uma máquina virtual provisionada ao reiniciar

Escolha se deseja preservar uma máquina virtual provisionada ao reiniciar. Use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provisionada persiste quando reiniciada. Defina a propriedade `PersistVm` como **true** para manter uma máquina virtual quando desligada, ou defina a propriedade como **false** para garantir que a máquina virtual não seja preservada quando desligada.

Observação:

A propriedade `PersistVm` se aplica apenas a um esquema de provisionamento com as propriedades `CleanOnBoot` e `UseWriteBackCache` habilitadas. Se a propriedade `PersistVm` não for especificada para máquinas virtuais não persistentes, elas serão excluídas do ambiente Azure quando desligadas.

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` define a propriedade `PersistVm` como **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` preserva o cache de write-back definindo `PersistVM` como **true**:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
```

```
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

Dica:

A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco do SO deve persistir. Para preservar uma máquina virtual provisionada, preserve o disco do SO primeiro. Não exclua o disco do SO sem antes excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem especificar o parâmetro `PersistVm`.

Personalizar o comportamento de ligar em caso de falha na alteração do tipo de armazenamento

Ao ligar, o tipo de armazenamento de um disco gerenciado pode falhar ao mudar para o tipo desejado devido a uma falha no Azure. Nesses cenários, a VM permaneceria desligada com uma mensagem de falha enviada a você. No entanto, você pode optar por ligar a VM mesmo quando o armazenamento não puder ser restaurado para o tipo configurado ou optar por manter a VM desligada.

- Se você configurar a propriedade personalizada `FailSafeStorageType` como **true** (configuração padrão) ou não a especificar nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM é ligada com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.
- Se você configurar a propriedade personalizada `FailSafeStorageType` como **false** nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM permanece desligada com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.

Para criar um catálogo de máquinas:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado.
4. Adicione a propriedade personalizada em `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"
```

```
-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. Crie o catálogo de máquinas. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`.

Para atualizar um catálogo de máquinas existente para incluir a propriedade personalizada `FailSafeStorageType`. Esta atualização não afeta as VMs existentes.

1. Atualize a propriedade personalizada no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />
```

```
</CustomProperties>"
```

Para aplicar a alteração feita em Set-ProvScheme às VMs existentes, execute o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

1. Execute o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`. Por exemplo:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. Reinicie as VMs.

Criar VMs com capacidade de hibernação

Em ambientes Azure, você pode criar um catálogo de máquinas MCS que suporta hibernação. Usando este recurso, você pode suspender uma VM e, em seguida, reconectar-se ao estado anterior da VM quando um usuário fizer login novamente.

A capacidade de hibernação aplica-se ao seguinte:

- SO de sessão única
- VMs persistentes e não persistentes
- Desktops VDI estáticos e aleatórios (agrupados)

Você pode retomar a mesma sessão depois de hibernar uma VM, independentemente de o desktop VDI ser estático ou aleatório.

Nesta seção, consulte o seguinte:

- Pré-requisitos
- Limitações
- Criar e gerenciar um catálogo de máquinas com capacidade de hibernação
- Criar um catálogo de máquinas para VMs existentes com capacidade de hibernação
- Verificar a propriedade de hibernação
- Gerenciamento de energia de VMs (Manual e Automatizado)

Pré-requisitos para usar a hibernação

Para usar a hibernação, certifique-se de concluir as seguintes tarefas:

- Instale o Agente de VM do Azure na imagem mestre para Windows e Linux. O arquivo de paginação da imagem do Windows pode estar no disco temporário. O MCS define o local do arquivo de paginação para a unidade C: no disco base quando a hibernação é ativada no catálogo de máquinas.
- O MCS define automaticamente a propriedade de hibernação para os recursos gerados. Você não precisa configurar as propriedades dos recursos mestre para oferecer suporte à hibernação.
- Use um tamanho de VM em sua assinatura que suporte a hibernação.
- Crie um perfil de máquina com capacidade de hibernação (VM ou especificação de modelo) para que as VMs herdem a capacidade de hibernação. Para criar a VM, consulte Introdução à hibernação.

> **Nota:**
>
> De acordo com a Microsoft, você pode implantar VMs com hibernação ativada a partir de um disco de SO. Este recurso é atualmente suportado em certas regiões e estará disponível para todas as regiões em breve. Para mais informações, consulte Implantar VMs com hibernação ativada a partir de um disco de SO.

Para criar a especificação do modelo, faça o seguinte:

a. Abra o Portal do Azure. Escolha uma VM cuja configuração você deseja usar no modelo. Selecione **Exportar modelo** no painel esquerdo.

b. Desmarque a caixa de seleção **Incluir parâmetros**. Copie o contexto e salve-o como um arquivo JSON, por exemplo, `VMExportTemplate.json`.

c. Certifique-se de que o parâmetro `hibernationEnabled` esteja `true` no modelo. Se o parâmetro não estiver `true`, verifique a configuração da VM que você usou. Você pode especificar um tamanho de VM suportado no arquivo de modelo. No entanto, você também pode especificar o tamanho da máquina ao criar o catálogo.

d. Adicione o modelo para o recurso de interface de rede ao arquivo JSON `VMExportTemplate.json`. Como resultado, você terá um arquivo de modelo ARM com dois recursos.

e. Selecione **Portal do Azure > Especificações de modelo > Importar modelo > Escolher arquivo de modelo local** para importar este arquivo de modelo como uma especificação de modelo ARM.

f. Após a criação da especificação do modelo ARM, você pode usá-la como um perfil de máquina.

> **Nota:**
>
> Pode levar alguns minutos para sincronizar com o Citrix Studio.

Para mais informações, consulte o documento da Microsoft Pré-requisitos para usar a hibernação.

Limitações

- Apenas catálogos de máquinas de SO de sessão única (persistentes e não persistentes) são suportados.
- Discos de SO efêmeros e recursos de E/S do MCS não suportam a hibernação do Azure.
- A hibernação pode falhar durante as atualizações automáticas do Windows.

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:

- Web Studio, ou
- Comandos do PowerShell

CRIAR UM CATÁLOGO USANDO O WEB STUDIO

1. Selecione **Criar Catálogo de Máquinas**. O assistente de criação de catálogo será aberto.
2. Na página **Tipo de Máquina**, selecione o tipo de máquina **SO de sessão única** para este catálogo.
3. Na página **Gerenciamento de Máquinas**, selecione as configurações da seguinte forma:

   a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.

   b. Selecione **Citrix Machine Creation Services™ (MCS)**.

4. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho aleatória ou estática conforme necessário.
5. Na página **Imagem**, selecione uma imagem mestre. Marque a caixa de seleção **Usar um perfil de máquina** e selecione um perfil de máquina que suporte hibernação. Clique na dica de ferramenta para saber se um perfil de máquina suporta hibernação.
6. Na página **Tipos de Armazenamento e Licença**, selecione o armazenamento e a licença a serem usados para este catálogo.
7. Na página **Máquinas Virtuais**, selecione a contagem de VMs, o tamanho da VM e a zona de disponibilidade.

> **Observação:**
>
> Os tamanhos de máquina que suportam hibernação são mostrados apenas para sua seleção.

8. Na página **NICs**, adicione as NICs que você deseja que as VMs usem.
9. Na página **Configurações de Disco**, selecione o tipo de armazenamento e o tamanho do disco de cache de write-back.
10. Na página **Grupo de Recursos**, selecione o grupo de recursos para provisionar VMs.
11. Na página **Identidades da Máquina**, selecione **Criar novas contas do Active Directory**. Em seguida, especifique um esquema de nomenclatura de conta.
12. Na página **Credenciais de Domínio**, clique em **Inserir credenciais**. Insira suas credenciais de domínio para realizar a criação da conta no domínio do Active Directory de destino.
13. Na página **Resumo**, insira um nome para o catálogo de máquinas e clique em **Concluir**.

Quando a criação do catálogo de máquinas MCS estiver concluída, localize o catálogo na lista de catálogos e clique na guia **Propriedades do Modelo**. O valor do parâmetro **Hibernação** deve ser **Suportado**.

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar.
  - Alterar o perfil da máquina para um que não seja capaz de hibernar.

- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
    - atualmente, altere o perfil da máquina para um capaz de hibernar usando o Web Studio.

CRIAR UM CATÁLOGO DE MÁQUINAS PARA GERENCIAR VMS EXISTENTES CAPAZES DE HIBERNAR

Se você já tiver VMs capazes de hibernar e quiser suspendê-las e retomá-las, crie um catálogo de máquinas para importar essas VMs para gerenciamento de energia.

> **Nota:**
>
> Você pode criar um catálogo de máquinas contendo VMs capazes e incapazes de hibernar. No entanto, se você quiser funcionalidade relacionada à hibernação, você deve criar o catálogo de máquinas apenas com VMs capazes de hibernar.

> Para criar um catálogo para VMs existentes capazes de hibernar usando o Web Studio, siga as instruções na tela para concluir as etapas e preste atenção às seguintes configurações principais:

1. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e, em seguida, selecione **Outro serviço ou tecnologia** como a forma de implantar máquinas.
2. Na página **Máquinas Virtuais**, adicione ou importe apenas as VMs capazes de hibernar.

CRIAR UM CATÁLOGO DE MÁQUINAS USANDO COMANDOS DO POWERSHELL

Depois de atender a todos os requisitos para usar a hibernação, você pode criar um catálogo de máquinas capaz de hibernar usando o comando `New-ProvScheme`. Para obter informações sobre como criar um catálogo usando o SDK do Remote PowerShell, consulte New-ProvScheme.

Ao criar o catálogo, você pode verificar se um tamanho de VM e um perfil de máquina suportam hibernação ou não usando os seguintes comandos do PowerShell:

- Para o tamanho da VM, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- Para o perfil da máquina, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar
  - Alterar o perfil da máquina para um que não seja capaz de hibernar
- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
  - atualmente, altere o perfil da máquina para um capaz de hibernar usando o Web Studio.

Para obter informações sobre como modificar o tamanho da VM e o perfil da máquina de um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

Verificar a propriedade de hibernação

Você pode verificar a propriedade de hibernação de um catálogo de máquinas, VM e uma máquina broker usando os comandos do PowerShell:

- Para verificar a propriedade de hibernação de um esquema de provisionamento, execute os seguintes comandos do PowerShell. O parâmetro `HibernationEnabled` deve ser `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- Para verificar a propriedade de hibernação de uma VM de provisionamento, execute os seguintes comandos PowerShell. O parâmetro `SupportsHibernation` deve ser `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- Para verificar a capacidade de hibernação de uma máquina broker, execute os seguintes comandos PowerShell. As ações de energia **Suspender** e **Retomar** indicam capacidade de hibernação.

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

Gerenciamento de energia de VMs com capacidade de hibernação

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs com capacidade de hibernação:

- **Suspender** VM do estado de execução
- **Retomar** VM do estado suspenso
- **Forçar desligamento** da VM de um estado suspenso
- **Forçar reinício** da VM do estado suspenso

Consulte o seguinte para obter mais informações:

- Suspender
- Retomar

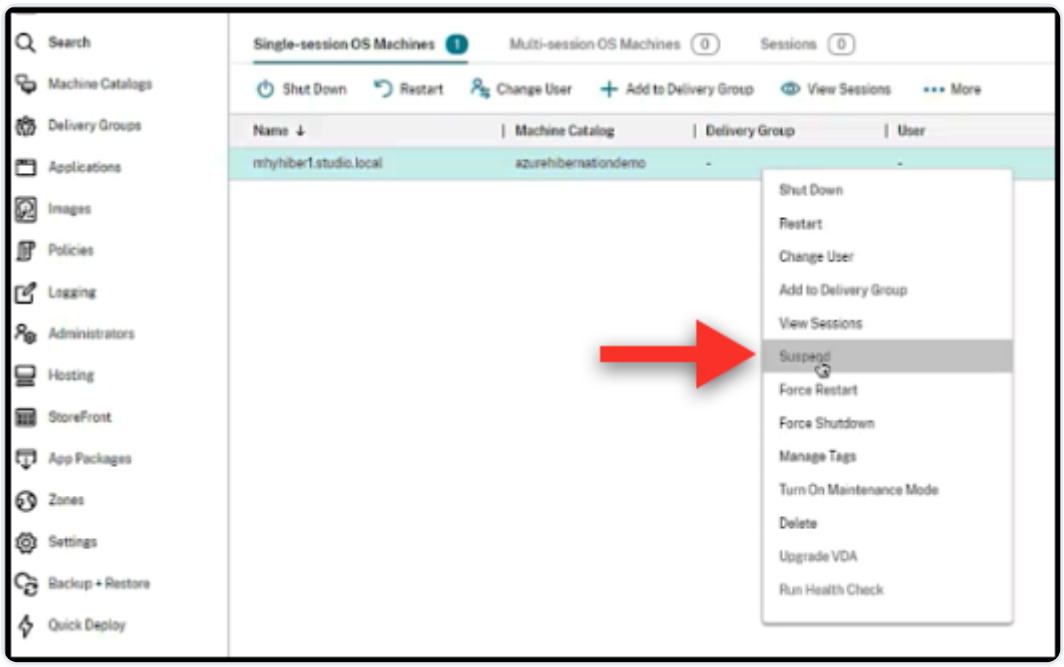
SUSPENDER

Você pode suspender uma VM usando uma das seguintes maneiras:

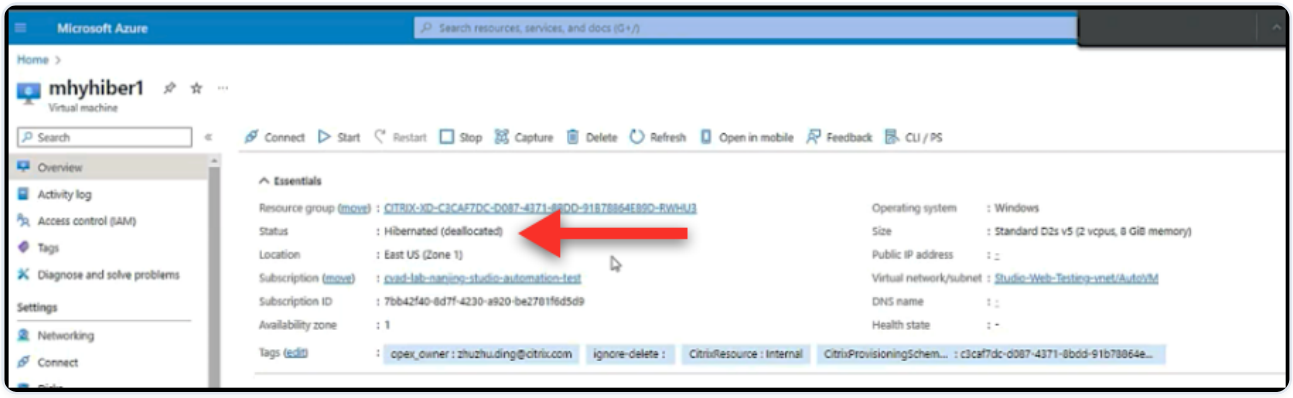
- **Manualmente** usando o Web Studio
- **Automaticamente** usando a política de tempo limite: Para obter mais informações, consulte Configurações diversas.

Para suspender manualmente uma VM:

1. Clique com o botão direito na VM e selecione **Suspender**. Clique em **Sim** para confirmar a ação. O **Estado de Energia** muda de **Suspensão** para **Suspenso**.



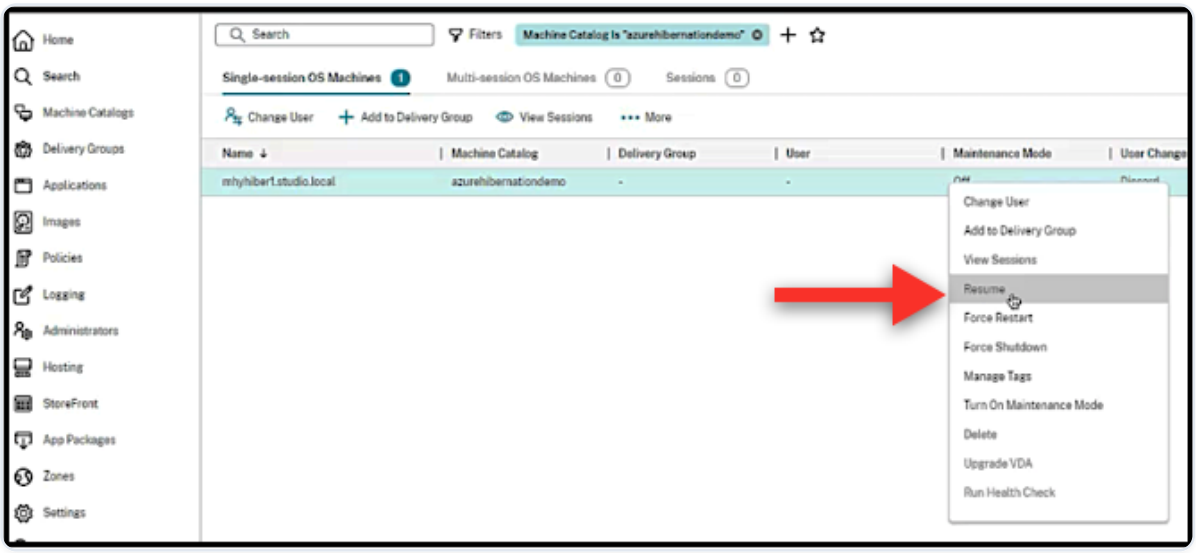
Você pode verificar o status da VM no portal do Azure.



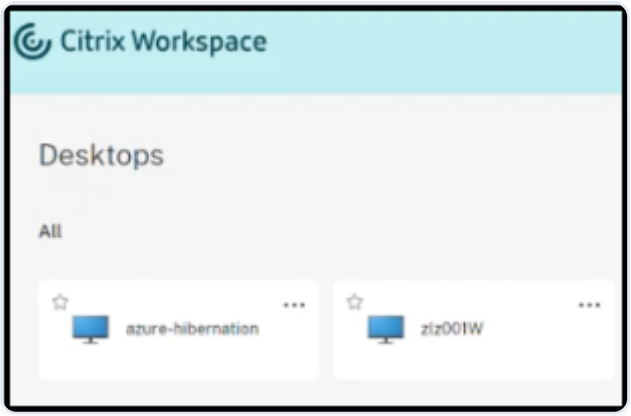
RETOMAR

Para retomar uma VM hibernada, use uma das seguintes maneiras:

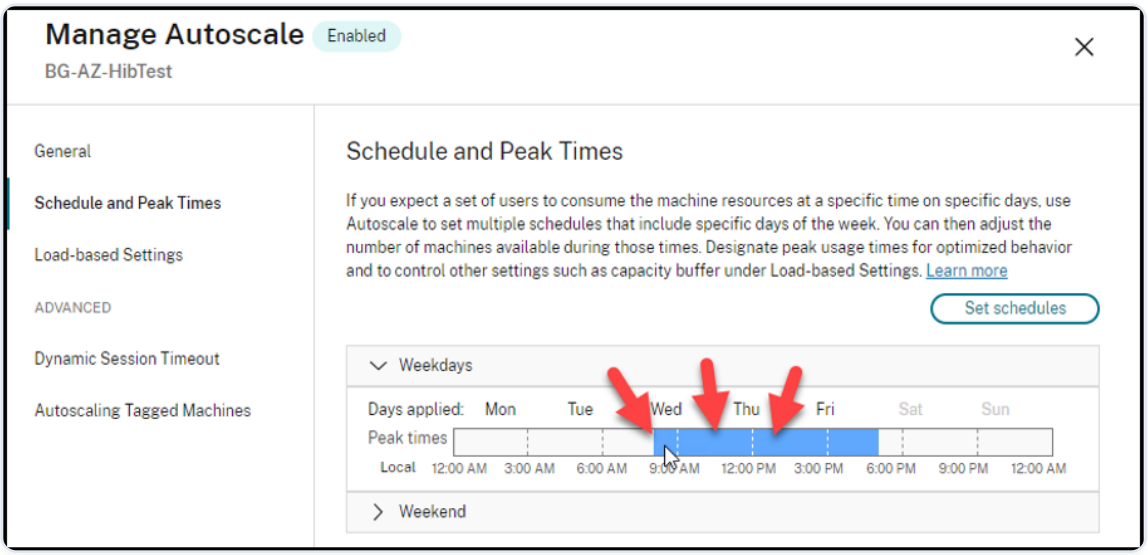
- **Manualmente**:
  - Os administradores podem retomar a VM usando o Web Studio.



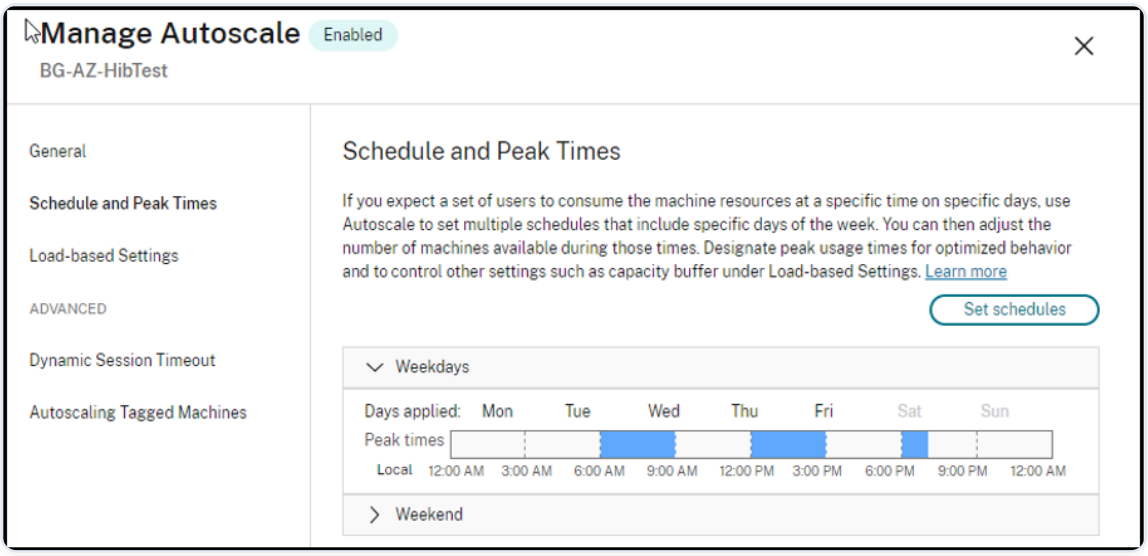
- Os usuários finais podem iniciar a VM usando o menu Citrix Workspace™ assim que clicarem no ícone da área de trabalho.



- **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 na programação de horários. Cada quadro azul representa um slot de tempo marcado como horário de pico. Os horários de pico podem ter slots de tempo consecutivos e não consecutivos.
    - Slots de tempo consecutivos

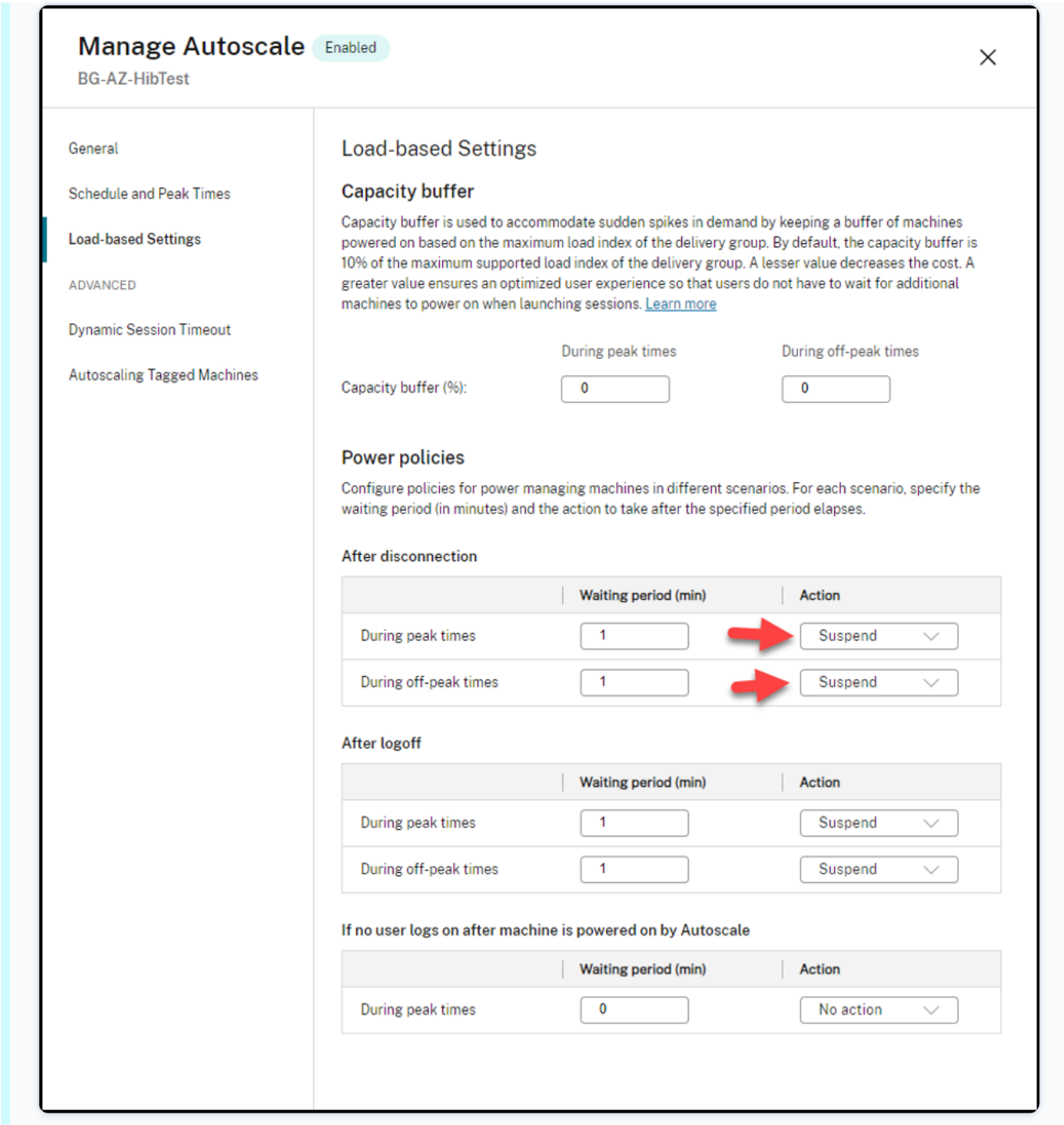


- Slots de tempo não consecutivos



Nota:

Em **Gerenciar Autoescala > Configurações baseadas em carga**, se a **Ação** estiver configurada como **Suspender**, então certifique-se de que todas as VMs dentro desse grupo de entrega tenham capacidade de hibernação. Caso contrário, as VMs que não podem hibernar continuarão a ser executadas.



Obter mensagens de aviso para falha de hibernação

Você pode obter mensagens de aviso usando um comando PowerShell `Get-ProvOperationEvent` em caso de falha de hibernação de VMs provisionadas por MCS e VMs existentes com capacidade de hibernação. Para obter informações sobre o comando Powershell, consulte a documentação do SDK Get-ProvOperationEvent.

Para fazer isso:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar módulos PowerShell específicos da Citrix.

3. Execute `Get-ProvOperationEvent` para obter a mensagem de aviso em caso de falha de hibernação.

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

Saída:

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {
```

```
                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                    powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                    component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend
```

```
OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

SOLUÇÃO DE PROBLEMAS DE HIBERNAÇÃO

Você recebe a seguinte mensagem de erro se você tentar habilitar os recursos de hibernação e de VM de inicialização confiável, no entanto, a configuração do sistema operacional convidado não está correta.

CÓDIGO DE ERRO	MENSAGEM DE ERRO
OperationNotAllowed	A Operação de Hibernar-Desalocar não pode ser realizada em uma VM que tenha a extensão 'AzureHibernateExtension' em estado de falha. Para obter mais informações, consulte `<https://aka.ms/hibernate-resume/errors/>`. Detalhes do erro da extensão: A habilitação da hibernação falhou. Resposta do comando powercfg. Código de Saída: 1. Mensagem de erro: A hibernação falhou com o seguinte erro: A solicitação não é suportada. Os seguintes itens estão impedindo a hibernação neste sistema. **A configuração atual do Device Guard desativou a hibernação. Um componente interno do sistema desativou a hibernação**.

Para resolver o problema, certifique-se de que a virtualização esteja habilitada dentro da VM convidada. Por exemplo, confirme se o Hyper-V está habilitado em um ambiente Windows. De acordo com a limitação do Microsoft Windows, a hibernação é suportada apenas com virtualização aninhada quando o lançamento confiável está habilitado na VM.

Para obter mais informações sobre mensagens de aviso, consulte o documento da Microsoft Solução de problemas de hibernação de VM.

Nota:

> Mensagens de erro relacionadas à falha na retomada de uma VM estarão disponíveis em uma versão futura.

Mais informações

Para obter mais informações sobre a hibernação do Citrix Azure, consulte o artigo da Citrix Tech Zone.

Políticas de segurança

Grupos de segurança

Grupo de segurança é um grupo de regras de segurança para filtrar o tráfego de rede entre recursos em uma rede virtual. As regras de segurança permitem ou negam o tráfego de rede de entrada para, ou o tráfego de rede de saída de, vários tipos de recursos. Cada regra especifica as seguintes propriedades:

- Nome: Um nome exclusivo dentro do grupo de segurança de rede
- Prioridade: As regras são processadas em ordem de prioridade, com números menores processados antes de números maiores, porque números menores têm prioridade mais alta
- Origem ou Destino: Qualquer, ou um endereço IP individual, bloco de roteamento entre domínios sem classe (CIDR) (10.0.0.0/24, por exemplo), tag de serviço ou grupo de segurança de aplicativo
- Protocolo: Os protocolos com base nos quais você adiciona regras para cada grupo de segurança
- Direção: Se a regra se aplica ao tráfego de entrada ou de saída
- Intervalo de portas: Você pode especificar uma porta individual ou um intervalo de portas
- Ação: Permitir ou negar

Consulte o seguinte para obter mais informações sobre hipervisores suportados:

- Grupos de segurança na AWS
- Grupos de segurança no Microsoft Azure
- Grupos de segurança no Google Cloud Platform

Grupos de segurança na AWS

Grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também pode associar esses grupos de segurança a cada instância em sua VPC. As regras de entrada controlam o tráfego de entrada para sua instância, e as regras de saída controlam o tráfego de saída de 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.

Grupos de segurança no Microsoft Azure

O Citrix Virtual Apps and Desktops oferece suporte a grupos de segurança de rede no Azure. Espera-se que os grupos de segurança de rede se associem a sub-redes. Para obter mais informações, consulte Grupos de segurança de rede.

Para obter mais informações sobre o grupo de segurança de rede criado durante a preparação da imagem, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Grupos 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 da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total. Para obter mais informações, consulte Regras de Firewall.

Inicialização Segura e vTPM

A Inicialização Segura é um recurso da Unified Extensible Firmware Interface (UEFI), que é responsável pela inicialização do sistema. Ela garante que apenas software confiável seja carregado durante o processo de inicialização.

Trusted Platform Module (TPM) é um chip de hardware que fornece armazenamento seguro para chaves criptográficas e outros dados confidenciais. Um Virtual Trusted Platform Module (vTPM)

executa as mesmas funções que um TPM, mas executa recursos de coprocessador criptográfico em software. Embora o TPM possa aumentar a segurança, ele não é um requisito para o Secure Boot.

Consulte o seguinte para obter mais informações sobre os serviços de nuvem compatíveis:

- Inicialização Segura e vTPM no Google Cloud Platform
- Inicialização Segura e vTPM no Microsoft Azure
- vTPM no VMware

Inicialização Segura e vTPM no Google Cloud Platform

Você pode provisionar máquinas virtuais blindadas no Google Cloud Platform (GCP). A integridade verificável da VM blindada é alcançada usando os seguintes recursos:

- Inicialização Segura
- Inicialização Medida habilitada para vTPM
- Monitoramento de integridade

Para obter mais informações sobre como usar o PowerShell para criar um catálogo com VM blindada, consulte Usando o PowerShell para criar um catálogo com VM blindada.

> **Nota:**
>
> Se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, se você usar um perfil de máquina para criar o catálogo, deverá habilitar o vTPM na origem do perfil de máquina (VM ou modelo de instância). Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte Criar VMs do Windows 11 no nó de locatário único.

Inicialização Segura e vTPM no Microsoft Azure

Em ambientes Azure, você pode criar catálogos de máquinas habilitados com o Trusted Launch. O Azure oferece o Trusted Launch como uma forma contínua de melhorar a segurança das VMs de geração 2. O Trusted Launch protege contra técnicas de ataque avançadas e persistentes. Para habilitar o Trusted Launch, use uma configuração de catálogo baseada em perfil de máquina. Na raiz do Trusted Launch está o Secure Boot para sua VM. O Trusted Launch também usa o vTPM para realizar atestado remoto pela nuvem. Isso é usado para verificações de integridade da plataforma e para tomar decisões baseadas em confiança. Você pode habilitar individualmente o

Secure Boot e o vTPM. Para obter mais informações sobre como criar um catálogo de máquinas com o Trusted Launch, consulte Catálogos de máquinas com Trusted Launch.

vTPM no VMware

O MCS oferece suporte à criação de um catálogo de máquinas com vTPM. Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Se a configuração baseada em perfil de máquina for usada e o vTPM estiver habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM do modelo de VM. Se o perfil de máquina não for usado e a imagem mestre tiver o vTPM habilitado, as VMs no catálogo terão o vTPM em branco. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Recursos de criptografia

Os recursos de criptografia protegem o conteúdo das máquinas virtuais contra ataques de convidados mal-intencionados em um host de máquina virtual compartilhado e contra ataques lançados pelo software de controle do hipervisor que gerencia todas as máquinas virtuais no host.

Consulte o seguinte para obter mais informações sobre os serviços de nuvem suportados:

- Recursos de criptografia na AWS
- Recursos de criptografia no Google Cloud Platform
- Recursos de criptografia no Microsoft Azure

Recursos de criptografia na AWS

Esta seção descreve os recursos de criptografia em ambientes de virtualização da AWS.

Criptografia automática

Você pode ativar a criptografia automática de novos volumes Amazon EBS e cópias de snapshot criadas em sua conta. Para obter mais informações, consulte Criptografia automática.

Recursos de criptografia no Google Cloud Platform

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Google Cloud Platform (GCP).

Se você precisar de mais controle sobre as operações de chave do que o permitido pelas chaves de criptografia gerenciadas pelo Google, poderá usar chaves de criptografia gerenciadas pelo cliente. Ao usar uma chave de criptografia gerenciada pelo cliente, um objeto é criptografado com a chave pelo Cloud Storage no momento em que é armazenado em um bucket, e o objeto é

automaticamente descriptografado pelo Cloud Storage quando é 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 MCS. Para obter mais informações, consulte Usando Chaves de Criptografia Gerenciadas pelo Cliente (CMEK).

Recursos de criptografia no Microsoft Azure

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Azure.

Criptografia do lado do servidor do Azure

A maioria dos discos gerenciados do Azure é criptografada com a criptografia 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 Virtual Apps and Desktops oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host.

Este método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, este método de criptografia criptografa os dados de ponta a ponta.

Para obter mais informações sobre como criar um catálogo de máquinas MCS com capacidade de criptografia no host, consulte Criptografia de disco do Azure no host.

Criptografia dupla do Azure

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente com alta sensibilidade à segurança e preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por esta criptografia dupla. Discos de SO e de dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla em disco gerenciado.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto a VM quanto o modelo ARM como entrada de perfil de máquina.

Para obter mais informações, consulte VMs confidenciais do Azure.

Criar grupos de entrega

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente em Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> Um grupo de entrega é uma coleção de máquinas selecionadas de um ou mais catálogos de máquinas. O grupo de entrega especifica quais usuários podem usar essas máquinas, além dos aplicativos e desktops disponíveis para esses usuários.

A criação de um grupo de entrega é o próximo passo na configuração da sua implantação após criar um site e criar um catálogo de máquinas. Posteriormente, você pode alterar as configurações iniciais no primeiro grupo de entrega e criar outros grupos de entrega. Existem também recursos e configurações que você pode configurar apenas ao editar um grupo de entrega, e não ao criá-lo.

Para Acesso Remoto a PC, ao criar um site, um grupo de entrega chamado "Remote PC Access Desktops" é criado automaticamente.

Para criar um grupo de entrega:

1. Se você criou um site e um catálogo de máquinas sem um grupo de entrega, o Web Studio o guiará para o local de partida correto para criar um.
2. Se você já criou um grupo de entrega e deseja criar outro, siga estas etapas:
    a. Selecione **Delivery Groups**. Selecione **Create Delivery Group** no painel de ações.
    b. Para organizar grupos de entrega usando pastas, crie pastas sob a pasta padrão **Delivery Groups**. Para obter mais informações, consulte Criar uma pasta.
    c. Selecione a pasta onde deseja criar o grupo e, em seguida, clique em **Create Delivery Group**. O assistente de criação de grupo é aberto.

3. O assistente é iniciado com uma página de **Introdução**, que você pode remover de futuros lançamentos deste assistente.
4. O assistente o guiará pelas páginas descritas na seção a seguir. Ao terminar cada página, clique em **Next** até chegar à página final.

Etapa 1. Máquinas

Na página **Machines**, selecione um catálogo e selecione o número de máquinas que deseja usar desse catálogo.

É bom saber:

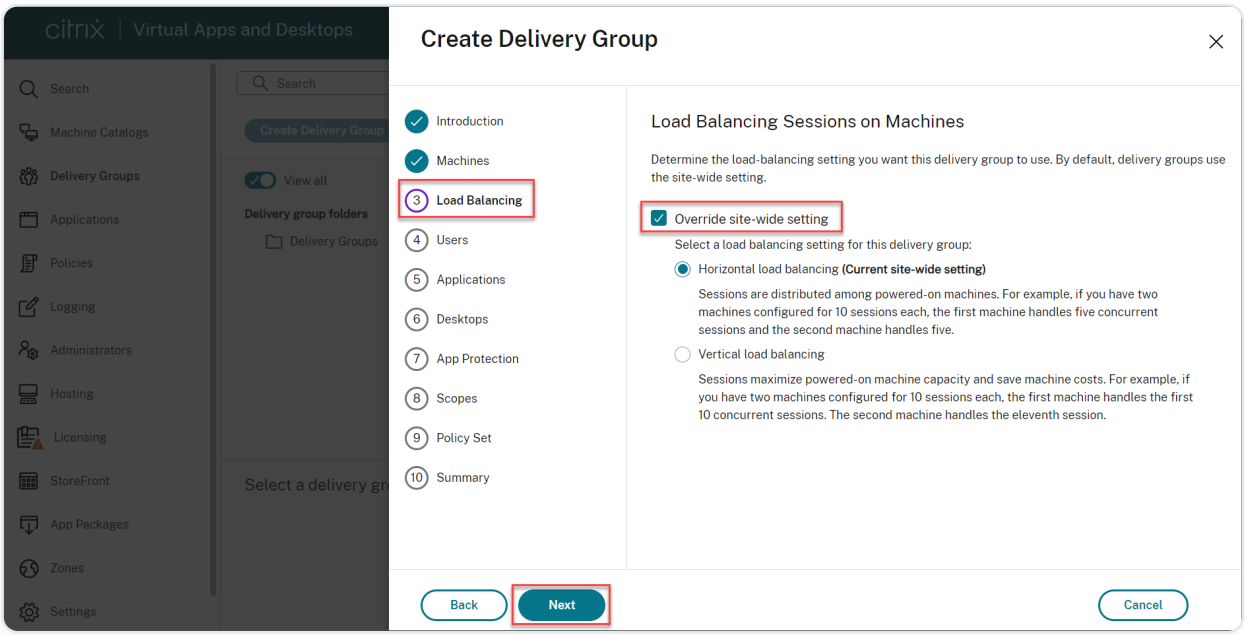
- Pelo menos uma máquina deve permanecer sem uso em um catálogo selecionado.
- Um catálogo pode ser especificado em mais de um grupo de entrega. Uma máquina pode ser usada em apenas um grupo de entrega.
- Um grupo de entrega pode usar máquinas de mais de um catálogo; no entanto, esses catálogos devem conter os mesmos tipos de máquina (SO multi-sessão, SO de sessão única ou Acesso Remoto a PC). Em outras palavras, você não pode misturar tipos de máquina em um grupo de entrega. Da mesma forma, se sua implantação tiver catálogos de máquinas Windows e catálogos de máquinas Linux, um grupo de entrega pode conter máquinas de qualquer tipo de SO, mas não de ambos.
- A Citrix recomenda que você instale ou atualize todas as máquinas com a versão mais recente do VDA. Atualize os catálogos e grupos de entrega conforme necessário. Ao criar um grupo de entrega, se você selecionar máquinas que têm diferentes versões de VDA instaladas, o grupo de entrega será compatível com a versão mais antiga do VDA. Isso é chamado de *nível funcional* do grupo. Por exemplo, se uma das máquinas tiver a versão 7.1 do VDA e as outras máquinas tiverem a versão atual, todas as máquinas do grupo poderão usar apenas os recursos que eram suportados no VDA 7.1. Isso significa que alguns recursos que exigem versões posteriores do VDA podem não estar disponíveis nesse grupo de entrega.
- Cada máquina em um catálogo de Acesso Remoto a PC é automaticamente associada a um grupo de entrega. Ao criar um site de Acesso Remoto a PC, um catálogo chamado "Máquinas de Acesso Remoto a PC" e um grupo de entrega chamado "Desktops de Acesso Remoto a PC" são criados automaticamente.
- As seguintes verificações de compatibilidade são realizadas:
    - MinimumFunctionalLevel deve ser compatível
    - SessionSupport deve ser compatível

- AllocationType deve ser compatível para SingleSession
- ProvisioningType deve ser compatível
- PersistChanges deve ser compatível para MCS e Citrix Provisioning™
- O catálogo RemotePC é compatível apenas com o catálogo de Acesso Remoto a PC
- Verificação relacionada ao AppDisk

Etapa 2. Balanceamento de carga

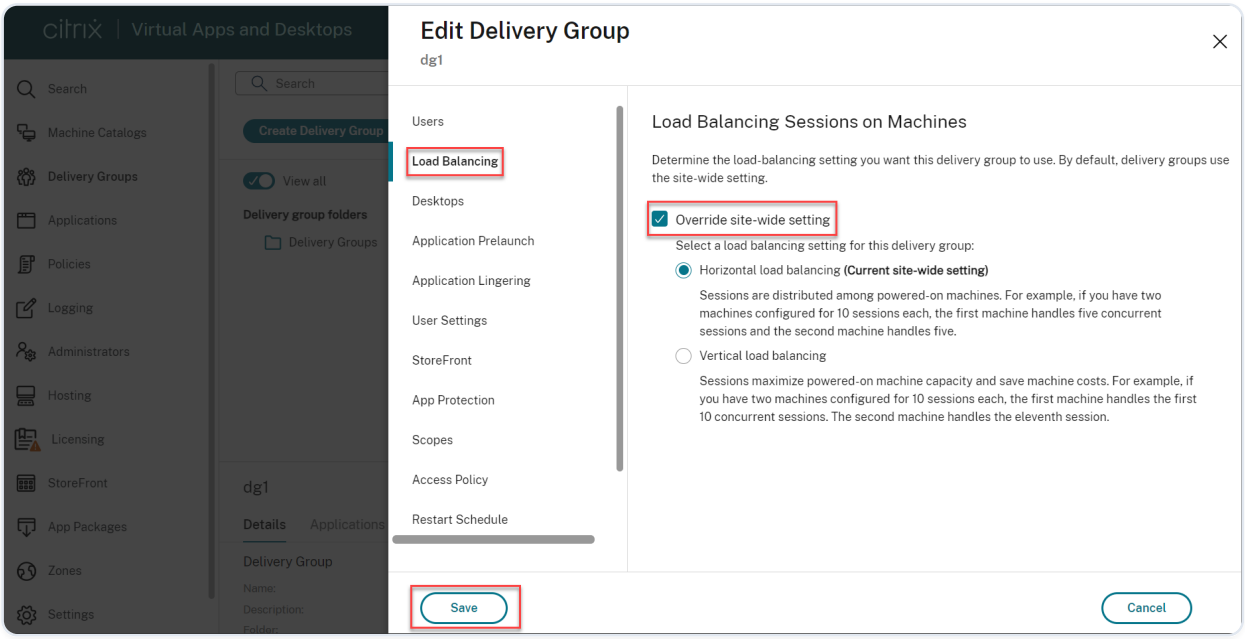
Para configurar as definições de balanceamento de carga ao criar um grupo de entrega:

1. Faça login no Web Studio.
2. Na navegação à esquerda, clique em **Grupos de Entrega**.
3. Na página **Grupos de Entrega**, clique em **Criar Grupo de Entrega**.
4. No assistente **Criar Grupo de Entrega**, clique em **Avançar**. O assistente **Máquina** é aberto.
5. No assistente **Máquinas**, selecione um catálogo de máquinas necessário e clique em **Avançar**. O assistente **Balanceamento de Carga** é aberto.
6. No assistente **Balanceamento de Carga**, selecione a caixa de seleção **Substituir configuração de todo o site**.
7. Selecione a opção **Balanceamento de carga horizontal** ou **Balanceamento de carga vertical** conforme necessário e clique em **Avançar**.



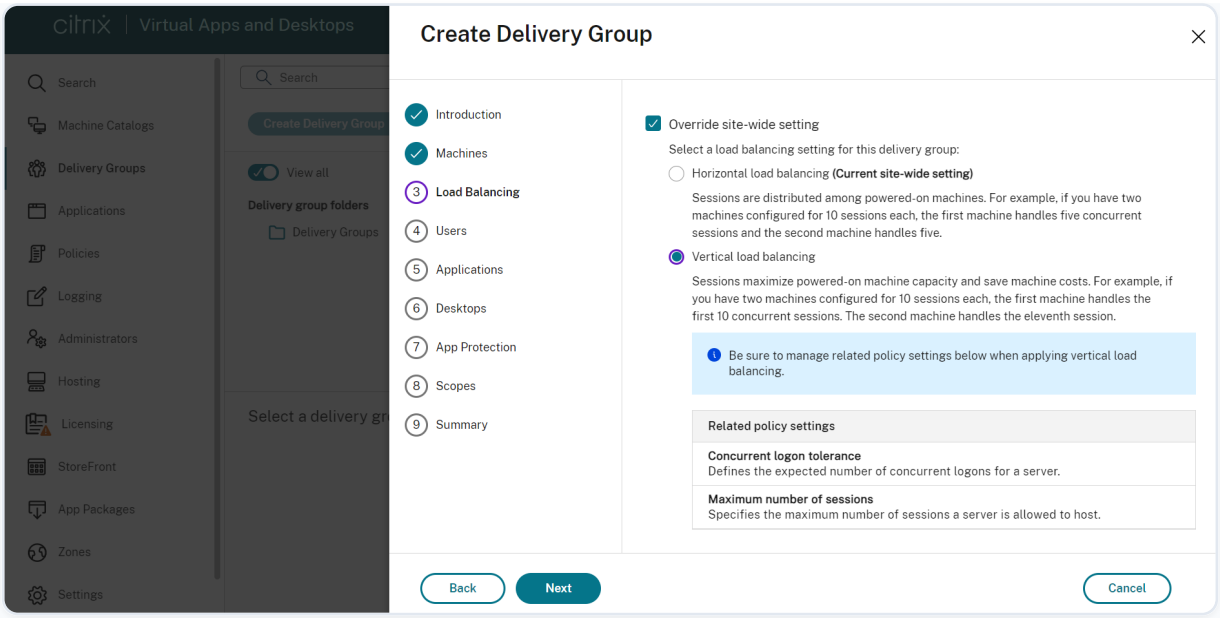
Para configurar as configurações de balanceamento de carga ao editar um grupo de entrega existente:

1. Faça login no Web Studio.
2. No painel esquerdo, clique em **Grupos de Entrega**.
3. Selecione um **Grupo de Entrega** na lista e clique em **Editar**. O assistente **Editar Grupo de Entrega** é aberto.
4. Na página **Editar Grupo de Entrega**, clique em **Balanceamento de Carga**.
5. Marque a caixa de seleção **Substituir configuração de todo o site**.
6. Selecione a opção **Balanceamento de carga horizontal** ou **Balanceamento de carga vertical** conforme necessário e clique em **Salvar**.



Observação:

Quando a configuração de balanceamento de carga vertical é aplicada, certifique-se de que as políticas **Tolerância de logon simultâneo** e **Número máximo de sessões** estejam configuradas adequadamente.



> Para obter mais informações sobre balanceamento de carga no nível do site e do grupo de entrega, consulte Balancear carga de máquinas

Etapa 3. Tipo de entrega

Esta página aparece somente se você escolheu um catálogo que contém máquinas OS estáticas (atribuídas) de sessão única.

Na página **Tipo de Entrega**, escolha **Aplicativos** ou **Desktops**. Não é possível habilitar ambos.

Se você selecionou máquinas de um catálogo de SO de várias sessões ou de SO de sessão única aleatório (agrupado), o tipo de entrega é considerado aplicativos e desktops: você pode entregar aplicativos, desktops ou ambos.

Etapa 4. Usuários

Especifique os usuários e grupos de usuários que podem usar os aplicativos e desktops no grupo de entrega.

Onde as listas de usuários são especificadas

As listas de usuários do Active Directory são especificadas ao criar ou editar o seguinte:

- Uma lista de acesso de usuário de um site, que não é configurada através do Web Studio. Por padrão, as regras da política de direitos de aplicativo incluem todos. Consulte os cmdlets `BrokerAppEntitlementPolicyRule` do SDK do PowerShell para obter detalhes.
- Grupos de aplicativos (se configurados).

- Grupos de entrega.
- Aplicativos.

A lista de usuários que podem acessar um aplicativo através do StoreFront™ é formada pela interseção das listas de usuários acima. Por exemplo, para configurar o uso do aplicativo A para um departamento específico, sem restringir indevidamente o acesso a outros grupos:

- Use a regra de política de direitos de aplicativo padrão que inclui todos.
- Configure a lista de usuários do grupo de entrega para permitir que todos os usuários da sede usem qualquer um dos aplicativos especificados no grupo de entrega.
- (Se os grupos de aplicativos estiverem configurados) Configure a lista de usuários do grupo de aplicativos para permitir que os membros da unidade de negócios de Administração e Finanças acessem os aplicativos A a L.
- Configure as propriedades do aplicativo A para restringir sua visibilidade apenas à equipe de Contas a Receber em Administração e Finanças.

Usuários autenticados e não autenticados

Existem dois tipos de usuários: autenticados e não autenticados (não autenticados também são chamados de anônimos). Você pode configurar um ou ambos os tipos em um grupo de entrega.

- **Autenticados:** Para acessar aplicativos e desktops, os usuários e membros do grupo que você especificar pelo nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha ao StoreFront ou ao aplicativo Citrix Workspace™. Para grupos de entrega que contêm máquinas de SO de sessão única, você pode importar dados de usuário (uma lista de usuários) posteriormente, editando o grupo de entrega.
- **Não autenticados (anônimos):** Para grupos de entrega que contêm máquinas de SO de múltiplas sessões, você pode permitir que os usuários acessem aplicativos e desktops sem apresentar credenciais ao StoreFront ou ao aplicativo Citrix Workspace. Por exemplo, em quiosques, o aplicativo pode exigir credenciais, mas o portal de acesso e as ferramentas Citrix 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 para Windows Server OS (versão mínima 7.6) instalado. Quando usuários não autenticados são habilitados, você deve ter uma loja StoreFront não autenticada.

  Contas de usuário não autenticadas são criadas sob demanda quando uma sessão é iniciada e são nomeadas Anon*XYZ*, onde *XYZ* é um valor exclusivo de três dígitos.

Sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desconectadas automaticamente quando o cliente se desconecta. Reconexão, roaming entre clientes e Workspace Control não são suportados.

A tabela a seguir descreve suas escolhas na página **Usuários**:

HABILITAR ACESSO PARA	ADICIONAR/ATRIBUIR USUÁRIOS E GRUPOS DE USUÁRIOS?	HABILITAR A CAIXA DE SELEÇÃO "CONCEDER ACESSO A USUÁRIOS NÃO AUTENTICADOS"?
Apenas usuários autenticados	Sim	Não
Apenas usuários não autenticados	Não	Sim
Usuários autenticados e não autenticados	Sim	Sim

Etapa 5. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada Aplicativos. Você pode especificar uma pasta diferente. Para obter detalhes, consulte o artigo Gerenciar 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 Gerenciar Aplicativos.
- Se você tentar adicionar um aplicativo e já existir um com o mesmo nome nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você recusar, o aplicativo será adicionado com um sufixo que o torna exclusivo dentro dessa pasta de aplicativo.
- Ao adicionar um aplicativo a mais de um grupo de entrega, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos de entrega. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos de entrega aos quais o aplicativo foi adicionado.
- Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade Nome do aplicativo (para usuário) no Web Studio; caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

- Você pode adicionar aplicativos empacotados a grupos de entrega estáticos de sessão única e de Acesso Remoto a PC. Esses pacotes são montados automaticamente cada vez que os usuários fazem login em seus desktops ou PCs remotos.

Clique em **Adicionar** para exibir as fontes do aplicativo.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina criada a partir da imagem mestre no catálogo selecionado. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos; selecione aqueles que você deseja adicionar e clique em **OK**.
- **Manualmente:** Aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. A seleção desta origem abre uma nova página onde você especifica um aplicativo para adicionar das seguintes maneiras:
  - Digite o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Procurar**, insira as credenciais para acessar o VDA, aguarde a conexão com o VDA e, em seguida, selecione um aplicativo do VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.
- **Existente:** Aplicativos adicionados anteriormente ao site, talvez em outro grupo de entrega. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos. Adicione os aplicativos e clique em **OK**.
- **Pacotes de aplicativos:** Aplicativos em pacotes de aplicativos App-V, MSIX ou MSIX app attach. Ao selecionar esta origem, uma nova página é aberta onde você pode selecionar o tipo de origem e, em seguida, os aplicativos que deseja adicionar a partir da exibição resultante.

Se uma origem de aplicativo ou aplicativo não estiver disponível ou for inválido, ele não estará visível ou não poderá ser selecionado. Por exemplo, a origem **Existente** não estará disponível se nenhum aplicativo tiver sido adicionado ao site. Ou, um aplicativo pode não ser compatível com os tipos de sessão suportados nas máquinas do catálogo selecionado.

Etapa 6. Desktops

O título desta página depende do catálogo que você escolheu na página **Máquinas**:

- Se você escolheu um catálogo contendo máquinas agrupadas, esta página é intitulada **Desktops**.

- Se você escolheu um catálogo contendo máquinas estáticas de sessão única e especificou "Desktops" na página **Tipo de Entrega**, esta página é intitulada **Atribuições de Usuário de Desktop**.
- Se você escolheu um catálogo contendo máquinas estáticas de sessão única e especificou "Aplicativos" na página **Tipo de Entrega**, esta página é intitulada **Atribuições de Usuário de Máquina de Aplicativo**.

Clique em **Adicionar**. Na caixa de diálogo:

- Nos campos Nome de exibição e Descrição, digite as informações a serem exibidas no Citrix Workspace app.
- Para adicionar uma restrição de tag a um desktop, selecione **Restringir inicializações a máquinas com esta tag** e, em seguida, selecione a tag na lista suspensa. Para obter mais informações, consulte Tags.
- Use os botões de opção para iniciar um desktop ou para atribuir uma máquina ao iniciar o desktop. Os usuários podem ser todos que podem acessar este grupo de entrega, ou usuários e grupos de usuários específicos.
- Se o grupo contiver máquinas estáticas de sessão única, especifique o número máximo de desktops por usuário. Este deve ser um valor de um ou maior.
- Habilite ou desabilite o desktop (para máquinas agrupadas) ou a regra de atribuição de desktop (para máquinas estáticas de sessão única). Desabilitar um desktop interrompe a entrega do desktop. Desabilitar uma regra de atribuição de desktop interrompe a atribuição automática de desktop aos usuários.
- Quando terminar de usar a caixa de diálogo, clique em **OK**.

Número máximo de instâncias de um desktop em um site (somente PowerShell)

Para configurar o número máximo de instâncias de um desktop no site (somente PowerShell):

- No PowerShell, use o cmdlet BrokerEntitlementPolicyRule apropriado com o parâmetro MaxPerEntitlementInstances. Por exemplo, o cmdlet a seguir modifica a regra `tsvda-desktop` para definir o número máximo de instâncias simultâneas de um desktop permitidas no site para duas. Quando há duas instâncias de desktop em execução, ocorre um erro se um terceiro assinante tentar iniciar um desktop.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- Para obter orientação, use o cmdlet Get-Help. Por exemplo, `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`.

Etapa 7: Configuração do Cache de Host Local

Essa configuração é visível apenas para grupos de entrega que contêm máquinas agrupadas de sessão única gerenciadas por energia.

Por padrão, essas máquinas ficam indisponíveis no modo Cache de Host Local (LHC) devido a riscos de exposição de dados. Para alterar o comportamento padrão e torná-las disponíveis para novas conexões de usuário no modo LHC, selecione **Manter recursos disponíveis**.

Alternativamente, você pode alterar o comportamento padrão usando comandos PowerShell. Para obter mais informações, consulte Suporte a aplicativos e desktops.

> **Importante:**
>
> Habilitar o acesso a máquinas agrupadas de sessão única gerenciadas por energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.

Etapa 8. Resumo

Insira um nome para o grupo de entrega. Você também pode (opcionalmente) inserir uma descrição, que aparece no aplicativo Citrix Workspace e no Web Studio.

Revise as informações de resumo e clique em **Concluir**.

Gerenciar grupos de entrega

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Este artigo descreve os procedimentos para gerenciar grupos de entrega a partir do console de gerenciamento. Além de alterar as configurações especificadas ao criar o grupo, você pode configurar outras configurações que não estão disponíveis ao criar um grupo de entrega.

As categorias de procedimento incluem: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Impedir que usuários se conectem a máquinas" é descrito na categoria de máquinas, mas também afeta os usuários. Se você não conseguir encontrar uma tarefa em uma categoria, verifique uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Aplicativos contêm informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer as permissões da função interna de Administrador de Grupo de Entrega. Para obter detalhes, consulte Administração delegada.

Geral

- Exibir detalhes do grupo
- Alterar o tipo de entrega
- Alterar endereços do StoreFront™
- Alterar o nível funcional
- Gerenciar grupos de entrega do Acesso Remoto para PC
- Organizar grupos de entrega usando pastas
- Gerenciar Proteção de Aplicativos

Exibir detalhes do grupo

1. Use a função de pesquisa para localizar um grupo de entrega específico. Consulte Pesquisar instâncias para obter instruções.
2. Nos resultados da pesquisa, selecione um grupo conforme necessário.
3. Consulte a tabela a seguir para obter descrições das colunas do grupo.
4. Clique em uma guia no painel de detalhes inferior para obter mais informações sobre este grupo.

COLUNA	DESCRIÇÃO
Grupo de Entrega	O nome do grupo e o tipo de sessão. Os tipos de sessão incluem SO de sessão única e SO de múltiplas sessões.
Entregando	O tipo de recursos entregues por este grupo. Os valores possíveis incluem Aplicativos, Desktops e Aplicativos e Desktops. "Atribuição de máquina estática" aparece se o grupo de entrega consistir em máquinas dedicadas.
Sessão em Uso	O número de máquinas configuradas e o número de máquinas que estão em estado Desconectado.
Contagem Alocada	O número de máquinas no catálogo atribuídas a um grupo de entrega.
Pasta	O local do grupo na árvore de **Grupos de Entrega**. Ele exibe o nome da pasta em que o grupo está (incluindo a barra invertida final), ou `-` se o grupo estiver no nível raiz.

Alterar o tipo de entrega de um grupo de entrega

O tipo de entrega indica o que o grupo pode entregar: aplicativos, desktops ou ambos.

Antes de alterar um tipo **somente aplicativo** ou **desktops e aplicativos** para o tipo **somente desktops**, exclua todos os aplicativos do grupo.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Tipo de Entrega**, selecione o tipo de entrega desejado.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Alterar endereços do StoreFront

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.

3. Na página **StoreFront**, selecione ou adicione URLs do StoreFront. Essas URLs são usadas pelo aplicativo Citrix Workspace™, que é instalado em cada máquina no grupo de entrega.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Você também pode especificar endereços de servidor StoreFront selecionando **StoreFront** no painel esquerdo.

Alterar o nível funcional

Altere o nível funcional do grupo de entrega depois de atualizar os VDAs em suas máquinas e os catálogos de máquinas que contêm as máquinas usadas no grupo de entrega.

Antes de começar:

- Se você usa o Citrix Provisioning™ (anteriormente Provisioning Services), atualize a versão do VDA no console do Citrix Provisioning.
- Inicie as máquinas que contêm o VDA atualizado para que elas possam se registrar em um Delivery Controller. Este processo informa ao console o que precisa ser atualizado no grupo de entrega.
- Se você precisar continuar a usar versões anteriores do VDA, os recursos mais recentes do produto não estarão disponíveis. Para obter mais informações, consulte a documentação de atualização.

Para alterar o nível funcional de um grupo de entrega:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e clique em **Alterar Nível Funcional** na barra de ações. A ação **Alterar Nível Funcional** aparece somente se VDAs atualizados forem detectados.
3. Clique em **Alterar**.

A exibição indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Você pode então cancelar a ação de alteração, resolver os problemas da máquina e, em seguida, executar a ação de alteração novamente.

Após a conclusão da alteração, você pode reverter as máquinas para seus estados anteriores. Selecione o grupo de entrega e, em seguida, selecione **Desfazer Alteração de Nível Funcional** na barra de ações.

Gerenciar grupos de entrega do Remote PC Access

Se uma máquina em um catálogo de máquinas de Acesso Remoto para PC não for atribuída, a máquina será temporariamente atribuída a um grupo de entrega associado a esse catálogo. Essa atribuição temporária permite que a máquina seja atribuída a um usuário posteriormente.

A associação do grupo de entrega ao catálogo de máquinas tem um valor de prioridade. A prioridade determina o grupo de entrega atribuído à máquina 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 de Acesso Remoto para PC tiver várias atribuições de grupo de entrega, o software selecionará a correspondência com a prioridade mais alta. Use o SDK do PowerShell para definir esse valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas de Acesso Remoto para PC são associados a um grupo de entrega. Contas de máquina ou Unidades Organizacionais adicionadas ao catálogo posteriormente podem ser adicionadas ao grupo de entrega. Essa associação pode ser desativada ou ativada.

Para adicionar ou remover uma associação de catálogo de máquinas do Remote PC Access com um grupo de entrega:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo do Remote PC Access.
3. Na seção **Detalhes**, clique na guia **Catálogos de Máquinas** e, em seguida, selecione um catálogo de Acesso Remoto para PC.
4. Para adicionar ou restaurar uma associação, clique em **Adicionar Desktops**. Para remover uma associação, clique em **Remover Associação**.

Organizar grupos de entrega usando pastas

Você pode criar pastas para organizar grupos de entrega para facilitar o acesso.

Funções necessárias

Por padrão, você precisa ter a seguinte função interna para criar e gerenciar pastas de grupo de entrega: Administrador de Nuvem, Administrador Completo ou Administrador de Grupo de Entrega. Se necessário, você pode personalizar as funções para criar e gerenciar pastas de grupo de entrega. Para obter mais informações, consulte Permissões necessárias.

Criar uma pasta de grupo de entrega

Antes de começar, planeje como organizar seus grupos de entrega. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de entrega e subpastas.
- Todos os nós (como os nós de **Catálogos de Máquinas**, **Aplicativos** e **Grupos de entrega**) compartilham uma árvore de pastas no back-end. Para evitar conflitos de nomes com outros nós ao renomear ou mover pastas, recomendamos que você dê nomes diferentes às pastas de primeiro nível em nós diferentes.

Para criar uma pasta de grupo de entrega, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra **Ação**.
3. Insira um nome para a nova pasta e, em seguida, clique em **Concluído**.

> **Dica:**
>
> Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

Mover um grupo de entrega

Você pode mover um grupo de entrega entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Visualize os grupos por pasta. Você também pode ativar **Ver todos** acima da hierarquia de pastas para visualizar todos os grupos de uma vez.
3. Clique com o botão direito do mouse em um grupo e, em seguida, selecione **Mover Grupo de Entrega**.
4. Selecione a pasta para a qual deseja mover o grupo e, em seguida, clique em **Concluído**.

> **Dica:**
>
> Você pode arrastar um grupo para uma pasta.

Gerenciar pastas de grupos de entrega

Você pode excluir, renomear e mover pastas de grupos de entrega.

Esteja ciente 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. Selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

Permissões necessárias

A tabela a seguir lista as permissões necessárias para executar ações em pastas de grupos de entrega.

AÇÃO	PERMISSÕES NECESSÁRIAS
Criar pastas de grupos de entrega	Criar Pasta de Grupo de Entrega
Excluir pastas de grupo de entrega	Remover Pasta de Grupo de Entrega
Mover pastas de grupo de entrega	Mover Pasta de Grupo de Entrega
Renomear pastas de grupo de entrega	Editar Pasta de Grupo de Entrega
Mover grupos de entrega para pastas	Editar Pasta de Grupo de Entrega e Editar Propriedades do Grupo de Entrega

Gerenciar Proteção de Aplicativo

As informações a seguir são complementares a Proteção de aplicativo. Observe os seguintes detalhes:

- Você deve ter um direito válido de Proteção de Aplicativo. Para adquirir o recurso Proteção de Aplicativo, entre em contato com seu representante de vendas da Citrix.
- A Proteção de Aplicativo requer confiança XML. Para habilitar a confiança XML, vá para **Configurações > Habilitar confiança XML**.

- Em relação à captura anti-tela:
  - No Windows e macOS, apenas a janela do conteúdo protegido fica em branco. A Proteção de Aplicativo está ativa quando uma janela protegida não está minimizada.
  - No Linux, a captura inteira fica em branco. A Proteção de Aplicativo está ativa independentemente de uma janela protegida estar minimizada ou não.

Para escolher um método de Proteção de Aplicativo para um grupo de entrega, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Proteção de Aplicativos**, você pode ver as seguintes opções:

OPÇÕES	DESCRIÇÃO
Não aplicar	Selecione esta opção para não aplicar a configuração.
Aplicar a este grupo de entrega	Selecione as opções **Anti-keylogging** e/ou **Anti key capturing**. Passe o mouse sobre cada uma dessas configurações para ler os detalhes na dica de ferramenta.
Aplicar contextualmente	Para aplicar esta configuração, configure a política de acesso na página **Configurações da Política de Acesso**.
	1. Clique em **Política de Acesso** no painel esquerdo e clique em **Adicionar**.
	1. Na página **Adicionar Política**, faça o seguinte
	- i. Insira um **Nome da política** e configure as configurações conforme necessário.
	- ii. Nos campos **Filtro** e **Valor**, insira os detalhes e clique em **Concluído**. A nova política é listada na página **Proteção de Aplicativos**. Habilite as configurações necessárias para esta política.

OPÇÕES	DESCRIÇÃO
	- iii. Clique em **Salvar**.

4. Na página **Delivery Group**, selecione o **Delivery Group** e clique na guia **Details** na parte inferior. As novas configurações de **App Protection** aplicadas são exibidas.

Usuários

Esta seção aborda os seguintes tópicos:

- Alterar configurações do usuário
- Adicionar ou remover usuários
- Gerenciar atribuições de usuário

Alterar configurações do usuário em um grupo de entrega

O nome desta página aparece como **Configurações do Usuário** ou **Configurações Básicas**.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Configurações do Usuário** (ou **Configurações Básicas**), altere qualquer uma das configurações na tabela a seguir.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

CONFIGURAÇÃO	DESCRIÇÃO
Descrição	O texto que o Citrix Workspace (ou StoreFront) usa e que os usuários veem.
Habilitar grupo de entrega	Se o grupo de entrega está habilitado.
Fuso horário	O fuso horário em que as máquinas deste grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site. **Nota:** Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

CONFIGURAÇÃO	DESCRIÇÃO
Habilitar Secure ICA®	Protege as comunicações de e para as máquinas no grupo de entrega usando SecureICA, que criptografa o protocolo ICA. O nível padrão é de 128 bits. O nível pode ser alterado usando o SDK. A Citrix recomenda usar mais métodos de criptografia, como a criptografia TLS, ao atravessar redes públicas. Além disso, o SecureICA não verifica a integridade dos dados.

Adicionar ou remover usuários em um grupo de entrega

Para obter informações detalhadas sobre usuários, consulte Usuários.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Usuários**:
    - Para adicionar usuários, clique em **Adicionar** e, em seguida, especifique os usuários que você deseja adicionar.
    - Para remover usuários, selecione um ou mais usuários e, em seguida, clique em **Remover**.
    - Marque ou desmarque a caixa de seleção para permitir o acesso por usuários não autenticados.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Importar ou exportar listas de usuários

Para grupos de entrega que contêm máquinas físicas de SO de sessão única, você pode importar informações de usuário de um arquivo .csv após criar o grupo de entrega. Você também pode exportar informações de usuário para um arquivo .csv. O arquivo .csv pode conter dados de uma versão anterior do produto.

A primeira linha no arquivo CSV deve conter dois cabeçalhos de coluna, separados por uma vírgula. Certifique-se de que o primeiro cabeçalho seja `Machine Account` e o segundo cabeçalho seja `User Names`. (Você pode incluir cabeçalhos adicionais, mas eles não são suportados.) As linhas subsequentes no arquivo contêm dados separados por vírgulas. As

entradas `Machine Account` podem ser SID do computador, FQDN ou pares de nome de domínio e computador.

Para importar ou exportar informações do usuário:

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Alocação de Máquina**, selecione **Importar** lista ou **Exportar** lista e, em seguida, navegue até o local do arquivo.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Gerenciar atribuições de usuário

Gerencie as atribuições de usuário para máquinas em um grupo de entrega. Quando as regras de atribuição de desktop são configuradas para o grupo de entrega, as máquinas são atribuídas aleatoriamente aos usuários no lançamento inicial do desktop e permanecem atribuídas aos usuários, a menos que suas atribuições de usuário sejam modificadas. Se você quiser atribuir manualmente uma máquina não atribuída a usuários específicos ou alterar a atribuição de usuário existente para uma máquina, siga as etapas descritas neste tópico para fazer as alterações. Usando essas etapas, você também pode modificar os nomes exibidos no Citrix Workspace App para máquinas atribuídas a usuários.

As etapas detalhadas são as seguintes:

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. No painel esquerdo, selecione **Machine Allocation**. Os seguintes detalhes para cada máquina no grupo aparecem:
    - **Nome da máquina:** Mostra o nome de uma máquina.
    - **Nome de exibição:** Mostra o nome de exibição da máquina no Citrix Workspace App.
    - **Usuários:** Mostra os usuários atribuídos a esta máquina. Se as regras de atribuição de desktop forem configuradas, as máquinas serão atribuídas aleatoriamente aos usuários no lançamento inicial do desktop e permanecerão atribuídas a eles, a menos que suas atribuições de usuário sejam modificadas.
4. Localize uma máquina e, em seguida, atribua usuários a ela ou altere sua atribuição de usuário:

- Clique em **Browser** para navegar até os usuários.
- Na coluna **Usuários**, insira uma lista de nomes de usuário separados por ponto e vírgula.
- Clique em **Importar do arquivo CSV** para importar os detalhes da configuração usando um arquivo CSV.

5. (Opcional) Se a máquina for atribuída a usuários, modifique seu nome de exibição conforme necessário.

> **Observação:**
>
> O campo Nome de exibição é habilitado somente quando a máquina é atribuída a usuários:
>
> - Se a máquina for atribuída a um usuário com base em uma regra de atribuição de área de trabalho, este campo mostrará o nome de exibição configurado nessa regra.
> - Se a máquina for atribuída manualmente aos usuários e o campo for deixado em branco, o nome publicado do grupo de entrega (se especificado) será usado como nome de exibição da máquina. O nome do grupo de entrega será usado se o nome publicado não for especificado. Observe que você pode especificar nomes publicados para grupos de entrega apenas via PowerShell.

6. Selecione **Aplicar** para aplicar as alterações e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Máquinas

- Alterar atribuições de máquinas a usuários
- Habilitar Cache de Host Local para VDAs agrupados de sessão única gerenciados por energia
- Alterar o número máximo de máquinas por usuário
- Atualizar uma máquina
- Adicionar, alterar ou remover uma restrição de tag para um desktop
- Remover uma máquina
- Restringir acesso a máquinas
- Impedir que usuários se conectem a uma máquina (modo de manutenção)

- Desligar e reiniciar máquinas
- Criar e gerenciar agendamentos de reinício para máquinas
- Habilitar agendamento de reinício único
- Carregar máquinas gerenciadas
- Máquinas gerenciadas por energia

Alterar atribuições de máquinas a usuários em um grupo de entrega

Você pode alterar as atribuições de máquinas de SO de sessão única provisionadas com MCS. Você não pode alterar as atribuições para máquinas de SO de várias sessões ou máquinas provisionadas com Citrix Provisioning.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Desktops** ou **Regras de Atribuição de Desktop** (o título da página depende do tipo de catálogo de máquinas que o grupo de entrega usa), especifique os novos usuários.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Habilitar Cache de Host Local para VDAs agrupados de sessão única gerenciados por energia

Por padrão, as máquinas agrupadas de sessão única gerenciadas por energia ficam indisponíveis quando no modo Cache de Host Local. Você pode substituir o comportamento padrão por grupo de entrega. As etapas detalhadas são as seguintes:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.

   Na lista de grupos, os grupos que contêm máquinas agrupadas de sessão única provisionadas por MCS ou Citrix Provisioning exibem um ícone de aviso.
2. Selecione um grupo conforme necessário e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Cache de Host Local**, selecione **Manter recursos disponíveis**.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Alternativamente, você pode substituir o comportamento padrão usando comandos PowerShell. Para mais informações, consulte Suporte a aplicativos e desktops.

> **Importante:**

> Habilitar o acesso a máquinas agrupadas de sessão única gerenciadas por energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.

Alterar o número máximo de máquinas por usuário em um grupo de entrega

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Regras de Atribuição de Desktop**, defina o valor máximo de desktops por usuário.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Atualizar uma máquina em um grupo de entrega

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Exibir Máquinas** na barra de ações.
3. Selecione uma máquina e, em seguida, clique em **Atualizar Máquinas** na barra de ações.

Para escolher uma imagem diferente, selecione **Imagem** e, em seguida, selecione um instantâneo.

Para aplicar as alterações e notificar os usuários da máquina, selecione **Notificação de lançamento para usuários finais**. Em seguida, especifique:

- Quando atualizar a imagem mestre: agora ou na próxima reinicialização
- O tempo de distribuição da reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados da reinicialização
- A mensagem que os usuários recebem

Adicionar, alterar ou remover uma restrição de tag para um desktop

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais desktops são considerados para lançamento. Revise as considerações e precauções em Tags.

1. Selecione **Delivery Groups** no painel esquerdo.

2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Desktops**, selecione o desktop e clique em **Editar**.
4. Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag.
5. Para alterar ou remover uma restrição de tag, faça o seguinte:
   - Selecione uma tag diferente.
   - Remova a restrição de tag desmarcando **Restringir inicializações a máquinas com esta tag**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Remover uma máquina de um grupo de entrega

Remover uma máquina a exclui de um grupo de entrega. Isso não a exclui do catálogo de máquinas que o grupo de entrega usa. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes de serem removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto você a remove, coloque a máquina em modo de manutenção antes de desligá-la.

As máquinas podem conter dados pessoais, portanto, tenha cuidado antes de alocar a máquina para outro usuário. Considere refazer a imagem da máquina.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Exibir Máquinas** na barra de ações.
3. Certifique-se de que a máquina esteja desligada.
4. Selecione a máquina e clique em **Remover do Grupo de Entrega** na barra de ações.

Você também pode remover uma máquina de um grupo de entrega através da conexão que a máquina usa.

Restringir o acesso a máquinas em um grupo de entrega

Quaisquer alterações feitas para restringir o acesso a recursos em um grupo de entrega substituem as configurações anteriores, independentemente do método usado. Você pode:

- **Restringir acesso para administradores usando escopos de administração delegada:** Você pode criar e atribuir um escopo que permite aos administradores acessar todos os

aplicativos e outro escopo que fornece acesso apenas a determinados aplicativos. Para obter detalhes, consulte Administração delegada.

- **Restringir acesso para usuários por meio de expressões de política de acesso inteligente:** Você pode configurar regras de política de acesso para controlar o acesso do usuário a um grupo de entrega específico. Os exemplos incluem:
  - Restringir o acesso a um subconjunto de usuários e especificar os dispositivos de usuário permitidos.
  - Restringir o acesso a usuários conectados via Workspace (em vez de StoreFront).
  - Restringir o acesso a usuários conectados via uma URL específica do Workspace.

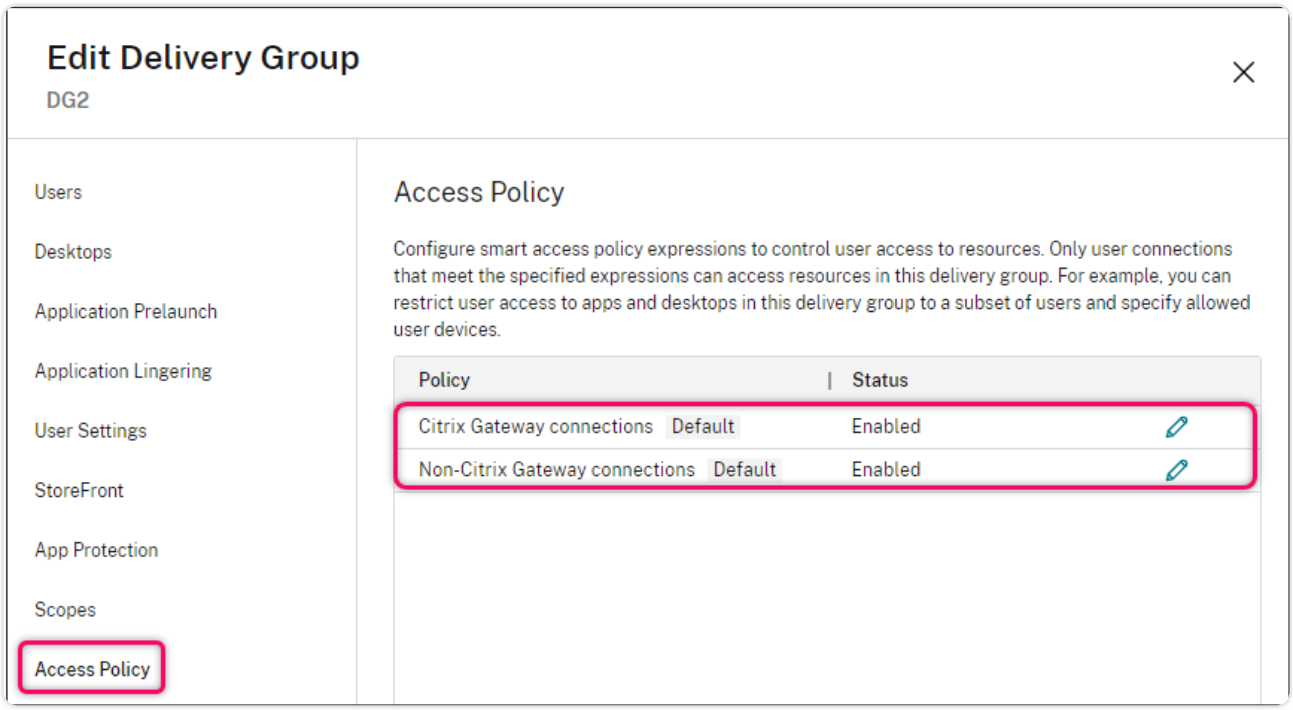
Esta seção o orienta sobre como restringir o acesso do usuário a grupos de entrega por meio de regras de política de acesso:

- Sobre as regras de política de acesso
- Adicionar regras de política de acesso
- Gerenciar regras de política de acesso usando o Web Studio
- Adicionar e refinar regras de política usando o PowerShell

Sobre as regras de política de acesso

Você pode configurar várias regras de política de acesso para um grupo de entrega. Aplicativos e desktops em um grupo de entrega aparecem no StoreFront ou Workspace de um usuário quando a conexão do usuário corresponde a qualquer regra de política de acesso que você definiu para o grupo de entrega, independentemente da ordem.

Cada regra pode ser ativada ou desativada individualmente. Uma regra desativada é ignorada quando a política de acesso é avaliada.



No Web Studio, a lista de Política de Acesso inclui as seguintes regras de política SmartAccess padrão. Você pode adicionar mais, se necessário.

- **Conexões do Citrix Gateway.** Esta política permite que apenas conexões de usuário feitas através do Citrix Gateway acessem recursos dentro do grupo de entrega. Conexões de usuário feitas através do Workspace quando os recursos de Postura do Dispositivo ou Localização da Rede estão habilitados também são consideradas conexões através do Citrix Gateway.
- **Conexões que não são do Citrix Gateway.** Esta política permite que apenas conexões de usuário que não são feitas através do Citrix Gateway acessem recursos dentro do grupo de entrega.

Observação:

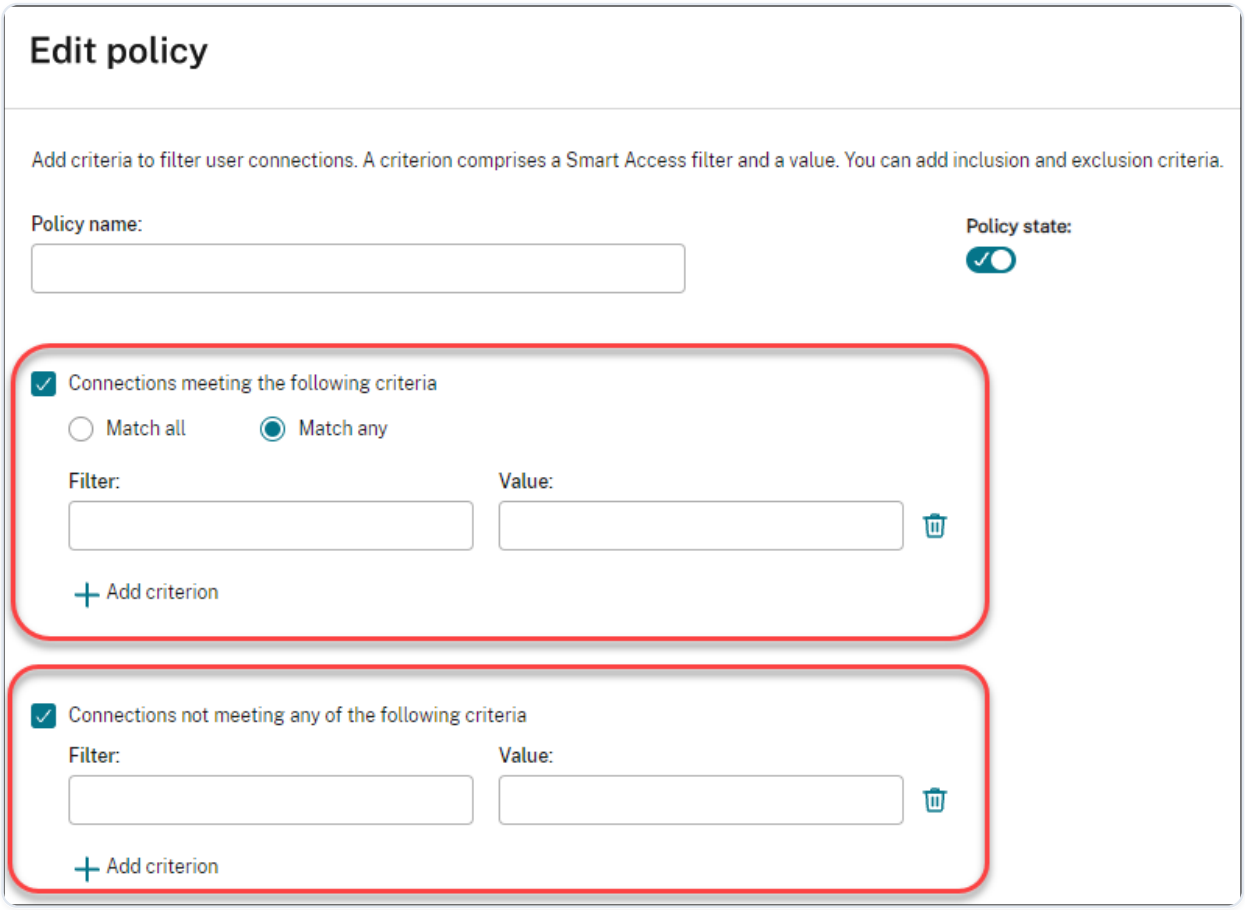
- Para evitar que as regras padrão substituam uma recém-configurada, você deve desabilitar as regras padrão ou refiná-las para excluir os filtros usados na nova política.
- As políticas padrão não podem ser excluídas, mas podem ser desabilitadas. Para desabilitar uma política, clique no ícone **Editar** e, em seguida, altere o **Estado da política** para **Desabilitado**.
- A lista de políticas também mostra regras adicionadas usando comandos PowerShell. Essas políticas podem ser excluídas, mas não podem ser editadas no Web Studio.

Adicionar regras de política de acesso usando o Web Studio

Uma regra de política de acesso compreende um conjunto de filtros. Para obter mais informações sobre filtros, consulte este artigo. Ao adicionar uma regra de política de acesso, você adiciona vários filtros de condição à regra conforme necessário.

Para adicionar uma política para um grupo de entrega usando o Web Studio, siga estas etapas:

1. No console, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Política de Acesso**, clique em **Adicionar**. A página **Adicionar Política** é exibida.



4. No campo **Nome da política**, digite um nome descritivo para a política. O nome deve ser exclusivo em sua implantação.
5. Para definir os critérios para conexões de usuário permitidas, siga estas etapas:
   a. Selecione **Conexões que atendem aos seguintes critérios**.
   b. Clique em **Adicionar critério**.
   c. No campo **Filtro**, digite o nome do filtro que você deseja usar. No campo **Valor**, digite um valor desejado para o filtro. Por exemplo, para permitir que apenas usuários conectados

via Workspace (em vez de StoreFront) acessem recursos neste grupo de entrega, digite `Citrix-Via-Workspace` para **Filtro** e `True` para **Valor**.

d. Para adicionar mais critérios, repita as etapas b-c.

e. Selecione o relacionamento entre os critérios:

- **Corresponder a qualquer**. Permite o acesso somente quando a conexão de usuário de entrada atende a qualquer um dos critérios de filtro configurados.
- **Corresponder a todos**. Permite o acesso somente quando a conexão de usuário de entrada atende a todos os critérios de filtro configurados.

6. Para definir os critérios para conexões de usuário proibidas, siga estas etapas:

a. Selecione **Conexões que não atendem a nenhum dos seguintes critérios**.

b. Clique em **Adicionar critério**.

c. No campo **Filter**, digite o nome do filtro que você deseja usar. No campo **Value**, digite um valor desejado para o filtro. Por exemplo, para proibir que usuários conectados através da URL do Workspace `example.cloud.com` acessem recursos neste grupo de entrega. Digite `Citrix.Workspace.UsingDomain` para **Filter** e `example.cloud.com` para **Value**.

d. Para adicionar mais critérios, repita as etapas b-c.

> **Observação:**
>
> As conexões de usuário que atendem a qualquer um dos critérios configurados são proibidas de acessar recursos neste grupo de entrega.

7. Clique em **Concluído**.

A nova política aparece na lista de políticas.

8. Revise e refine as regras de política padrão para evitar sobreposições não intencionais com conexões cobertas por esta nova política. Para refinar as políticas existentes, use as seguintes maneiras:

- Desative as regras de política padrão.
- Configure as regras de política padrão para excluir os filtros SmartAccess que você adicionou aos critérios de inclusão da nova política. Para obter mais informações, consulte Gerenciar regras de política usando o Web Studio e Adicionar e gerenciar regras de política de acesso usando o PowerShell.

> **Importante:**
>
> Conforme explicado em Sobre as regras de política de acesso, quando a conexão de um usuário corresponde a uma ou mais regras de política em um grupo de entrega, o usuário obtém acesso aos seus recursos. Portanto, após criar uma regra, você deve revisar e refinar cuidadosamente as regras existentes para evitar sobreposições não intencionais com conexões cobertas pela nova regra.

Gerenciar regras de política de acesso usando o Web Studio

Você pode usar os critérios de inclusão e exclusão para refinar as políticas padrão. Por exemplo, para restringir o acesso a um subconjunto dessas conexões, siga estas etapas:

1. Edite uma política padrão.
2. Selecione **Conexões que atendem a qualquer um dos seguintes critérios**.
3. Adicione, edite ou remova as expressões de política SmartAccess para os cenários de acesso de usuário permitidos.

Para obter mais informações, consulte a documentação do Citrix Gateway.

Adicionar e gerenciar regras de política de acesso usando o PowerShell

Você pode usar os seguintes cmdlets do PowerShell para adicionar e gerenciar regras de política de acesso para grupos de entrega:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Para obter mais informações, consulte os artigos relacionados na Citrix Developer Documentation.

Impedir que usuários se conectem a uma máquina (modo de manutenção) em um grupo de entrega

Quando você precisa interromper temporariamente novas conexões com máquinas, pode ativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega. Você pode fazer isso antes de aplicar patches ou usar ferramentas de gerenciamento.

- Quando uma máquina de SO multi-sessão está no modo de manutenção, os usuários podem se conectar a sessões existentes, mas não podem iniciar novas sessões.
- Quando uma máquina de SO de sessão única (ou um PC usando Acesso Remoto a PC) está no modo de manutenção, os usuários não podem se conectar ou reconectar. As conexões atuais permanecem conectadas até que se desconectem ou façam logoff.

Para ativar ou desativar o modo de manutenção:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo.
3. Para ativar o modo de manutenção para todas as máquinas no grupo de entrega, clique em **Turn On Maintenance Mode** na barra de ações.

   Para ativar o modo de manutenção para uma máquina, clique em **View Machines** na barra de ações. Selecione uma máquina e, em seguida, clique em **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 clique em **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 de SO multi-sessão está no modo de manutenção. O modo de manutenção é ativado quando ocorre qualquer um dos seguintes:

- O modo de manutenção está ativado, conforme descrito anteriormente.
- A RDC está configurada para **Não permitir conexões a este computador**.
- O RDC não está definido como **Don't allow connections to this computer**. A configuração **Remote Host Configuration User Logon Mode** é **Allow reconnections, but prevent new logons** ou **Allow reconnections, but prevent new logons until the server is restarted**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, o que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, o que afeta as máquinas nesse catálogo.

Desligar e reiniciar máquinas em um grupo de entrega

Este procedimento não é suportado para máquinas de Acesso Remoto a PC.

1. Selecione **Delivery Groups** no painel esquerdo.

2. Selecione um grupo e, em seguida, clique em **View Machines** na barra de ações.
3. Selecione a máquina e, em seguida, clique em uma das seguintes entradas na barra de ações:

    - **Forçar desligamento:** Desliga a máquina à força e atualiza a lista de máquinas.
    - **Reiniciar:** Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a máquina permanecerá em seu estado atual.
    - **Forçar reinício:** Desliga o sistema operacional à força e, em seguida, reinicia a máquina.
    - **Suspender:** Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
    - **Desligar:** Solicita ao sistema operacional que seja desligado.

Para ações não forçadas, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

A Citrix recomenda que você impeça que usuários de máquinas de SO de sessão única selecionem **Desligar** dentro de uma sessão. Consulte a documentação da política da Microsoft para obter detalhes.

Você também pode desligar e reiniciar máquinas em uma conexão.

Criar e gerenciar agendamentos de reinicialização para máquinas em um grupo de entrega

> **Nota:**
>
> - Quando um agendamento de reinicialização é aplicado a um grupo de entrega com o Autoscale™ ativado, suas máquinas são apenas desligadas e deixadas para o Autoscale ligá-las.
> - Quando os agendamentos de reinicialização são aplicados a máquinas aleatórias de sessão única, essas máquinas são desligadas em vez de reiniciadas, para economizar custos. Recomendamos que você use o Autoscale para ligar as máquinas.
> - Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

> Um agendamento de reinicialização especifica quando as máquinas em um grupo de entrega são reiniciadas periodicamente. Você pode criar um ou mais agendamentos para um grupo de entrega. Um agendamento pode afetar:

- Todas as máquinas do grupo.
- Uma ou mais (mas não todas) máquinas no grupo. As máquinas são identificadas por uma tag que você aplica à máquina. Isso é chamado de restrição de tag, porque a tag restringe uma ação apenas a itens que possuem a tag.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você deseja que cada máquina seja reiniciada uma vez por semana e que as máquinas usadas pela equipe de contabilidade sejam reiniciadas diariamente. Para conseguir isso, configure um agendamento para todas as máquinas e outro agendamento apenas para as máquinas da contabilidade.

Um agendamento inclui o dia e a hora em que a reinicialização começa e a duração.

Você pode ativar ou desativar um agendamento. Desativar um agendamento pode ser útil durante testes, em intervalos especiais ou ao preparar agendamentos antes de precisar deles.

Você não pode usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reiniciar.

Sobreposição de agendamentos

Vários agendamentos podem se sobrepor. No exemplo acima, ambos os agendamentos afetam as máquinas de contabilidade. Essas máquinas podem ser reiniciadas duas vezes no domingo. O código de agendamento foi projetado para evitar reiniciar a mesma máquina com mais frequência do que o pretendido, mas isso não pode ser garantido.

- Se os agendamentos coincidirem precisamente nos horários de início e duração, é mais provável que as máquinas sejam reiniciadas apenas uma vez.
- Quanto mais os agendamentos diferirem nos horários de início e duração, mais provável é que ocorram várias reinicializações.
- O número de máquinas afetadas por um agendamento também afeta a chance de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário para máquinas de contabilidade, dependendo da duração especificada para cada um.

Para uma análise aprofundada dos agendamentos de reinicialização, consulte Detalhes internos do agendamento de reinicialização.

Exibir agendamentos de reinicialização

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Selecione a página **Agendamento de Reinicialização**.

A página **Agendamento de Reinicialização** contém as seguintes informações para cada agendamento configurado:

- Nome do agendamento
- Restrição de tag usada, se houver
- Com que frequência as reinicializações da máquina ocorrem
- Se os usuários da máquina recebem uma notificação
- Se o agendamento está ativado

Adicionar (aplicar) tags

Ao configurar um agendamento de reinicialização que usa uma restrição de tag, certifique-se de que a tag tenha sido adicionada às máquinas que o agendamento afeta. No exemplo acima, cada uma das máquinas usadas pela equipe de contabilidade tem uma tag aplicada. Para obter detalhes, consulte Tags.

Embora você possa aplicar mais de uma tag a uma máquina, um agendamento de reinício pode especificar apenas uma tag.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo que contém as máquinas controladas pelo agendamento.
3. Clique em **Exibir Máquinas** e, em seguida, selecione as máquinas às quais você deseja adicionar uma tag.
4. Clique em **Gerenciar Tags** na barra de ações.
5. Se a tag existir, marque a caixa de seleção ao lado do nome da tag. Se a tag não existir, clique em **Criar** e especifique o nome da tag. Depois que a tag for criada, marque a caixa de seleção ao lado do nome da tag recém-criada.
6. Clique em **Salvar** na caixa de diálogo **Gerenciar Tags**.

Criar um agendamento de reinício

> **Nota:**

> Os agendamentos de reinício podem ser aplicados a todas as máquinas multissessão gerenciadas por energia e não gerenciadas por energia.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Agendamento de Reinicialização**, clique em **Adicionar**.
4. Na página **Add Restart Schedule**:

    - Para habilitar o agendamento, selecione **Yes**. Para desabilitar o agendamento, selecione **No**.
    - Digite um nome e uma descrição para o agendamento.
    - Para **Restrict to tag**, aplique uma restrição de tag.
    - Para **Include machines in maintenance mode**, escolha se deseja incluir máquinas que estão no modo de manutenção neste agendamento. Para usar o PowerShell, consulte Reinicializações agendadas para máquinas em modo de manutenção.
    - Para **Restart frequency**, selecione a frequência com que a reinicialização ocorre: diariamente, semanalmente, mensalmente ou uma vez. Se você selecionar **Weekly** ou **Monthly**, poderá especificar um ou mais dias específicos.
    - Para **Repeats every**, especifique a frequência com que você deseja que o agendamento seja executado.
    - Para **Start date**, especifique uma data de início para a primeira ocorrência do agendamento.
    - Para **Begin restart at**, especifique, no formato de 24 horas, a hora do dia para iniciar a reinicialização.
    - Para **Restart duration**:

        - Se você não quiser usar a reinicialização natural, selecione **Reiniciar todas as máquinas ao mesmo tempo** ou **Reiniciar todas as máquinas dentro de um período de tempo**.
        - Se você quiser usar a reinicialização natural, selecione **Reiniciar todas as máquinas após o esgotamento de todas as sessões**.

        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 a um grupo de entrega com uma ou mais sessões ativas é reiniciada quando todas as sessões são desconectadas.

> **Nota:**
>
> Os agendamentos de reinicialização natural só podem reiniciar máquinas com gerenciamento de energia.

- Em **Enviar notificação aos usuários**, escolha se deseja exibir uma mensagem de notificação nas máquinas aplicáveis antes do início de uma reinicialização. Por padrão, nenhuma mensagem é exibida.
- Se você optar por exibir uma mensagem 15 minutos antes do início da reinicialização, poderá escolher (em **Frequência de notificação**) repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não se repete.
- Insira o título e o texto da notificação. Não há texto padrão.

  Se você quiser que a mensagem inclua uma contagem regressiva para o reinício, inclua a variável **%m%**. A menos que você tenha escolhido reiniciar todas as máquinas ao mesmo tempo, a mensagem aparecerá em cada máquina no momento apropriado antes do reinício.

5. Clique em **Concluído** para aplicar as alterações e fechar a janela **Adicionar Agendamento de Reinício**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Reiniciar após esvaziamento

Outro valor de duração de reinício está disponível ao usar o PowerShell para criar ou atualizar um agendamento de reinício de máquina (`New-BrokerRebootSchedulev2` ou `Set-BrokerRebootSchedulev2`).

Ao habilitar o recurso de reinício após esvaziamento com o parâmetro `-UseNaturalReboot <Boolean>`, todas as máquinas são reiniciadas após esvaziar todas as sessões. Quando o tempo

de reinício é atingido, as máquinas são colocadas no estado de esvaziamento e, em seguida, reiniciadas quando todas as sessões são encerradas.

Este recurso é suportado para grupos de entrega que contêm máquinas de sessão única ou multi-sessão. Você pode usar esta opção para máquinas que são gerenciadas por energia e também para máquinas que não são gerenciadas por energia.

Em um ambiente local, este recurso é suportado apenas ao usar o PowerShell. O recurso não está disponível no Web Studio.

Editar, remover, habilitar ou desabilitar um agendamento de reinicialização

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Agendamento de Reinício**, selecione a caixa de seleção para um agendamento.

    - Para editar um agendamento, clique em **Editar**. Atualize a configuração do agendamento, usando as orientações em Criar um agendamento de reinício.
    - Para habilitar ou desabilitar um agendamento, clique em **Editar**. Selecione ou desmarque a caixa de seleção **Habilitar agendamento de reinício**.
    - Para remover um agendamento, clique em **Remover**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma tag aplicada às máquinas nas máquinas afetadas.

Reinicializações agendadas atrasadas devido a interrupção do banco de dados

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.
>
> Se ocorrer uma interrupção do banco de dados do site antes do início de um reinício agendado para máquinas (VDAs) em um grupo de entrega, os reinícios começarão quando a interrupção terminar. Isso pode ter resultados não intencionais.

Por exemplo, digamos que você agendou os reinícios de um grupo de entrega para ocorrerem fora do horário de produção (começando às 03:00). Uma interrupção do banco de dados do site ocorre uma hora antes do início de um reinício agendado (02:00). A interrupção dura seis horas (até às 08:00). O agendamento de reinício começa quando a conexão entre o Delivery Controller e

o banco de dados do site é restaurada. Os reinícios dos VDAs agora começam cinco horas após o agendamento original, resultando em VDAs reiniciando durante o horário de produção.

Para ajudar a evitar essa situação, você pode usar o parâmetro `MaxOvertimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além do horário de início agendado em que um agendamento de reinicialização pode começar.

- Se a conexão do banco de dados for restaurada dentro desse tempo (horário agendado + `MaxOvertimeStartMins`), as reinicializações do VDA começarão.
- Se a conexão do banco de dados não for restaurada dentro desse tempo, as reinicializações do VDA não começarão.
- Se este parâmetro for omitido ou tiver um valor zero, a reinicialização agendada começará quando a conexão com o banco de dados for restaurada, independentemente da duração da interrupção.

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell. Você não pode definir este valor ao configurar um agendamento de reinício no Web Studio.

Reinicializações agendadas para máquinas em modo de manutenção

> **Observação:**

> Este recurso está disponível apenas no PowerShell. A opção `IgnoreMaintenanceMode` é suportada com o Citrix Virtual Apps and Desktops 7 2006 e posterior.

> Para indicar se um agendamento de reinício afeta máquinas que estão em modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o seguinte cmdlet cria um agendamento que reinicia máquinas que estão em modo de manutenção (além de máquinas que não estão em modo de manutenção).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

O cmdlet a seguir modifica um agendamento de reinicialização existente.

`Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true`

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell.

Habilitar agendamento de reinicialização única

Se você quiser habilitar um agendamento de reinicialização único usando o PowerShell, use os seguintes comandos `BrokerCatalogRebootSchedule` do PowerShell para criar, modificar e excluir um agendamento de reinicialização:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Limitações:

- Um agendamento de reinicialização de catálogo associado a um catálogo sem um fuso horário configurado é criado, mas não é iniciado.
- Quando um agendamento de reinicialização de catálogo é criado, o agendamento de reinicialização é executado apenas nas VMs do catálogo pertencentes a um grupo de entrega.

Exemplo,

- Para criar um agendamento de reinicialização das VMs no catálogo chamado **BankTellers** para começar em Feb 3, 2022, entre 2h e 4h.

  ```
  C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
  BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
  -RebootDuration 120
  ```

- Para criar um agendamento de reinicialização das VMs no catálogo com UID 17 para começar em Feb 3, 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM é configurada para exibir uma caixa de mensagem com o título **AVISO: Reinicialização pendente**, e a mensagem **Salve seu trabalho**, em cada sessão de usuário.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- Para renomear o agendamento de reinicialização do catálogo chamado **Nome Antigo** para **Novo Nome**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- Para exibir todos os agendamentos de reinicialização de catálogo com UID 1 e, em seguida, renomear o agendamento de reinicialização de catálogo com o UID 1 para **Novo Nome**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Para definir o agendamento de reinicialização do catálogo chamado **Contabilidade** para exibir uma mensagem com o título **AVISO: Reinicialização pendente** e a mensagem **Salve seu trabalho**, dez minutos antes da reinicialização de cada VM. A mensagem aparece em cada sessão de usuário nessa VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- Para exibir todos os agendamentos de reinicialização desabilitados e, em seguida, habilitar todos os agendamentos de reinicialização desabilitados.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- Para definir o agendamento de reinicialização do catálogo com UID 17 para exibir a mensagem **Reiniciando em %m% minutos** quinze, dez e cinco minutos antes da reinicialização de cada VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- Para configurar o fuso horário para o catálogo chamado **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

Gerenciar carga de máquinas em grupos de entrega

Você pode gerenciar a carga apenas de máquinas de SO multi-sessão.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as condições ambientais atuais. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** Uma máquina de SO multi-sessão é considerada para balanceamento de carga somente quando o modo de manutenção está desativado.
- **Índice de carga do servidor:** Determina a probabilidade de um servidor que entrega máquinas de SO de várias sessões receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações para métricas de desempenho, como uso de CPU, disco e memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga.

  Um índice de carga do servidor de 10000 indica que o servidor está totalmente carregado. Se nenhum outro servidor estiver disponível, os usuários poderão receber uma mensagem de que a área de trabalho ou o aplicativo está indisponível ao iniciar uma sessão.

  Você pode monitorar o índice de carga no Director (Monitor), na pesquisa do Web Studio (Gerenciar) e no SDK.

  Nas exibições do console, para exibir a coluna **Índice de Carga do Servidor** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse em um cabeçalho de coluna e selecione **Selecionar Coluna**. Na **categoria Máquina**, selecione **Índice de Carga**.

  No SDK, use o cmdlet `Get-BrokerMachine`. Para obter detalhes, consulte CTX202150.
- **Configuração da política de tolerância de logon simultâneo**: O número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões do XenApp 6.x.)

Quando todos os servidores estão no nível ou acima da configuração de tolerância de logon simultâneo, a próxima solicitação de logon é atribuída ao servidor com o menor número de logons pendentes. Se mais de um servidor atender a esses critérios, o servidor com o menor índice de carga será selecionado.

Máquinas com gerenciamento de energia em um grupo de entrega

Você pode gerenciar a energia apenas de máquinas virtuais de SO de sessão única, não de máquinas físicas (incluindo máquinas de Acesso Remoto a PC). Máquinas de SO de sessão única com recursos de GPU não podem ser suspensas, portanto, as operações de desligamento falham. Para máquinas de SO de várias sessões, você pode criar um agendamento de reinicialização.

Em grupos de entrega que contêm máquinas em pool, as máquinas virtuais de SO de sessão única podem estar em um dos seguintes estados:

- Alocadas aleatoriamente e em uso
- Não alocadas e desconectadas

Em grupos de entrega que contêm máquinas estáticas, as máquinas virtuais de SO de sessão única podem ser:

- Alocadas permanentemente e em uso
- Alocadas permanentemente e desconectadas (mas prontas)
- Não alocados e desconectados

Durante o uso normal, os grupos de entrega estáticos geralmente contêm máquinas alocadas permanentemente e não alocadas. Inicialmente, todas as máquinas não são alocadas, exceto as alocadas manualmente quando o grupo de entrega foi criado. À medida que os usuários se conectam, as máquinas se tornam alocadas permanentemente. Você pode gerenciar totalmente a energia das máquinas não alocadas nesses grupos de entrega, mas apenas gerenciar parcialmente a energia das máquinas alocadas permanentemente.

- **Pools e buffers:** Para grupos de entrega em pool e grupos de entrega estáticos com máquinas não alocadas, um pool (neste caso) é um conjunto de máquinas não alocadas ou temporariamente alocadas que são mantidas em estado ligado, prontas para os usuários se conectarem. Um usuário obtém uma máquina imediatamente após o logon. O tamanho do pool (o número de máquinas mantidas ligadas) é configurável por hora do dia. Para grupos de entrega estáticos, use o SDK para configurar o pool.

  Um buffer é um conjunto extra de máquinas não alocadas em espera que são ligadas quando o número de máquinas no pool cai abaixo de um limite. O limite é uma porcentagem do

tamanho do grupo de entrega. Para grupos de entrega grandes, um número significativo de máquinas pode ser ligado quando o limite é excedido. Portanto, planeje os tamanhos dos grupos de entrega cuidadosamente ou use o SDK para ajustar o tamanho do buffer padrão.

- **Temporizadores de estado de energia:** Você pode usar temporizadores de estado de energia para suspender máquinas depois que os usuários se desconectarem por um período de tempo especificado. Por exemplo, as máquinas são suspensas automaticamente fora do horário de expediente se os usuários estiverem desconectados por pelo menos 10 minutos.

  Você pode configurar temporizadores para dias úteis e fins de semana, e para intervalos de pico e fora de pico.

- **Gerenciamento parcial de energia de máquinas alocadas permanentemente:** Para máquinas alocadas permanentemente, você pode definir temporizadores de estado de energia, mas não pools ou buffers. As máquinas são ligadas no início de cada período de pico e desligadas no início de cada período fora de pico. Você não tem o controle preciso que tem com máquinas não alocadas sobre o número de máquinas que se tornam disponíveis para compensar as máquinas que são consumidas.

Gerenciar energia de máquinas virtuais de SO de sessão única

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e clique em **Editar Grupo de Entrega** na barra de ações.
3. Na página **Gerenciamento de Energia**, selecione **Dias úteis** em **Gerenciar energia das máquinas**. Por padrão, os dias úteis são de segunda a sexta-feira.
4. Para grupos de entrega aleatórios, em **Máquinas a serem ligadas**, clique em **Editar** e especifique o tamanho do pool durante os dias úteis. Em seguida, selecione o número de máquinas a serem ligadas.
5. Em **Horas de pico**, defina as horas de pico e fora de pico para cada dia.
6. Defina os temporizadores de estado de energia para horas de pico e fora de pico durante os dias úteis: Em **Durante as horas de pico > Quando desconectado**, especifique o atraso (em minutos) antes de suspender qualquer máquina desconectada no grupo de entrega e selecione **Suspender**. Em **Durante as horas fora de pico > Quando desconectado**, especifique o atraso antes de desligar qualquer máquina com sessão encerrada no grupo de entrega e selecione **Desligar**. Este temporizador não está disponível para grupos de entrega com máquinas aleatórias.
7. Selecione **Fim de semana** em **Gerenciar energia das máquinas** e configure as horas de pico e os temporizadores de estado de energia para os fins de semana.

8. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Use o SDK para:

- Desligar, em vez de suspender, máquinas em resposta a temporizadores de estado de energia, ou se você quiser que os temporizadores sejam baseados em logoffs, em vez de desconexões.
- Alterar as definições padrão de dias úteis e fins de semana.
- Desabilitar o gerenciamento de energia. Consulte CTX217289.

Gerenciar energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas

> **Importante:**

> Este aprimoramento se aplica apenas a máquinas VDI com sessões desconectadas. Não se aplica a máquinas VDI com sessões encerradas.

> Em versões anteriores, uma máquina VDI em transição para um período de tempo em que uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Esse cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) em que nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir do Citrix Virtual Apps and Desktops 7 1909, a máquina é suspensa ou desligada quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega VDI:

- Defina `PeakDisconnectAction` como "Nada"
- Defina `OffPeakDisconnectAction` como "Desligar"
- Defina `OffPeakDisconnectTimeout` como "10"

Para obter mais informações sobre a ação de desconexão na política de energia, 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 VDI com uma sessão desconectada durante os horários de pico permanecia ligada ao fazer a transição do pico para fora do pico. A partir do Citrix Virtual Apps and Desktops 7 1909, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina VDI na transição de período. Como resultado, a máquina é desligada 10 minutos após a transição para fora do pico.

Se você quiser reverter para o comportamento anterior (ou seja, não realizar nenhuma ação em máquinas que fazem a transição de pico para fora de pico ou de fora de pico para pico com sessões desconectadas), faça uma das seguintes opções:

- Defina o valor do registro `LegacyPeakTransitionDisconnectedBehaviour` como `1`, o equivalente a *true*, que habilita o comportamento anterior. Por padrão, o valor é `0`, ou *false*, que aciona ações de política de energia de desconexão na transição de período.
  - Caminho: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Nome: `LegacyPeakTransitionDisconnectedBehaviour`
  - Tipo: `REG_DWORD`
  - Dados: `0x00000001 (1)`
- Configure a configuração usando o comando PowerShell `Set-BrokerServiceConfigurationData`. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações da política de energia possam ser aplicadas a ela na transição de período:

- Ter uma sessão desconectada.
- Não ter ações de energia pendentes.
- Pertencer a um grupo de entrega VDI (sessão única) que faz a transição 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 faz a transição para um período onde uma ação de energia é atribuída.

Alterar a porcentagem de VDAs em estado ligado para catálogos

1. Ajuste os horários de pico para o grupo de entrega na seção **Gerenciamento de energia** do grupo de entrega.
2. Anote o nome do Grupo de Área de Trabalho.
3. Com privilégios de administrador, inicie o PowerShell e execute os seguintes comandos. Substitua "Desktop Group Name" pelo nome do seu grupo de área de trabalho que tem uma porcentagem alterada de VDAs em execução.

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   Um valor de 100 significa que 100% dos VDAs estão no estado pronto.
4. Verifique a solução executando:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```

   Nome do grupo de desktops(/en-us/citrix-virtual-apps-desktops/2407/media/desktop-group-name.png)

Pode levar até uma hora para que as alterações entrem em vigor.

Para desligar os VDAs depois que o usuário fizer logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

Para reiniciar os VDAs durante o horário de pico, para que estejam prontos para os usuários depois que eles fizerem logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

Sessões

- Fazer logoff ou desconectar uma sessão, ou enviar uma mensagem aos usuários
- Configurar o pré-lançamento e a permanência da sessão
- Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção
- Configurar o roaming de sessão

Fazer logoff ou desconectar uma sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** na barra de ações.
3. No painel do meio, selecione a máquina, selecione **View Sessions** na barra de ações e, em seguida, selecione uma sessão.
    - Alternativamente, no painel do meio, selecione a guia **Session** e, em seguida, selecione uma sessão.
4. Para fazer logoff de uma sessão, selecione **Log off** na barra de ações. A sessão é fechada e o usuário é desconectado. A máquina fica disponível para outros usuários, a menos que seja alocada para um usuário específico.
5. Para desconectar uma sessão, selecione **Disconnect** na barra de ações. Os aplicativos continuam a ser executados na sessão e a máquina permanece alocada para esse usuário. O usuário pode se reconectar à mesma máquina.

Você pode configurar temporizadores de estado de energia para máquinas de SO de sessão única para manipular automaticamente sessões não utilizadas. Para obter detalhes, consulte Máquinas gerenciadas por energia.

Enviar uma mensagem para um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **View Machines** na barra de ações.
3. No painel do meio, selecione uma máquina para a qual você deseja enviar uma mensagem.
4. Na barra de ações, selecione **Exibir Sessões**.
5. No painel do meio, selecione todas as sessões e, em seguida, selecione **Enviar Mensagem** na barra de ações.
6. Digite sua mensagem e clique em **OK**. Você pode especificar o nível de severidade, se necessário. As opções incluem **Crítico**, **Pergunta**, **Aviso** e **Informação**.

Alternativamente, você pode enviar uma mensagem usando o Citrix Director. Para obter mais informações, consulte Enviar mensagens para usuários.

Configurar o pré-lançamento e a permanência da sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas de SO multi-sessão.

Os recursos de pré-lançamento de sessão e persistência de sessão ajudam usuários especificados a acessar aplicativos rapidamente, iniciando sessões antes que sejam solicitadas (pré-lançamento de sessão) e mantendo as sessões de aplicativo ativas depois que um usuário fecha todos os aplicativos (persistência de sessão).

Por padrão, o pré-lançamento de sessão e a permanência de sessão não são usados. Uma sessão é iniciada (lançada) quando um usuário inicia um aplicativo e permanece ativa até que o último aplicativo aberto na sessão seja fechado.

Considerações:

- O grupo de entrega deve suportar aplicativos, e as máquinas devem estar executando um VDA para SO multi-sessão, versão mínima 7.6.
- Esses recursos são suportados apenas ao usar o aplicativo Citrix Workspace para Windows e também exigem configuração extra do aplicativo Citrix Workspace. Para obter instruções, procure por pré-lançamento de sessão na documentação do produto para sua versão do aplicativo Citrix Workspace para Windows.
- O Citrix Workspace app para HTML5 não é compatível.
- Ao usar o pré-lançamento de sessão, se a máquina de um usuário for colocada em modo de suspensão ou hibernação, o pré-lançamento não funciona (independentemente das configurações de pré-lançamento de sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário sair do Citrix Workspace app, a sessão é encerrada e o pré-lançamento não se aplica mais.
- Ao usar o pré-lançamento de sessão, as máquinas cliente físicas não podem usar as funções de gerenciamento de energia de suspensão ou hibernação. Os usuários da máquina cliente podem bloquear suas sessões, mas não devem fazer logoff.
- Sessões pré-lançadas e persistentes consomem uma licença simultânea, mas apenas quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. Sessões pré-lançadas e persistentes não utilizadas são desconectadas após 15 minutos por padrão. Este valor pode ser configurado no PowerShell (cmdlet `New/Set-BrokerSessionPreLaunch`).
- O planejamento e o monitoramento cuidadosos dos padrões de atividade dos seus usuários são essenciais para adaptar esses recursos para que se complementem. A configuração ideal equilibra os benefícios da disponibilidade antecipada de aplicativos para os usuários com o custo de manter as licenças em uso e os recursos alocados.
- Você também pode configurar o pré-lançamento de sessão para um horário agendado no Citrix Workspace app.

Por quanto tempo as sessões pré-lançadas e persistentes não utilizadas permanecem ativas

Existem várias maneiras de especificar por quanto tempo uma sessão não utilizada permanece ativa se o usuário não iniciar um aplicativo: um tempo limite configurado e limites de carga do servidor. Você pode configurar todos eles. O evento que ocorre primeiro faz com que a sessão não utilizada seja encerrada.

- **Tempo limite:** Um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-lançada ou persistente não utilizada permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-lançadas terminam antes de fornecerem ao usuário o benefício de um acesso mais rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário de entrada podem ser negadas porque o servidor não tem recursos suficientes.

  Você pode habilitar esse tempo limite apenas no SDK (cmdlet `New/Set-BrokerSessionPreLaunch`), não no console de gerenciamento. Se você desabilitar o tempo limite, ele não aparecerá na exibição do console para esse grupo de entrega ou nas páginas **Editar Grupo de Entrega**.
- **Limites:** O encerramento automático de sessões pré-lançadas e persistentes com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, assumindo que os recursos do servidor estejam disponíveis. As sessões pré-lançadas e persistentes não utilizadas não causam conexões negadas porque são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

  Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-lançamento ou persistência por mais tempo são encerradas. As sessões são encerradas uma a uma em intervalos de um minuto até que a carga caia abaixo do limite. Enquanto o limite é excedido, nenhuma nova sessão de pré-lançamento é iniciada.

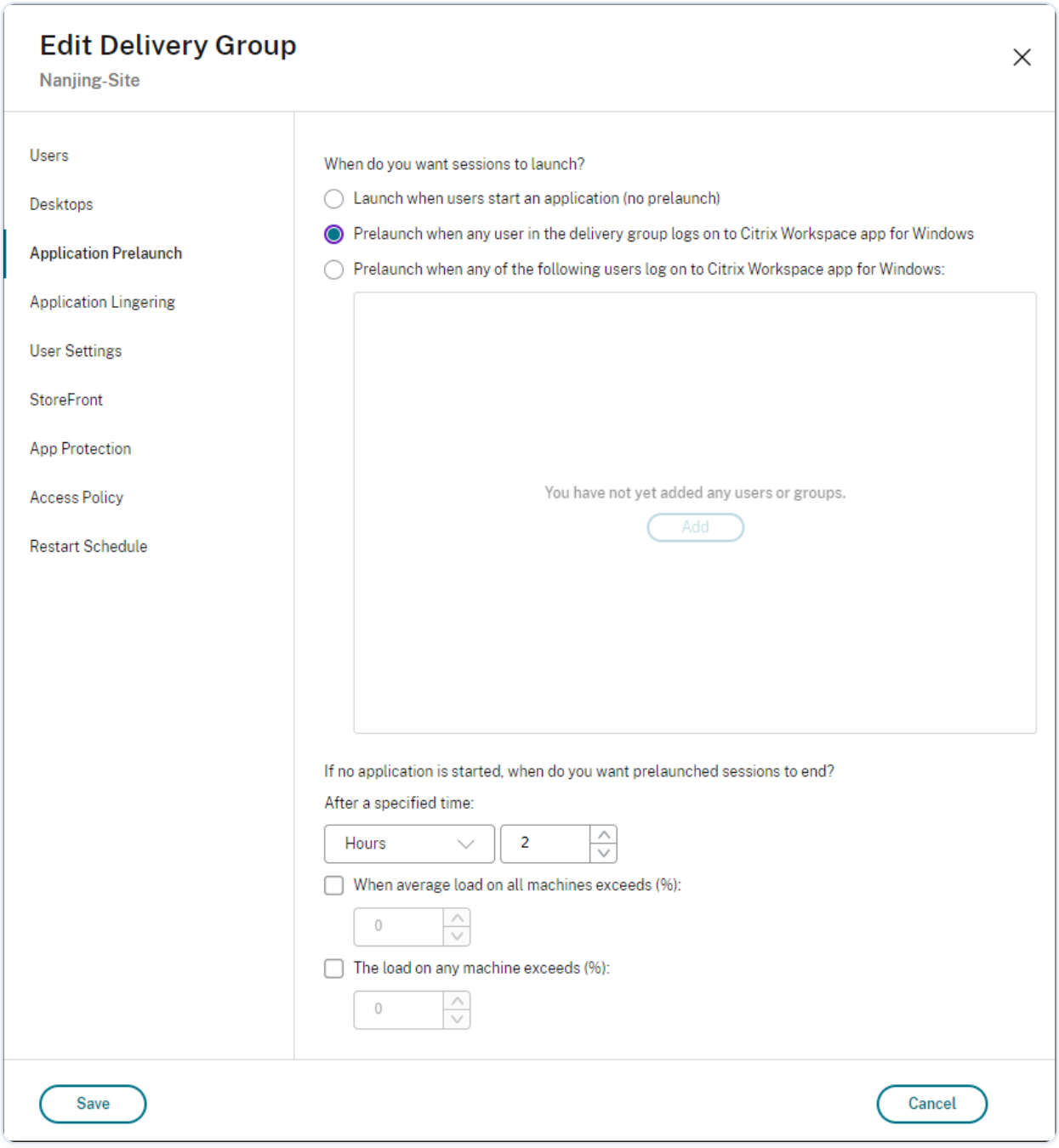
Servidores com VDAs que não se registraram em um Controller e servidores em modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-lançamento e persistentes sejam encerradas automaticamente para liberar capacidade.

Para habilitar o pré-lançamento de sessão

1. Selecione um grupo e, em seguida, clique em **Editar Grupo de Entrega** na barra de ações.

2. Na página **Pré-lançamento de Aplicativos**, ative o pré-lançamento de sessão escolhendo quando as sessões são iniciadas:

   - Quando um usuário inicia um aplicativo. Esta é a configuração padrão. O pré-lançamento de sessão está desativado.
   - Quando qualquer usuário no grupo de entrega faz logon no Citrix Workspace app para Windows.
   - Quando qualquer pessoa em uma lista de usuários e grupos de usuários faz logon no Citrix Workspace app para Windows. Certifique-se de especificar também usuários ou grupos de usuários se você escolher esta opção.



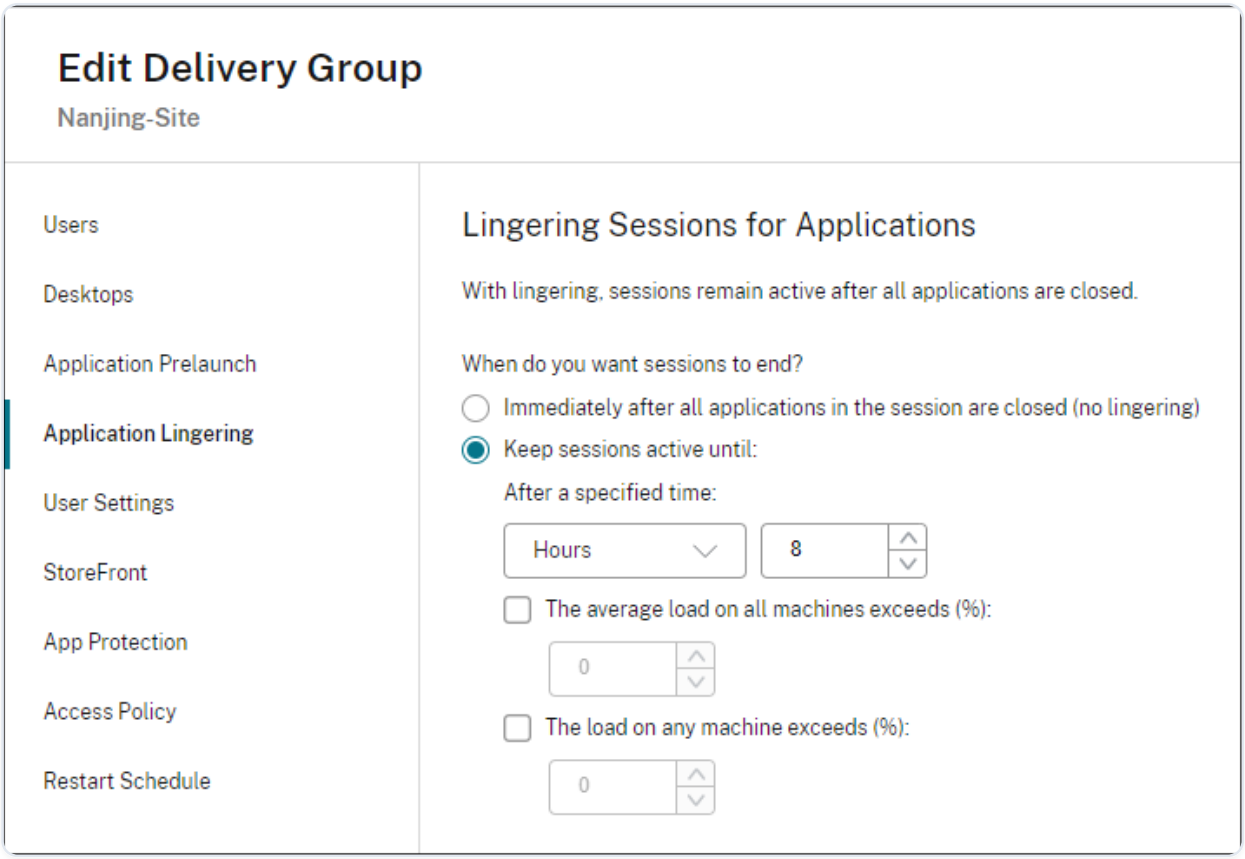
3. Uma sessão pré-lançada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-lançada não for usada), as seguintes configurações afetam por quanto tempo essa sessão permanece ativa.

   - Quando um intervalo de tempo especificado expira. Você pode alterar o intervalo de tempo (1–99 dias, 1–2376 horas ou 1–142.560 minutos)
   - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada (1–99%)
   - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada (1–99%)

   Recapitulação: Uma sessão pré-lançada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado decorre ou um limite de carga especificado é excedido.

Para habilitar a permanência da sessão

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Editar Grupo de Entrega** na barra de ações.
3. Na página **Permanência do Aplicativo**, ative a permanência da sessão selecionando **Manter sessões ativas até**.



4. Várias configurações afetam por quanto tempo uma sessão persistente permanece ativa se o usuário não iniciar outro aplicativo.

    - Quando um intervalo de tempo especificado expira. Você pode alterar o intervalo de tempo: 1–99 dias, 1–2376 horas ou 1–142.560 minutos.
    - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada: 1–99%.
    - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada: 1–99%.

    Recapitulação: Uma sessão persistente permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado expira ou um limite de carga especificado é excedido.

Controlar a reconexão de sessão quando desconectado da máquina em modo de manutenção

> **NOTA:**
>
> Este recurso está disponível apenas no PowerShell.
>
> Você pode controlar se as sessões que são desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes da versão 2106, a reconexão não era permitida para sessões de desktop agrupadas de sessão única que haviam sido desconectadas de máquinas em modo de manutenção. A partir da versão 2106, você pode configurar um grupo de entrega para permitir ou proibir reconexões (independentemente do tipo de sessão) após a desconexão de uma máquina em modo de manutenção.

Ao criar ou editar um grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use o parâmetro `-AllowReconnectInMaintenanceMode <boolean>` para permitir ou proibir reconexões para máquinas que foram desconectadas de uma máquina em modo de manutenção.

- Quando definido como true, as sessões podem se reconectar às máquinas do grupo.
- Quando definido como falso, as sessões não podem se reconectar às máquinas no grupo.

Valores padrão:

- Sessão única: Desabilitado
- Multi-sessão: Habilitado

Configurar o roaming de sessão

Por padrão, o roaming de sessão é habilitado para grupos de entrega. As sessões transitam entre os dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos ficam simultaneamente disponíveis em ambos os dispositivos. Você pode visualizar os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo ou se as sessões atuais existem. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem. Alternativamente, você pode usar o PowerShell. Para obter mais informações, consulte Roaming de sessão.

Configurar o roaming de sessão para aplicativos

Para configurar o roaming de sessão para aplicativos, siga estas etapas:

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar Grupo de Entrega** na barra de ações.
3. Na página **Usuários**, habilite o roaming de sessão selecionando a caixa de seleção **As sessões transitam com os usuários à medida que eles se movem entre os dispositivos**.
    - Quando habilitado, se um usuário iniciar uma sessão de aplicativo e depois se mover para outro dispositivo, a mesma sessão será usada e estará disponível em ambos os dispositivos. Quando desabilitado, a sessão não fará mais roaming entre os dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

Configurar roaming de sessão para desktops

Para configurar o roaming de sessão para um desktop, siga estas etapas:

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Desktops**, selecione o desktop e selecione **Edit**.
4. Habilite o roaming de sessão selecionando a caixa de seleção **Roaming de sessão**.

- Quando ativado, se o usuário iniciar o desktop e depois mudar para outro dispositivo, a mesma sessão será usada e os aplicativos estarão disponíveis em ambos os dispositivos. Quando desativado, a sessão não faz mais roaming entre os dispositivos.

Selecione **OK** para aplicar as alterações e fechar a janela.

Aplicativos

Visualize e adicione aplicativos a um grupo de entrega.

1. No console, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo. Se este grupo contiver aplicativos, **Visualizar Aplicativos** aparecerá na barra de ações.
3. Selecione **Visualizar Aplicativos**. Você será direcionado para o nó **Aplicativos**, onde todos os aplicativos disponíveis neste grupo aparecerão.
4. Para adicionar mais aplicativos a este grupo, vá para o nó **Grupos de Entrega**, selecione o grupo e selecione **Adicionar Aplicativos** na barra de ações.

Solução de problemas

- VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização de recursos que de outra forma estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador pode solucionar. A exibição de detalhes fornece informações de solução de problemas no assistente de criação de catálogo e depois que você adiciona um catálogo a um grupo de entrega.

  Depois de criar um grupo de entrega, o painel de detalhes de um grupo de entrega indica o número de máquinas que podem ser registradas, mas não estão. Por exemplo, uma ou mais máquinas estão ligadas e não em modo de manutenção, mas não estão atualmente registradas em um Controller. Ao visualizar uma máquina "não registrada, mas deveria estar", revise a guia **Solucionar problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

  Para mensagens sobre o nível funcional, consulte Versões de VDA e níveis funcionais.

  Para obter informações sobre a solução de problemas de registro de VDA, consulte CTX136668.
- Na exibição de um grupo de entrega, a **versão do VDA instalada** no painel de detalhes pode ser diferente da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas com status de **Estado de Energia Desconhecido**, consulte CTX131267 para obter orientação.

Criar grupos de aplicativos

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Grupos de aplicativos permitem gerenciar coleções de aplicativos. Crie grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega. Ou, aplicativos 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. Associe grupos de entrega a mais de um grupo de aplicativos e associe um grupo de aplicativos a mais de um grupo de entrega.

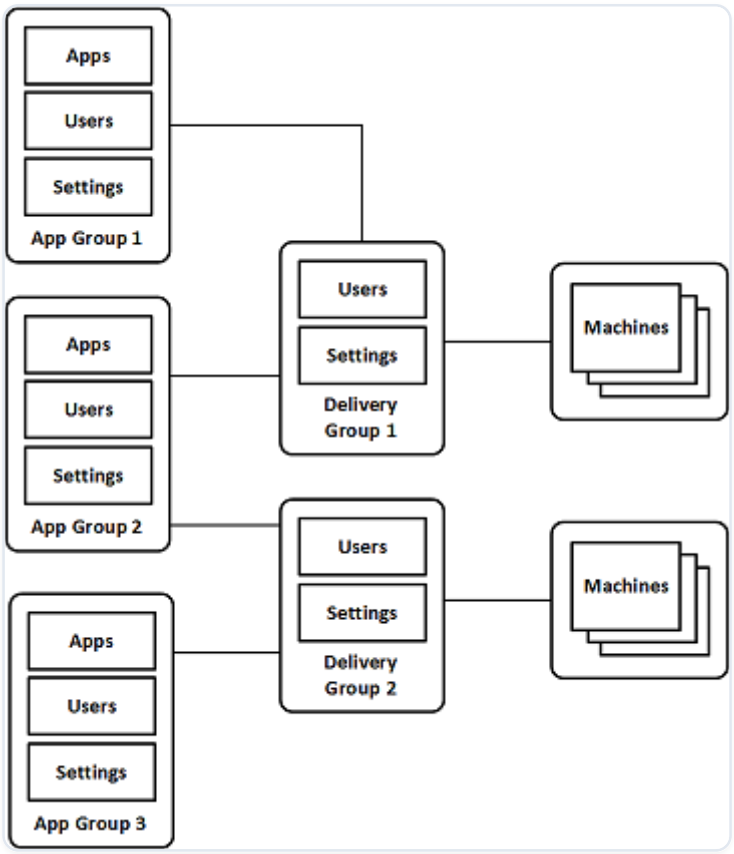
O uso de grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega:

- O agrupamento lógico de aplicativos e suas configurações permite gerenciar esses aplicativos como uma única unidade. Por exemplo, você não precisa adicionar (publicar) o mesmo aplicativo a grupos de entrega individuais um por um.
- O compartilhamento de sessão entre grupos de aplicativos pode conservar o consumo de recursos. Em outros casos, desabilitar o compartilhamento de sessão entre grupos de aplicativos pode ser benéfico.
- Você pode usar o recurso de restrição de tags para publicar aplicativos de um grupo de aplicativos, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Com as restrições de tags, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de máquinas extras. Uma restrição de tag pode ser pensada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Configurações de exemplo

Exemplo 1:

O gráfico a seguir mostra uma implantação do Citrix Virtual Apps and Desktops 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 são usadas. (Embora não mostrado, as máquinas estão em catálogos de máquinas.)

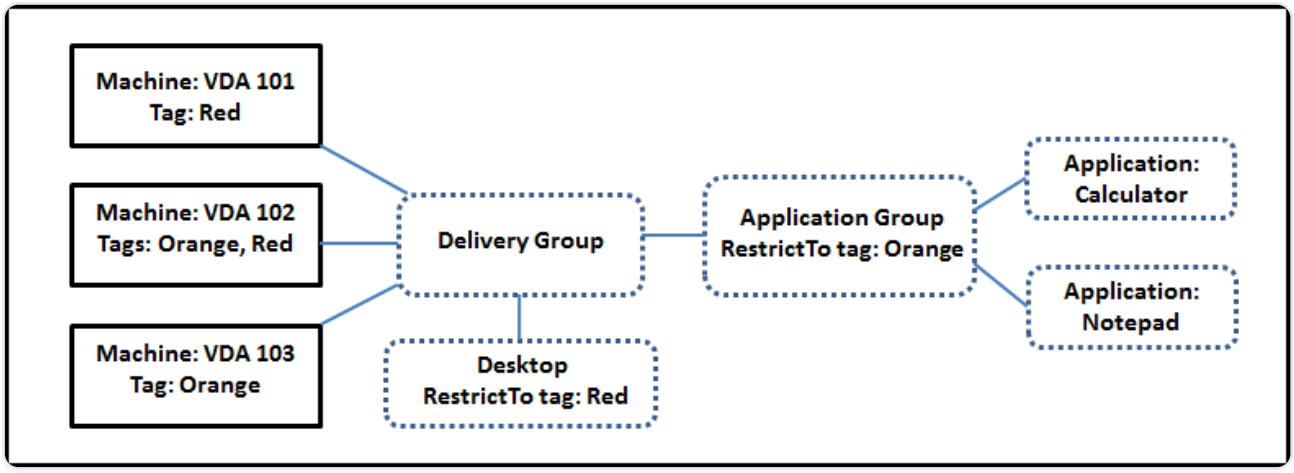
O grupo de aplicativos 1 está associado ao grupo de entrega 1. Os usuários especificados no grupo de aplicativos 1 acessam os aplicativos no grupo de aplicativos 1. Esses grupos só aparecem enquanto também estiverem na lista de usuários do grupo de entrega 1. Esta configuração segue a orientação de que a lista de usuários para um grupo de aplicativos é um subconjunto (uma restrição) das listas de usuários para os grupos de entrega associados. As configurações no grupo de aplicativos 1 (como compartilhamento de sessão de aplicativo entre grupos de aplicativos, grupos de entrega associados) se aplicam aos aplicativos e usuários nesse grupo. As configurações no grupo de entrega 1 se aplicam aos usuários nos grupos de aplicativos 1 e 2, porque esses grupos de aplicativos foram associados a esse grupo de entrega.

O grupo de aplicativos 2 está associado a dois grupos de entrega: 1 e 2. Cada um desses grupos de entrega recebe uma prioridade no grupo de aplicativos 2, indicando a ordem em que os grupos

de entrega são verificados quando um aplicativo é iniciado. Grupos de entrega com prioridade igual são balanceados por carga. Os usuários especificados no grupo de aplicativos 2 acessam os aplicativos no grupo de aplicativos 2. No entanto, eles também devem aparecer nas listas de usuários para o grupo de entrega 1 e o grupo de entrega 2.

Exemplo 2:

Este layout simples usa restrições de tags para limitar quais máquinas são consideradas para determinados lançamentos de desktop e aplicativos. O site possui um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.



Tags foram adicionadas a cada uma das três máquinas (VDA 101–103).

O grupo de aplicativos foi criado com a restrição de tag "Orange". Cada um de seus aplicativos é iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Orange", VDA 102 e 103.

Para exemplos mais abrangentes e orientações sobre o uso de restrições de tag em grupos de aplicativos (e para desktops), consulte Tags.

Orientação e considerações

A Citrix recomenda adicionar aplicativos a grupos de aplicativos ou a grupos de entrega, mas não a ambos. Caso contrário, a complexidade adicional de ter aplicativos em dois tipos de grupo pode dificultar o gerenciamento.

Por padrão, um grupo de aplicativos é habilitado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado. Consulte Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. Este processo requer:

1. Atualizar VDAs nas máquinas usadas no grupo de entrega.
2. Atualizar os catálogos de máquinas que contêm essas máquinas.
3. Atualizar o grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ser no mínimo da versão 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo se refere a "associar" um aplicativo a mais de um grupo de aplicativos. Ele diferencia essa ação de adicionar instâncias desse aplicativo de uma fonte disponível. Da mesma forma, os grupos de entrega são associados a grupos de aplicativos, em vez de serem adições ou componentes uns dos outros.

Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão de aplicativo está habilitado, todos os aplicativos são iniciados na mesma sessão de aplicativo. Isso economiza os custos associados ao lançamento de mais sessões de aplicativo e permite o uso de recursos de aplicativo que envolvem a área de transferência, como operações de copiar e colar. No entanto, em algumas situações, você pode desativar o compartilhamento de sessão.

Ao usar grupos de aplicativos, você pode configurar o compartilhamento de sessão de aplicativo das três maneiras a seguir, que estendem o comportamento padrão de compartilhamento de sessão disponível ao usar apenas grupos de entrega:

- Compartilhamento de sessão habilitado entre grupos de aplicativos.
- Compartilhamento de sessão habilitado apenas entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desabilitado.

Compartilhamento de sessão entre grupos de aplicativos

Você pode habilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos ou pode desabilitá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo em que habilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  O grupo de aplicativos 1 contém aplicativos do Microsoft Office, como Word e Excel. O grupo de aplicativos 2 contém outros aplicativos, como Bloco de Notas e Calculadora, e ambos os grupos de aplicativos estão anexados ao mesmo grupo de entrega. Um usuário que tem acesso a ambos os grupos de aplicativos inicia uma sessão de aplicativo ao iniciar o Word e, em seguida, inicia o Bloco de Notas. Se o controlador descobrir que 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 tag excluir a máquina em que a sessão está sendo executada — então uma nova sessão em uma máquina adequada é criada em vez de usar o compartilhamento de sessão.
- **Um exemplo em que desabilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  Uma configuração com um conjunto de aplicativos que não interoperam bem com outros aplicativos instalados nas mesmas máquinas. Como duas versões diferentes da mesma suíte de software ou duas versões diferentes do mesmo navegador da web. Você prefere não permitir que um usuário inicie ambas as versões na mesma sessão.

  Crie um grupo de aplicativos para cada versão da suíte de software e adicione os aplicativos de cada versão da suíte de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desabilitado para cada um desses grupos de aplicativos, um usuário especificado nesses grupos poderá executar aplicativos da mesma versão na mesma sessão. O usuário ainda pode executar outros aplicativos ao mesmo tempo, mas não na mesma sessão. Ao iniciar um dos aplicativos de versão diferente, ou qualquer aplicativo que não esteja contido em um grupo de aplicativos, esse aplicativo é iniciado em uma nova sessão.

Este recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de sandboxing de segurança. Não é infalível e não pode impedir que os usuários iniciem aplicativos em suas sessões por outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver com capacidade máxima, novas sessões não serão iniciadas nela. Novos aplicativos são iniciados em sessões existentes na máquina conforme necessário, usando o compartilhamento de sessão.

Você só pode disponibilizar sessões pré-iniciadas para grupos de aplicativos que permitem o compartilhamento de sessão de aplicativos. (As sessões que usam o recurso de permanência de sessão estão disponíveis para todos os grupos de aplicativos.) Esses recursos devem ser habilitados e configurados em cada um dos grupos de entrega associados ao grupo de aplicativos. Você não pode configurá-los nos grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Desabilitar o compartilhamento de sessão dentro de um grupo de aplicativos

Você pode impedir o compartilhamento de sessão de aplicativo entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo de quando desabilitar o compartilhamento de sessão dentro de grupos de aplicativos é útil:**

  Você deseja que seus usuários acessem várias sessões simultâneas em tela cheia de um aplicativo em monitores separados.

  Você cria um grupo de aplicativos e adiciona os aplicativos a ele.

Por padrão, o compartilhamento de sessão de aplicativo é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Criar um grupo de aplicativos

Para criar um grupo de aplicativos:

1. Faça login no Web Studio.
2. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
3. Para organizar grupos de aplicativos usando pastas, crie pastas na pasta raiz **Grupos de Aplicativos**.

4. Selecione a pasta onde você deseja criar o grupo e clique em **Criar Grupo de Aplicativos**. O assistente de criação de grupo é iniciado com uma página de **Introdução**. Você pode remover a página de futuras inicializações deste assistente.
5. Siga o assistente para configurar as definições nas páginas descritas abaixo. Quando terminar cada página, selecione **Avançar** até chegar à página de **Resumo**.

Etapa 1. Grupos de Entrega

A página **Grupos de Entrega** lista todos os grupos de entrega, com o número de máquinas que cada grupo contém.

- A lista **Grupos de Entrega Compatíveis** contém grupos de entrega que você pode selecionar. Grupos de entrega compatíveis contêm máquinas de SO de sessão única ou multi-sessão aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Grupos de Entrega Incompatíveis** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como conter máquinas atribuídas estaticamente.

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando o assistente de criação de grupo de aplicativos é confirmado.

Embora você possa criar um grupo de aplicativos que não tenha grupos de entrega associados (talvez para organizar aplicativos ou para servir como armazenamento para aplicativos não utilizados atualmente), o grupo de aplicativos não pode ser usado para entregar aplicativos até que especifique pelo menos um grupo de entrega. Além disso, você não pode adicionar aplicativos ao grupo de aplicativos a partir da fonte do menu **Do Iniciar** se nenhum grupo de entrega for especificado.

Os grupos de entrega que você seleciona especificam as máquinas que são usadas para entregar aplicativos. Marque as caixas de seleção ao lado dos grupos de entrega que você deseja associar ao grupo de aplicativos.

Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista suspensa.

Etapa 2. Usuários

Especifique os usuários do aplicativo no grupo de aplicativos. Permita todos os usuários e grupos de usuários nos grupos de entrega que você selecionou na página anterior, ou selecione usuários e grupos de usuários específicos desses grupos de entrega. Se você restringir o uso a usuários especificados, então apenas os usuários especificados no grupo de entrega, o grupo de aplicativos poderá acessar os aplicativos neste grupo. Essencialmente, a lista de usuários no grupo de aplicativos fornece um filtro nas listas de usuários nos grupos de entrega.

Habilitar ou desabilitar o uso de aplicativos por usuários não autenticados está disponível apenas em grupos de entrega, não em grupos de aplicativos.

Para obter informações sobre onde as listas de usuários são especificadas em uma implantação, consulte Onde as listas de usuários são especificadas.

Etapa 3. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e um com o mesmo nome já existir nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você concordar com o nome exclusivo sugerido, o aplicativo será adicionado com esse novo nome. Caso contrário, você deve renomeá-lo antes que possa ser adicionado. Para obter detalhes, consulte Gerenciar pastas de aplicativos.
- Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Consulte Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Nome do aplicativo (para usuário)** no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.
- Quando você adiciona um aplicativo a mais de um grupo de aplicativos, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo foi adicionado.

Clique em **Adicionar** no menu suspenso para exibir as fontes do aplicativo.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta fonte não pode ser selecionada se você selecionou qualquer um dos seguintes:

  - Grupos de aplicativos que não têm grupos de entrega associados.
  - Grupos de aplicativos com grupos de entrega associados que não contêm máquinas.
  - Um grupo de entrega que não contém máquinas.

- **Definido manualmente:** Aplicativos localizados no site ou em outro lugar da sua rede. Ao selecionar esta fonte, uma nova página é aberta onde você digita o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Após inserir essas informações, clique em **OK**.
- **Existente**: Aplicativos adicionados anteriormente ao site. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**. Esta fonte não pode ser selecionada se o site não tiver aplicativos.
- **App-V**: Aplicativos em pacotes App-V. Ao selecionar esta fonte, uma nova página é aberta onde você seleciona **Servidor App-V** ou **Biblioteca de Aplicativos**. Na exibição resultante, marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V. Esta fonte não pode ser selecionada (ou pode não aparecer) se o App-V não estiver configurado para o site.

Conforme observado, certas entradas no menu suspenso **Adicionar** não são selecionáveis se não houver uma fonte válida desse tipo. Fontes incompatíveis não são listadas (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos, então essa fonte não é listada ao criar um grupo de aplicativos).

Etapa 4. Escopos

Esta página aparece somente se você tiver criado anteriormente um escopo personalizado. Por padrão, o escopo **Todos** é selecionado. Para obter mais informações, consulte Administração delegada.

Etapa 5. Resumo

Insira um nome para o grupo de aplicativos. Você também pode (opcionalmente) inserir uma descrição.

Revise as informações de resumo e clique em **Concluir**.

Gerenciar grupos de aplicativos

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Este artigo descreve como gerenciar os grupos de aplicativos que você criou.

Consulte Aplicativos para obter informações sobre como gerenciar aplicativos em grupos de aplicativos ou grupos de entrega, incluindo como:

- Adicionar ou remover aplicativos em um grupo de aplicativos.
- Alterar associações de grupo de aplicativos.

O gerenciamento de grupos de aplicativos requer as permissões de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Habilitar ou desabilitar um grupo de aplicativos

Quando um grupo de aplicativos está habilitado, ele pode entregar os aplicativos que foram adicionados a ele. Desabilitar um grupo de aplicativos desabilita cada aplicativo nesse grupo. No entanto, se esses aplicativos também estiverem associados a outros grupos de aplicativos habilitados, eles poderão ser entregues a partir desses outros grupos. Se o aplicativo foi explicitamente adicionado a grupos de entrega associados ao grupo de aplicativos, desabilitar o grupo de aplicativos não afeta os aplicativos nesses grupos de entrega.

Um grupo de aplicativos é habilitado quando você o cria. Você não pode alterar essa configuração ao criar o grupo.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.

2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, marque ou desmarque a caixa de seleção **Habilitar Grupo de Aplicativos**.
4. Clique em **Aplicar** para manter a janela aberta ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Habilitar ou desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração ao criar o grupo. Para obter mais informações, consulte Compartilhamento de sessão com grupos de aplicativos.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, marque ou desmarque a caixa de seleção **Habilitar compartilhamento de sessão de aplicativo entre Grupos de Aplicativos**.
4. Clique em **Aplicar** para manter a janela aberta ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Desabilitar o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é habilitado por padrão ao criar um grupo de aplicativos. Se você desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanecerá habilitado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão de aplicativo desabilitado entre os aplicativos que eles contêm. Em algumas circunstâncias, essa opção é desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não-seamless em janelas de aplicativo em tamanho real em monitores separados.

Quando você desabilita o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão de aplicativo. Se uma sessão desconectada adequada estiver disponível e executando o mesmo aplicativo, ela será reconectada. Por exemplo, ao iniciar o Bloco de Notas com uma sessão desconectada com o Bloco de Notas em execução, essa sessão é reconectada em vez de criar uma nova. Quando várias sessões desconectadas adequadas estão disponíveis, uma das sessões é escolhida para reconectar, de forma aleatória, mas determinística. Quando a situação ocorre novamente nas mesmas circunstâncias, a mesma sessão é escolhida, mas a sessão não é necessariamente previsível de outra forma.

Use o SDK do PowerShell para desabilitar o compartilhamento de sessão de aplicativo para todos os aplicativos em um grupo de aplicativos existente ou para criar um grupo com o compartilhamento de sessão de aplicativo desabilitado.

Exemplos de cmdlets do PowerShell

Para desabilitar o compartilhamento de sessão, use os cmdlets do Broker PowerShell `New-BrokerApplicationGroup` ou `Set-BrokerApplicationGroup` com o parâmetro `SessionSharingEnabled` definido como `False` e o parâmetro `SingleAppPerSession` definido como `True`.

- Por exemplo, para criar um grupo de aplicativos com o compartilhamento de sessão de aplicativo desabilitado para todos os aplicativos no grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Por exemplo, para desabilitar o compartilhamento de sessão de aplicativo entre todos os aplicativos em um grupo de aplicativos existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

Considerações

- Para habilitar a propriedade `SingleAppPerSession`, você deve definir a propriedade `SessionSharingEnabled` como False. As duas propriedades não devem ser habilitadas ao mesmo tempo. O parâmetro `SessionSharingEnabled` refere-se ao compartilhamento de sessões entre grupos de aplicativos.

- O compartilhamento de sessão de aplicativo funciona apenas para aplicativos associados a grupos de aplicativos, mas não associados a grupos de entrega. Todos os aplicativos associados diretamente a um grupo de entrega compartilham a sessão por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, certifique-se de que os grupos não tenham configurações conflitantes. Por exemplo, um grupo com a opção definida como `True` e a opção de outro grupo definida como `False` resulta em comportamento imprevisível.

Renomear um grupo de aplicativos

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Renomear Grupo de Aplicativos** na barra de ações.
3. Especifique o novo nome exclusivo e, em seguida, clique em **OK**.

Adicionar, remover ou alterar a prioridade das associações de grupo de entrega com um grupo de aplicativos

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando a caixa de diálogo **Editar Grupo de Aplicativos** é confirmada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.

4. Para adicionar grupos de entrega, clique em **Adicionar**. Marque as caixas de seleção dos grupos de entrega disponíveis. (Grupos de entrega incompatíveis não podem ser selecionados.) Ao finalizar suas seleções, clique em **OK**.
5. Para remover grupos de entrega, marque as caixas de seleção dos grupos que deseja remover e, em seguida, clique em **Remover**. Confirme a exclusão quando solicitado.
6. Para alterar a prioridade dos grupos de entrega, marque a caixa de seleção do grupo de entrega e, em seguida, clique em **Editar Prioridade**. Insira a prioridade (0 = mais alta) e, em seguida, clique em **OK**.
7. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover uma restrição de tag em um grupo de aplicativos

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais máquinas são consideradas para o lançamento de aplicativos. Revise as considerações e precauções em Tags.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.
4. Para adicionar uma restrição de tag, selecione **Restringir lançamentos a máquinas com a tag** e, em seguida, selecione a tag na lista suspensa.
5. Para alterar ou remover uma restrição de tag, selecione uma tag diferente ou remova a restrição de tag completamente desmarcando **Restringir lançamentos a máquinas com esta tag**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Adicionar ou remover usuários em um grupo de aplicativos

Para obter informações detalhadas sobre usuários, consulte Criar grupos de aplicativos.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.

2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Usuários**. Indique se você deseja permitir que todos os usuários nos grupos de entrega associados usem aplicativos no grupo de aplicativos, ou apenas usuários e grupos específicos. Para adicionar usuários, clique em **Adicionar** e, em seguida, especifique os usuários que deseja adicionar. Para remover usuários, selecione um ou mais usuários e, em seguida, clique em **Remover**.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover um ícone de aplicativo em um grupo de aplicativos

Execute as seguintes etapas para adicionar, alterar ou remover um ícone de aplicativo.

1. Selecione **Aplicativos** no painel esquerdo.
2. Na guia **Aplicativos**, selecione um aplicativo e, em seguida, selecione **Propriedades**.

   Para fazer alterações no nível do grupo de aplicativos, navegar até a guia **Grupos de Aplicativos**, selecione um aplicativo em um grupo e, em seguida, selecione **Propriedades**.
3. Selecione a página **Entrega** e, em seguida, selecione **Alterar**. A janela **Selecionar Ícone** é exibida.
4. Na janela **Selecionar Ícone**, faça o seguinte:

   - Para adicionar um ícone, selecione **Adicionar** e, em seguida, navegue até o ícone.
   - Para remover um ícone, selecione-o e, em seguida, selecione **Remover**.
   - Para alterar um ícone, selecione-o para o aplicativo.

> **Importante:**
>
> - Você não pode adicionar um ícone cujo tamanho seja maior que 200 KB.
> - Você pode adicionar apenas arquivos .icon.
> - Você não pode remover ícones incorporados.
> - Você não pode remover um ícone de um aplicativo que está em uso.

5. Selecione **Salvar** 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 (você não pode editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Escopos**. Marque ou desmarque a caixa de seleção ao lado de um escopo.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (você não pode editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Escopos**. Marque ou desmarque a caixa de seleção ao lado dos escopos que você deseja alterar.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **Salvar** para aplicar as alterações e fechar a janela.

Excluir um grupo de aplicativos

Um aplicativo deve estar associado a pelo menos um grupo de entrega ou grupo de aplicativos. Se a exclusão de um grupo de aplicativos resultar em um ou mais aplicativos que não pertencem mais a um grupo, você será avisado de que a exclusão desse grupo também removerá esses aplicativos. Você pode então confirmar ou cancelar a exclusão.

A exclusão de um aplicativo não o exclui de sua fonte original. No entanto, se você quiser torná-lo disponível novamente, deverá adicioná-lo novamente.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Excluir Grupo** na barra de ações.
3. Confirme a exclusão quando solicitado.

Organizar grupos de aplicativos usando pastas

Você pode criar pastas para organizar grupos de aplicativos para facilitar o acesso.

Funções necessárias

Por padrão, você pode criar e gerenciar pastas para grupos de aplicativos se tiver uma das seguintes funções internas:

- Administrador de Nuvem
- Administrador Completo
- Administrador de Grupo de Aplicativos

Você pode delegar ações de gerenciamento a outros usuários criando funções personalizadas. A tabela a seguir lista as permissões necessárias para cada ação.

AÇÃO	PERMISSÕES NECESSÁRIAS
Criar pastas de grupo de aplicativos	Criar Pasta de Grupo de Aplicativos
Excluir pastas de grupo de aplicativos	Remover Pasta de Grupo de Aplicativos
Mover pastas de grupos de aplicativos	Mover Pasta de Grupo de Aplicativos
Renomear pastas de grupos de aplicativos	Editar Pasta de Grupo de Aplicativos
Mover grupos de aplicativos para pastas	Editar Pasta de Grupo de Aplicativos, Editar Propriedades do Grupo de Aplicativos

Para obter mais informações, consulte Criar e gerenciar funções.

Criar e gerenciar pastas

Você pode usar a barra de Ações ou o menu de clique com o botão direito para criar e gerenciar pastas de grupos de aplicativos. Além disso, você pode arrastar um grupo de aplicativos ou uma pasta para um local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas em até cinco níveis (excluindo a pasta 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 nós (como catálogos de máquinas, grupos de entrega, aplicativos e grupos de aplicativos) compartilham uma árvore de pastas no back-end. Para evitar conflitos de nomes com outras pastas de recursos ao renomear ou mover pastas, recomendamos que você dê nomes diferentes às pastas de primeiro nível em diferentes árvores de pastas.

Acesso Remoto a PC

Nota:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O Acesso Remoto a PC é um recurso do Citrix Virtual Apps and Desktops que permite às organizações permitir facilmente que seus funcionários acessem recursos corporativos remotamente de forma segura. A plataforma Citrix torna esse acesso seguro possível, dando aos usuários acesso aos seus PCs físicos do escritório. Se os usuários puderem acessar seus PCs do escritório, eles poderão acessar todos os aplicativos, dados e recursos de que precisam para realizar seu trabalho. O Acesso Remoto a PC elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, desktops ou aplicativos virtuais e sua infraestrutura associada.

O Acesso Remoto a PC usa os mesmos componentes do Citrix Virtual Apps and Desktops que fornecem desktops e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Acesso Remoto a PC são os mesmos exigidos para a implantação do Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários recebem a melhor experiência de usuário usando o Citrix HDX™ para entregar sua sessão de PC do escritório.

O recurso consiste em um catálogo de máquinas do tipo **Acesso Remoto a PC** que fornece esta funcionalidade:

- Capacidade de adicionar máquinas especificando UOs. Essa capacidade facilita a adição de PCs em massa.
- Atribuição automática de usuário com base no usuário que faz login no PC Windows do escritório. Suportamos atribuições de usuário único e de múltiplos usuários. Por padrão, atribuímos automaticamente múltiplos usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, faça login no Web Studio, vá para **Configurações** e desative a configuração **Habilitar atribuição automática de múltiplos usuários para Acesso Remoto a PC**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs Linux Físicos
- PCs físicos agrupados (ou seja, atribuídos aleatoriamente, não dedicados)

> **Notas:**

> Para obter detalhes sobre as versões de SO suportadas, consulte os requisitos de sistema para o VDA para SO de sessão única e VDA Linux.

> Para implantações locais, o Acesso Remoto a PC é válido apenas para licenças Citrix Virtual Apps and Desktops Advanced ou Premium. As sessões consomem licenças da mesma forma que outras sessões do Citrix Virtual Desktops™. Para o Citrix Cloud, o Acesso Remoto a PC é válido para o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) e Workspace Premium Plus.

Considerações

Embora todos os requisitos técnicos e considerações que se aplicam ao Citrix Virtual Apps and Desktops em geral também se apliquem ao Acesso Remoto a PC, alguns podem ser mais relevantes ou exclusivos para o caso de uso de PC físico.

> **Importante:**

Sistemas físicos com Windows 11 (e alguns com Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:

- Use a opção "/physicalmachine" juntamente com a opção "/remotepc" como parte da instalação do VDA por linha de comando
- Adicione o seguinte valor de registro após a instalação do VDA se a opção mencionada anteriormente não foi usada `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - Nome: ForceEnableRemotePC
  - Tipo: DWORD
  - Dados: 1

Considerações de implantação

Ao planejar a implantação do Acesso Remoto a PC, tome algumas decisões gerais.

- Você pode adicionar o Acesso Remoto a PC a uma implantação existente do Citrix Virtual Apps and Desktops. Antes de escolher esta opção, considere o seguinte:
  - Os Delivery Controllers ou Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os bancos de dados do site on-premises e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os VDAs existentes e os novos VDAs de Acesso Remoto a PC excederão o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs de escritório por meio de um processo automatizado. As seguintes são as opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instalar VDAs usando SCCM.
  - Scripts de implantação: Instalar VDAs usando scripts.
- Revise as considerações de segurança do Acesso Remoto a PC.

Observação:

Ao projetar o Acesso Remoto a PC, você deve considerar o número de monitores físicos conectados à GPU no PC remoto e atualmente configurados/operando. Mesmo que o monitor não seja usado na sessão Citrix, mas seja detectado pela GPU, a presença do monitor é contabilizada para o limite máximo de monitores suportados pela GPU.

Considerações sobre o catálogo de máquinas

O tipo de catálogo de máquinas necessário depende do caso de uso:

- Catálogo de máquinas de Acesso Remoto a PC
  - PCs Windows dedicados
  - PCs Windows dedicados multiusuário. Este caso de uso se aplica a PCs físicos de escritório que múltiplos usuários podem acessar remotamente em diferentes turnos.
  - PCs Windows em pool. Este caso de uso se aplica a PCs físicos que múltiplos usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas de SO de sessão única
  - Estático - PCs Linux Dedicados
  - Aleatório - PCs Linux Agrupados

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.
- Ao escolher as UOs nas quais as contas de máquina residem, selecione UOs de nível inferior para maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de Banco/Oficiais/Caixas, selecione **Caixas** para maior granularidade. Caso contrário, você pode selecionar **Oficiais** ou **Banco** com base no requisito.
- Mover ou excluir UOs depois de serem atribuídas a um catálogo de máquinas de Acesso Remoto a PC afeta as associações de VDA e causa problemas com atribuições futuras. Portanto, certifique-se de planejar adequadamente para que as atualizações de atribuição de

UO para catálogos de máquinas sejam consideradas no plano de alteração do Active Directory.

- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas devido à estrutura da UO, você não precisa selecionar nenhuma UO. Você pode usar o PowerShell para adicionar máquinas ao catálogo posteriormente. As atribuições automáticas de usuário continuam funcionando se a atribuição de desktop estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo de máquinas juntamente com as atribuições de usuário está disponível no GitHub.
- O Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Acesso Remoto a PC**.

Considerações sobre o VDA Linux

Estas considerações são específicas para o VDA Linux:

- Use o VDA Linux em máquinas físicas apenas no modo não 3D. Devido a limitações no driver da NVIDIA, a tela local do PC não pode ser desativada e exibe as atividades da sessão quando o modo HDX 3D está ativado. Exibir esta tela é um risco de segurança.
- Use catálogos de máquinas do tipo SO de sessão única para máquinas Linux físicas.
- A atribuição automática de usuário não está disponível para máquinas Linux.
- Se os usuários já estiverem logados em seus PCs localmente, as tentativas de iniciar os PCs do StoreFront™ falham.
- As opções de economia de energia não estão disponíveis para máquinas Linux.

Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e considerações para PCs físicos.

- O seguinte não é suportado:
  - Comutadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo laptops e PCs All-in-One e NVIDIA Optimus.
  - Máquinas com dual boot.
- Conecte o teclado e o mouse diretamente ao PC. A conexão a um monitor ou outros componentes que podem ser desligados ou desconectados pode tornar esses periféricos indisponíveis. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desligue esses componentes.

- Os PCs devem estar ingressados em um domínio do Active Directory Domain Services.
- O Secure Boot é compatível apenas com Windows 10 e Windows 11.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é preferível para maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:

  a. Defina as configurações de energia para manter o adaptador sem fio ligado.

  b. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registrará até que o usuário faça logon. O PC não estará disponível para acesso remoto até que um usuário tenha feito logon.

  c. Certifique-se de que os Delivery Controllers ou Cloud Connectors possam ser alcançados a partir da rede Wi-Fi.

- Você pode usar o Acesso Remoto ao PC em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionar com a bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:

  a. Desative o recurso de hibernação.

  b. Desative o recurso de suspensão.

  c. Defina a ação de fechar a tampa como **Não fazer nada**.

  d. Defina a ação de "pressionar o botão liga/desliga" como **Desligar**.

  e. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Acesso Remoto ao PC é compatível com dispositivos Surface Pro com Windows 10. Siga as mesmas diretrizes para laptops mencionadas anteriormente.
- Se estiver usando uma estação de acoplamento, você pode desacoplar e reacoplar laptops. Ao desacoplar o laptop, o VDA se registra novamente com os Delivery Controllers ou Cloud Connectors via Wi-Fi. No entanto, ao reacoplar o laptop, o VDA não muda para usar a conexão com fio, a menos que você desconecte o adaptador sem fio. Alguns dispositivos fornecem funcionalidade integrada para desconectar o adaptador sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador sem fio. Revise as considerações sobre Wi-Fi mencionadas anteriormente.

  Faça o seguinte para habilitar o acoplamento e desacoplamento para dispositivos de Acesso Remoto ao PC:

a. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão** e defina **Suspender** como **Nunca**.

b. Em **Gerenciador de Dispositivos > Adaptadores de rede > Adaptador Ethernet**, vá para **Gerenciamento de Energia** e desmarque **Permitir que o computador desligue este dispositivo para economizar energia**. Certifique-se de que **Permitir que este dispositivo reative o computador** esteja marcado.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, esse recurso aparece como indisponível se já estiver em uso por outro usuário.
- Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

Sequência de configuração

Esta seção contém uma visão geral de como configurar o Acesso Remoto ao PC ao usar o catálogo de máquinas do tipo **Acesso Remoto ao PC**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquinas.

1. Somente site local - Para usar o recurso integrado Wake on LAN, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para Acesso Remoto ao PC:

   a. Selecione o tipo de Site **Acesso Remoto a PC**.

   b. Na página **Gerenciamento de Energia**, escolha habilitar ou desabilitar o gerenciamento de energia para o catálogo de máquinas padrão de Acesso Remoto ao PC. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.

   c. Preencha as informações nas páginas **Usuários** e **Contas de Máquina**.

   A conclusão dessas etapas cria um catálogo de máquinas chamado **Máquinas de Acesso Remoto a PC** e um Grupo de Entrega chamado **Desktops de Acesso Remoto a PC**.
3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a. Crie um catálogo de máquinas do tipo **Acesso Remoto ao PC** (página Sistema Operacional do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Certifique-se de atribuir a OU correta para que os PCs de destino fiquem disponíveis para uso com o Acesso Remoto ao PC.

b. Crie um Grupo de Entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um Grupo de Entrega, consulte Criar Grupos de Entrega. Certifique-se de atribuir o Grupo de Entrega a um grupo do Active Directory que contenha os usuários que precisam de acesso aos seus PCs.

4. Implante o VDA nos PCs do escritório.

   - Recomendamos usar o instalador VDA principal do SO de sessão única (VDAWorkstationCoreSetup.exe).
   - Você também pode usar o instalador VDA completo de sessão única (VDAWorkstationSetup.exe) com a opção `/remotepc/physicalmachine`, o que alcança o mesmo resultado que usar o instalador VDA principal.

     > **Observação:**
     >
     > Para a instalação do RemotePC, use o argumento `/physicalmachine` com `/remotepc` para que o VDA se comporte conforme o esperado em determinados cenários de usuário.

   - Considere habilitar a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto através do Citrix Director. Para fazer isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para poder ver as informações de duração de logon no Director, você deve usar o instalador VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Inclua este componente usando a opção `/includeadditional`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para obter informações sobre como implantar o VDA usando o SCCM, consulte Instalar VDAs usando o SCCM.
   - Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

   Depois de concluir com sucesso as etapas 2 a 4, os usuários são automaticamente atribuídos às suas próprias máquinas quando fazem login localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente que eles usam para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace

está disponível em `https://www.citrix.com/downloads/` ou nas lojas de aplicativos para dispositivos móveis compatíveis.

Recursos gerenciados através do registro

> **Cuidado:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Desabilitar atribuições automáticas de múltiplos usuários

Em cada Delivery Controller™, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dados: 0

Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina de Acesso Remoto a PC entre em estado de suspensão, adicione esta configuração de registro no VDA e, em seguida, reinicie a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra em modo de suspensão após o tempo limite de inatividade pré-configurado. Depois que a máquina acorda, ela se registra novamente com o Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Valor: 1

Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é automaticamente desconectada quando um usuário local inicia uma sessão nessa máquina (pressionando CTRL+ALT+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e, em seguida, reinicie a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Valor: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é reconhecida dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Valor:
  - 1 - O usuário remoto sempre tem preferência se ele ou ela não responder à interface de mensagens no período de tempo limite especificado. Este comportamento é o padrão se esta configuração não for definida.
  - 2 - O usuário local tem preferência.

O tempo limite para aplicar o modo Acesso Remoto ao PC é de 30 segundos por padrão. Você pode configurar esse tempo limite, mas não o defina para menos de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dados: número de segundos para o tempo limite em valores decimais

Quando um usuário deseja obter acesso forçado ao console: O usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local sobre uma sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon nesse PC enquanto ele estiver em uso por um usuário remoto, o usuário remoto receberá um prompt. O prompt pergunta se deve permitir ou negar a conexão do usuário local. Permitir a conexão desconecta a sessão do usuário remoto.

Registro de gerenciamento de sessão

O Acesso Remoto ao PC agora possui recursos de registro que registram quando alguém tenta acessar um PC com uma sessão ICA® ativa. Isso permite que você monitore seu ambiente em busca de atividades indesejadas ou inesperadas e seja capaz de auditar tais eventos, caso precise investigar quaisquer incidentes.

Os eventos são registrados usando o Visualizador de Eventos do Windows e estão em **Aplicativos e Serviços > Citrix > HostCore > Serviço ICA > Admin**.

Existem três eventos distintos que são registrados ao usar o Acesso Remoto ao PC.

Evento Ctrl+Alt+Del

Este evento aparece quando o usuário local pressiona Ctrl+Alt+Del no teclado do console com uma sessão remota ativa.

Detalhes do evento

- Nome do log: Aplicativo e Serviços
- ID do Evento: 43, 44, 45
- Fonte: ICA Service

ID do Evento 43

Este ID de evento aparece quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

ID do Evento 44

Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The user preference is set to remote user.
```

ID do Evento 45

Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

Evento de desconexão de sessão remota

Este evento aparece quando a sessão remota foi desconectada por vários motivos.

Detalhes do evento

- Nome do log: Aplicativos e Serviços
- ID do Evento: 46, 47, 48
- Fonte: Serviço ICA

ID do Evento 46

Este ID de evento aparece quando a sessão remota foi desconectada e quando o valor do registro SasNotification não existe ou o valor do registro SasNotification é 0.

- Mensagem:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

ID do Evento 47

Este ID de evento aparece quando o usuário remoto concorda em desconectar a sessão e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode é 2 ou o valor do registro RpcaMode não existe.

- Mensagem:

> The remote session for <remoteUserName> has been disconnected because the user accepted the request to disconnect the session.

ID do Evento 48

Este ID de evento aparece quando o usuário remoto não recusa a solicitação de desconexão dentro do período de tempo limite específico e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

> The remote session for <remoteUserName> has been disconnected because the user did not decline the disconnection request within the configured timeout period (<timeout period>).

Evento Ctrl+Alt+Del pressionado duas vezes

Este evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

Detalhes do evento

- Nome do log: Aplicativo e Serviços
- ID do Evento: 49
- Origem: Serviço ICA

ID do Evento 49

Este ID de evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

- Mensagem:

> The remote session for <remoteUserName> has been forcibly disconnected.

Wake on LAN

O Acesso Remoto ao PC suporta Wake on LAN, o que oferece aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs de escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina foi desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede na qual o PC reside quando instruído pelo delivery controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura extras ou soluções de terceiros para a entrega de pacotes mágicos.

O recurso Wake on LAN difere do recurso legado Wake on LAN baseado em SCCM. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN – integrado ao SCCM.

Limitação

O Acesso Remoto ao PC com o recurso Wake on LAN não suporta o ligamento automático durante os horários de pico.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes de compatibilidade, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows

Configurar Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops local, a configuração do Wake on LAN integrado é suportada apenas usando o PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas do Acesso Remoto ao PC se você ainda não tiver um.
2. Crie a conexão de host do Wake on LAN se você ainda não tiver uma.

> **Observação:**
>
> Para usar o recurso Wake on LAN, se você tiver uma conexão de host do tipo "Microsoft Configuration Manager Wake on LAN", crie uma nova conexão de host.

3. Recupere o identificador exclusivo da conexão de host do Wake on LAN.
4. Associe a conexão de host do Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host do Wake on LAN:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `
```

```
                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

Quando a conexão de host estiver pronta, execute os seguintes comandos para recuperar o identificador exclusivo da conexão de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Depois de recuperar o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo de máquinas do Acesso Remoto ao PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

Considerações de design

Ao planejar usar o Wake on LAN com o Acesso Remoto ao PC, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host do Wake on LAN.
- Para que um PC ative outro PC, ambos os PCs devem estar na mesma sub-rede e usar a mesma conexão de host do Wake on LAN. Não importa se os PCs estão no mesmo catálogo de máquinas ou em catálogos diferentes.
- As conexões de host são atribuídas a zonas específicas. Se sua implantação contiver mais de uma zona, você precisará de uma conexão de host do Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Pacotes mágicos são transmitidos usando o endereço de broadcast global 255.255.255.255. Certifique-se de que o endereço não esteja bloqueado.
- Deve haver pelo menos um PC ligado na sub-rede — para cada conexão Wake on LAN — para poder ativar máquinas nessa sub-rede.

Considerações operacionais

A seguir estão as considerações para usar o recurso Wake on LAN:

- O VDA deve se registrar pelo menos uma vez antes que o PC possa ser ativado usando o recurso integrado Wake on LAN.
- O Wake on LAN só pode ser usado para ativar PCs. Ele não oferece suporte a outras ações de energia, como reiniciar ou desligar.
- Depois que a conexão Wake on LAN é criada, ela fica visível no Web Studio. No entanto, a edição de suas propriedades no Web Studio não é suportada se estiver usando o Citrix Virtual Apps and Desktops local.
- Pacotes mágicos são enviados de uma das duas maneiras:

  a. Quando um usuário tenta iniciar uma sessão em seu PC e o VDA está não registrado

  b. Quando um administrador envia manualmente um comando de ligar do Web Studio ou PowerShell

- Como o delivery controller não tem conhecimento do estado de energia de um PC, o Web Studio exibe **Não Suportado** sob o estado de energia. O delivery controller usa o estado de registro do VDA para determinar se um PC está ligado ou desligado.

Wake on LAN – integrado ao SCCM

O Wake on LAN integrado ao SCCM é uma opção alternativa de Wake on LAN para Acesso Remoto a PC que está disponível apenas com o Citrix Virtual Apps and Desktops local.

Requisitos do sistema

A seguir estão os requisitos de sistema para usar o recurso Wake on LAN integrado ao SCCM:

- Citrix Virtual Apps and Desktops 1912 ou posterior
- PCs físicos:
  - VDA versão 1912 ou posterior
  - Windows 10. Para obter detalhes de suporte, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou posterior

Configurar o Wake on LAN integrado ao SCCM

Conclua os seguintes pré-requisitos:

1. Configure o SCCM 2012 R2, 2016 ou 2019 na organização. Em seguida, implante o cliente SCCM em todas as máquinas de Acesso Remoto a PCs, dando tempo para que o ciclo de inventário agendado do SCCM seja executado, ou force um manualmente, se necessário.
2. Para suporte a Wake Proxy, habilite a opção no SCCM. Para cada sub-rede na organização que contém PCs que usam o recurso Wake on LAN do Acesso Remoto a PCs, certifique-se de que três ou mais máquinas possam servir como máquinas sentinela.
3. Para suporte a pacotes mágicos, configure roteadores de rede e firewalls para permitir que pacotes mágicos sejam enviados, usando uma transmissão direcionada à sub-rede ou unicast.
4. Configure o Wake on LAN nas configurações de BIOS/UEFI de cada PC.
5. Implante o VDA nos PCs físicos, se ainda não o fez.

Depois de atender aos pré-requisitos, conclua as seguintes etapas para permitir que o Delivery Controller se comunique com o SCCM:

1. Crie uma conexão de host para o SCCM. Para obter mais informações, consulte Conexões e recursos.

- Selecione **Microsoft Configuration Manager Wake on LAN** como o tipo de conexão.
- As credenciais inseridas devem ter acesso às coleções no escopo e devem ter a função de **Operador de Ferramentas Remotas**.

2. Selecione a conexão no Web Studio, depois selecione **Editar Conexão** e clique em **Avançado**.
3. Selecione a opção apropriada para lidar com o Wake on LAN:

   - Se você estiver usando o proxy de ativação, selecione a primeira opção: **Proxy de ativação do Microsoft System Center Configuration Manager**.
   - Se você estiver usando pacotes mágicos, selecione a segunda opção: **Pacotes Wake on LAN transmitidos pelo Delivery Controller**.
     - Selecione o método de transmissão apropriado: **transmissões direcionadas por sub-rede** ou **unicast**.

Depois de criar a conexão do host, associe a conexão a um catálogo do Remote PC Access:

- Se você estiver criando um novo catálogo do Remote PC Access, na página **Sistema Operacional** do assistente de criação de catálogo, selecione **Remote PC Access** como o tipo de catálogo e escolha a conexão apropriada na lista suspensa.
- Para adicionar o Wake on LAN a um catálogo existente do Remote PC Access:

  a. Vá para o nó **Catálogos de Máquinas** no Web Studio, selecione o catálogo de máquinas e, em seguida, selecione **Editar Catálogo de Máquinas**.
  b. Selecione a guia **Gerenciamento de Energia** e escolha **Sim** para habilitar o gerenciamento de energia para o catálogo de máquinas.
  c. Selecione a conexão apropriada na lista suspensa e clique em **OK**.

Solução de problemas

Escurecimento do monitor não funciona

Se o monitor local do PC Windows não estiver em branco enquanto houver uma sessão HDX ativa (o monitor local exibe o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê ao driver de exibição indireta (IDD) da Citrix uma prioridade maior do que o driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para mais detalhes sobre as prioridades do adaptador de vídeo e a criação de monitores, consulte o artigo do Knowledge Center CTX237608.

A sessão se desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão habilitada

A notificação de gerenciamento de sessão controlada pelo valor de registro **SasNotification** só funciona quando o modo Acesso Remoto para PC está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização habilitados, o PC será relatado como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desabilitará automaticamente o modo Acesso Remoto para PC. Para habilitar o modo Acesso Remoto para PC, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Informações de diagnóstico

As informações de diagnóstico sobre o Acesso Remoto para PC são gravadas no log de Eventos de Aplicativo do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas descartando mensagens duplicadas.

- 3300 (informativo): Máquina adicionada ao catálogo
- 3301 (informativo): Máquina adicionada ao grupo de entrega
- 3302 (informativo): Máquina atribuída ao usuário
- 3303 (erro): Exceção

Gerenciamento de energia

Se o gerenciamento de energia para o Remote PC Access estiver habilitado, as transmissões direcionadas por sub-rede podem falhar ao iniciar máquinas que estão em uma sub-rede diferente do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando

transmissões direcionadas por sub-rede, e o suporte AMT não estiver disponível, tente o proxy de ativação ou o método Unicast. Certifique-se de que essas configurações estejam habilitadas nas propriedades avançadas para a conexão de gerenciamento de energia.

A sessão remota ativa registra a entrada local da tela de toque

Quando o VDA ativa o modo de Acesso Remoto ao PC, a máquina ignora a entrada local da tela de toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização ativados, o PC se reporta como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo de Acesso Remoto ao PC. Para ativar o modo de Acesso Remoto ao PC, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Mais recursos

A seguir estão outros recursos para Acesso Remoto ao PC:

- Orientação de design da solução: Remote PC Access Design Decisions.
- Exemplos de arquiteturas de Acesso Remoto ao PC: Reference Architecture for Citrix Remote PC Access Solution.

Publicar conteúdo

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> Você pode publicar um aplicativo que é simplesmente um URL ou caminho UNC para um recurso, como um documento do Microsoft Word ou um link da web. Esse recurso é conhecido como conteúdo publicado. A capacidade de publicar conteúdo adiciona flexibilidade à forma como você entrega conteúdo aos usuários. Você se beneficia do controle de acesso e gerenciamento de aplicativos existentes. Você também pode especificar se deseja usar aplicativos locais ou publicados para abrir o conteúdo.

O conteúdo publicado aparece como outros aplicativos no StoreFront™ e no aplicativo Citrix Workspace™. Os usuários o acessam da mesma forma que acessam os aplicativos. No cliente, o recurso é aberto normalmente.

- Se um aplicativo instalado localmente for apropriado, ele será iniciado para abrir o recurso.
- Se uma Associação de Tipo de Arquivo tiver sido definida, um aplicativo publicado será iniciado para abrir o recurso.

Você publica conteúdo usando o PowerShell SDK. Você não pode usar o Web Studio para publicar conteúdo. No entanto, você pode usar o Web Studio para editar as propriedades do aplicativo posteriormente, depois que forem publicados.

Visão geral da configuração e preparação

A publicação de conteúdo usa o cmdlet `New-BrokerApplication` com as seguintes propriedades principais. (Consulte a ajuda do cmdlet para descrições de todas as propriedades do cmdlet.)

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

A propriedade `ApplicationType` deve ser `PublishedContent`.

A propriedade `CommandLineExecutable` especifica o local do conteúdo publicado. Os seguintes formatos são suportados, com um limite de 255 caracteres.

- Endereço de site HTML (por exemplo, `<http://www.citrix.com>`)
- Arquivo de documento em um servidor web (por exemplo, `https://www.citrix.com/press/pressrelease.doc`)
- Diretório em um servidor FTP (por exemplo, `ftp://ftp.citrix.com/code`)

- Arquivo de documento em um servidor FTP (por exemplo, `ftp://ftp.citrix.com/code/Readme.txt`>)
- Caminho de diretório UNC (por exemplo, `file://myServer/myShare or \\\\myServer\\myShare`)
- Caminho de arquivo UNC (por exemplo, `file://myServer/myShare/myFile.asf` ou `\\myServer\myShare\myFile.asf`)

Certifique-se de que você tenha o SDK correto.

- Para implantações do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), baixe e instale o SDK remoto do PowerShell do Citrix Virtual Apps and Desktops.
- Para implantações locais do Citrix Virtual Apps and Desktops, use o SDK do PowerShell que é instalado com o Delivery Controller. Adicionar um aplicativo de conteúdo publicado requer um Delivery Controller de versão mínima 7.11.

Os procedimentos a seguir usam exemplos. Nos exemplos:

- Um catálogo de máquinas foi criado.
- Um grupo de entrega chamado `PublishedContentApps` foi criado. O grupo usa uma máquina de SO multi-sessão do catálogo. O aplicativo WordPad foi adicionado ao grupo.
- As atribuições são feitas para o nome do grupo de entrega, o local `CommandLineExecutable` e o nome do aplicativo.

Começar

Na máquina que contém o SDK do PowerShell, abra o PowerShell.

O cmdlet a seguir adiciona o snap-in apropriado do SDK do PowerShell e atribui o registro do grupo de entrega retornado.

```
Add-PsSnapin Citrix&ast; $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Se você estiver usando o Citrix DaaS, autenticar inserindo suas credenciais do Citrix Cloud™. Se houver mais de um cliente, escolha um.

Publicar uma URL

Após atribuir o local e o nome do aplicativo, o cmdlet a seguir publica a página inicial da Citrix como um aplicativo.

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

Verificar sucesso:

- Abra o StoreFront e faça logon como um usuário que pode acessar aplicativos no grupo de entrega PublishedContentApps. A exibição inclui o aplicativo recém-criado com o ícone padrão. Para saber mais sobre como personalizar o ícone, consulte `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`.
- Clique no aplicativo **Citrix Home Page**. A URL é iniciada em uma nova guia em uma instância local do seu navegador padrão.

Publicar recursos localizados em caminhos UNC

Neste exemplo, o administrador já criou um compartilhamento chamado `PublishedResources`. Após atribuir os locais e nomes de aplicativos, os seguintes cmdlets publicam um arquivo RTF e um DOCX nesse compartilhamento como um recurso.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
```

```
$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

Verificar o sucesso:

- Atualize sua janela do StoreFront para ver os documentos recém-publicados.
- Clique nos aplicativos **PublishedRTF** e **PublishedDOCX**. Cada documento é aberto em um WordPad em execução localmente.

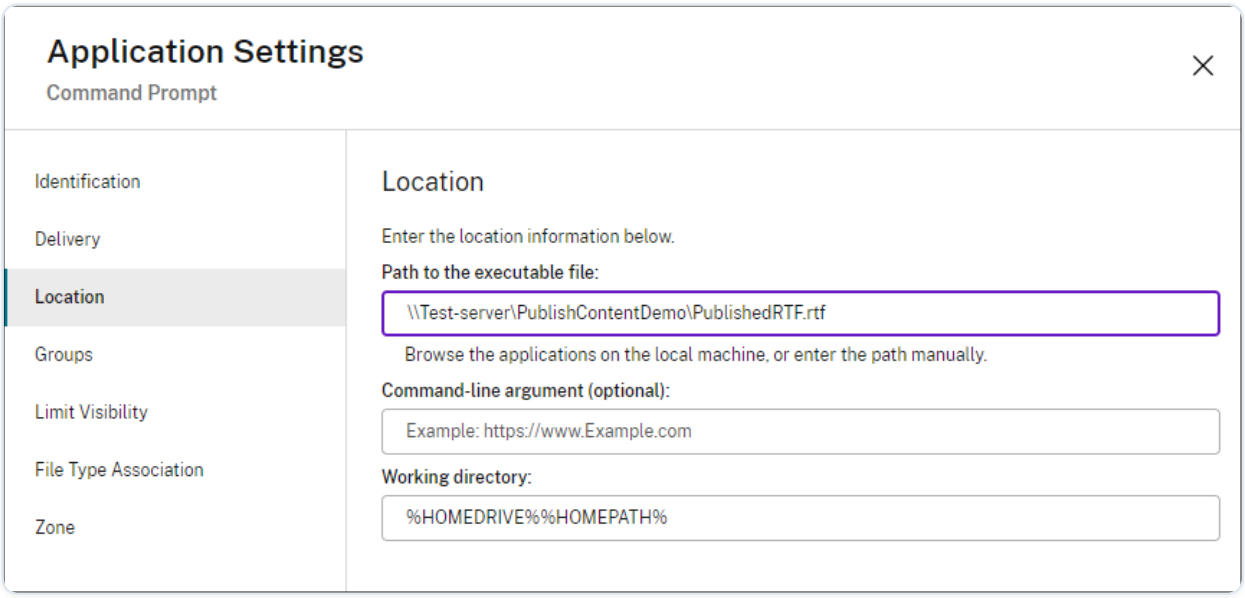
Visualizar e editar aplicativos PublishedContent

Você gerencia o conteúdo publicado usando os mesmos métodos que usa para outros tipos de aplicativos.

Para visualizar e editar aplicativos `PublishedContent`, siga estas etapas:

1. Faça login no Web Studio e selecione **Aplicativos** no painel esquerdo.
2. Na guia **Aplicativos**, selecione um aplicativo PublishedContent e, em seguida, selecione **Propriedades**.

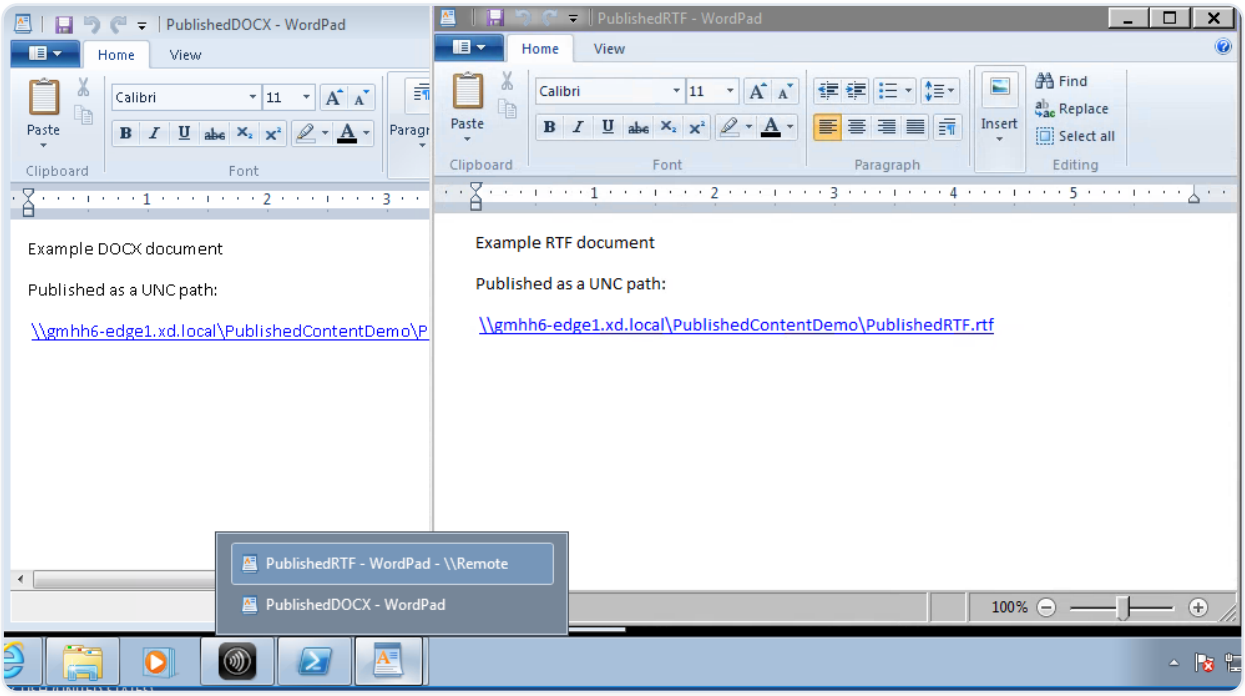
   As propriedades do aplicativo (como visibilidade do usuário, associação de grupo e atalho) se aplicam ao conteúdo publicado. No entanto, você não pode alterar o argumento da linha de comando ou as propriedades do diretório de trabalho na página **Local**.
3. Para alterar o recurso, modifique o campo **Caminho para o arquivo executável** nessa página.



4. Para usar um aplicativo publicado para abrir um aplicativo `PublishedContent` (em vez de um aplicativo local), siga estas etapas:

   Neste exemplo, o aplicativo WordPad publicado é editado para criar uma Associação de Tipo de Arquivo para arquivos .rtf.

   a. Ative o modo de manutenção para o grupo de entrega.
   b. Edite a propriedade **Associação de Tipo de Arquivo**.
   c. Desative o modo de manutenção quando terminar.
   d. Atualize o StoreFront para carregar as alterações da Associação de Tipo de Arquivo e, em seguida, clique nos aplicativos **PublishedRTF** e **PublishedDOCX**. Observe a diferença. **PublishedDOCX** ainda abre no WordPad local. No entanto, **PublishedRTF** agora abre no WordPad publicado devido à associação de tipo de arquivo.



Para obter mais informações

- Criar catálogos de máquinas
- Criar grupos de entrega
- Alterar propriedades do aplicativo

Server VDI

Use o recurso Server VDI (Virtual Desktop Infrastructure) para entregar um desktop de um sistema operacional de servidor para um único usuário.

- Administradores corporativos podem entregar sistemas operacionais de servidor como desktops VDI, o que pode ser valioso para usuários como engenheiros e designers.
- Provedores de Serviços podem oferecer desktops da nuvem. Esses desktops estão em conformidade com o Contrato de Licença de Provedor de Serviços da Microsoft (SPLA).

Suporte:

- Em implantações de Citrix Virtual Apps and Desktops™ e Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), o Server VDI é suportado no Windows Server 2022 e Windows Server 2019.
- Todas as implantações de Server VDI suportam a tecnologia de camada de personalização do usuário.

- Para que o Server VDI funcione com dispositivos TWAIN, como scanners, o recurso Experiência de Área de Trabalho do Windows Server deve ser instalado.
- Os seguintes recursos não podem ser usados com o Server VDI:
  - Aplicativos hospedados
  - Acesso a aplicativos locais
  - Conexões de desktop diretas (não intermediadas)
  - Acesso Remoto ao PC

Instalar e configurar o Server VDI

1. Prepare o servidor Windows para a instalação.
   - Use o Gerenciador do Servidor Windows para garantir que os serviços de função dos Serviços de Área de Trabalho Remota não estejam instalados. Se eles foram instalados anteriormente, remova-os. A instalação do VDA falha se esses serviços de função estiverem instalados.
   - Certifique-se de que a propriedade **Restringir cada usuário a uma única sessão** esteja habilitada. No servidor Windows, edite o registro para a configuração do Terminal Server:

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Use a interface de linha de comando do instalador do Citrix Virtual Apps and Desktops para instalar um VDA em um servidor compatível ou imagem mestra de servidor, especificando as opções `/quiet` e `/servervdi`. (Por padrão, a interface gráfica do instalador bloqueia o VDA de SO de sessão única do Windows em um sistema operacional de servidor. O uso da linha de comando substitui esse comportamento.) Use um dos seguintes comandos:
   - Implantações do Citrix Virtual Apps and Desktops:
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Implantações do Citrix DaaS™:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   Outras opções:

- Use `/controllers` para especificar Delivery Controllers ou Cloud Connectors.
- Use `/enable_hdx_ports` para abrir portas no firewall, a menos que o firewall deva ser configurado manualmente.
- Use `/mastermcsimage` (ou `/masterimage`) se você estiver instalando o VDA em uma imagem e for usar o MCS para criar VMs de servidor a partir dessa imagem.
- Para todos os detalhes das opções, consulte Instalar usando a linha de comando.

3. Crie um catálogo de máquinas para Server VDI. No assistente de criação de catálogo:
   - Na página **Sistema operacional**, selecione **SO de sessão única**.
   - Na página **Resumo**, especifique um nome e uma descrição de catálogo de máquinas para administradores que o identifique claramente como Server VDI. Este é o único indicador no Studio de que o catálogo oferece suporte ao Server VDI.

   Ao usar a pesquisa no Studio, o catálogo Server VDI é exibido na guia **Máquinas de SO de sessão única**, mesmo que o VDA esteja instalado em uma máquina multi-sessão.
4. Crie um Grupo de Entrega e selecione o catálogo Server VDI que você criou.

Se você não especificou Delivery Controllers ou Cloud Connectors durante a instalação do VDA, lembre-se de especificá-los depois. Para obter detalhes, consulte Registro de VDA.

Camada de personalização do usuário

> **Observação:**

> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> O recurso de camada de personalização do usuário para Citrix Virtual Apps and Desktops estende os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e os aplicativos instalados localmente entre as sessões. Alimentado pela tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e ao Machine Creation Services™ (MCS) em um catálogo de máquinas não persistente.

Você instala os componentes da camada de personalização do usuário junto com o Virtual Delivery Agent na imagem mestre. Um arquivo VHD armazena aplicativos instalados localmente pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

> **Importante:**
>
> Você pode implantar camadas de personalização do usuário no Citrix Virtual Apps and Desktops, ou camadas de usuário do App Layering habilitadas em um modelo de imagem, mas não ambos. Não instale o recurso de camada de personalização do usuário em uma camada dentro do App Layering.
>
> Este recurso substitui o Personal vDisk (PvD), ao mesmo tempo em que oferece uma experiência de espaço de trabalho persistente para usuários em um ambiente de desktop não persistente (agrupado).

Para implantar o recurso de camada de personalização do usuário, instale e configure-o usando as etapas detalhadas no artigo.

Suporte a aplicativos

Com exceção das seguintes exceções, todos os aplicativos que um usuário instala localmente na área de trabalho são suportados na camada de personalização do usuário.

Exceções

Os seguintes aplicativos são a exceção e não são suportados na camada de personalização do usuário:

- Aplicativos corporativos, como MS Office e Visual Studio.
- Aplicativos que modificam a pilha de rede ou hardware. Exemplo: um cliente VPN.
- Aplicativos que possuem drivers de nível de inicialização. Exemplo: um scanner de vírus.
- Aplicativos com drivers que usam o armazenamento de drivers. Exemplo: um driver de impressora.

> **Observação:**

> Você pode disponibilizar impressoras usando Objetos de Política de Grupo (GPOs) do Windows.

Não *permita* que os usuários instalem aplicativos não suportados localmente. Em vez disso, instale esses aplicativos diretamente na imagem mestre.

Aplicativos que exigem uma conta de usuário 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 persistem além da sessão.

> **Importante:**
>
> Adicione qualquer usuário ou grupo local necessário na imagem mestre.

Requisitos

O recurso de camada de personalização do usuário requer os seguintes componentes:

- Citrix Virtual Apps and Desktops 7 1909 ou posterior
- Virtual Delivery Agent (VDA), versão 1912 ou posterior
- Citrix Provisioning™, versão 1909 ou posterior
- Compartilhamento de Arquivos do Windows (SMB), ou Azure Files com autenticação AD local habilitada

Você pode implantar o recurso de camada de personalização do usuário nas seguintes versões do Windows quando o SO é implantado como 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 Server 2019 (Azure Files suportado)
- Windows Server 2022 (Azure Files suportado)

Para Citrix Virtual Apps and Desktops 7, o uso de Azure Files com camadas de personalização do usuário é suportado em clientes Windows Server 2022, Windows Server 2019 e Windows 10.

Observação:

Se você estiver usando um SO de servidor, apenas o Server VDI é suportado. Para detalhes de implantação, consulte o artigo Server VDI.

A camada de personalização do usuário suporta apenas um usuário por vez por máquina, e então a máquina precisa ser reiniciada para redefinir os discos. Você não pode usar a camada de personalização do usuário com sistemas operacionais de servidor multi-sessão, apenas com sistemas de servidor de sessão única. A camada de personalização do usuário é suportada apenas para desktops não persistentes.

Desinstale o recurso de camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

Configurar seu compartilhamento de arquivos

O recurso de camada de personalização do usuário requer armazenamento Windows Server Message Block (SMB). Para criar um compartilhamento de arquivos do Windows, siga as etapas usuais para o sistema operacional Windows que você está usando.

Para saber mais sobre como usar o Azure Files com catálogos baseados no Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

Recomendações

Siga as recomendações nesta seção para uma implantação bem-sucedida da camada de personalização do usuário.

Microsoft System Center Configuration Manager (SCCM)

Se você estiver usando o SCCM com o recurso de camada de personalização do usuário, siga as diretrizes da Microsoft para preparar sua imagem em um ambiente VDI. Consulte este artigo do Microsoft TechNet para obter mais informações.

Tamanho da camada de usuário

Uma camada de usuário é um disco de provisionamento dinâmico que se expande à medida que o espaço no disco é usado. O tamanho padrão permitido para uma camada de usuário é de 10 GB, o mínimo que recomendamos.

> **Observação:**

> Durante a instalação, se o valor for definido como zero (0), o tamanho padrão da camada de usuário será definido como 10 GB.

> Se você quiser alterar o tamanho da camada de usuário, pode inserir um valor diferente para a política **Tamanho da Camada de Usuário**. Consulte **Etapa 5: Criar políticas personalizadas de grupo de entrega**, em **Opcional: Clique em Selecionar ao lado de Tamanho da Camada de Usuário em GB.**

Ferramentas para substituir o Tamanho da Camada de Usuário (Opcional)

Você pode substituir o Tamanho da Camada de Usuário usando uma ferramenta do Windows para definir uma cota no compartilhamento de arquivos da camada de usuário.

Use uma das seguintes ferramentas de cota da Microsoft para definir uma cota rígida no diretório da camada de usuário chamado **Users**:

- Gerenciador de Recursos do Servidor de Arquivos (FSRM)
- Gerenciador de Cotas

> **Observação:**

> Aumentar a cota afeta novas camadas de usuário e expande as existentes. Diminuir a cota afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

Implantar uma camada de personalização do usuário

Ao implantar o recurso de personalização do usuário, você define as políticas no Web Studio. Em seguida, você atribui as políticas ao grupo de entrega vinculado ao catálogo de máquinas, onde o recurso é implantado.

Se você deixar a imagem mestre sem configuração de camada de personalização do usuário, os serviços permanecerão ociosos e não interferirão nas atividades de autoria.

Se você definir as políticas na imagem mestre, os serviços tentarão executar e montar uma camada de usuário dentro da imagem mestre. A imagem mestre exibirá comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, conclua as seguintes etapas nesta ordem:

- Etapa 1: Verifique a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Etapa 2: Prepare sua imagem mestre.
- Etapa 3: Crie um catálogo de máquinas.
- Etapa 4: Crie um grupo de entrega.
- Etapa 5: Crie políticas personalizadas de grupo de entrega.

> **Observação:**
>
> Fazer login pela primeira vez após atualizar o Windows 10 na imagem leva mais tempo do que o normal. A camada do usuário precisa ser atualizada para a nova versão do Windows 10, o que aumenta o tempo de logon.

Passo 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops esteja disponível para uso com este novo recurso. Para detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

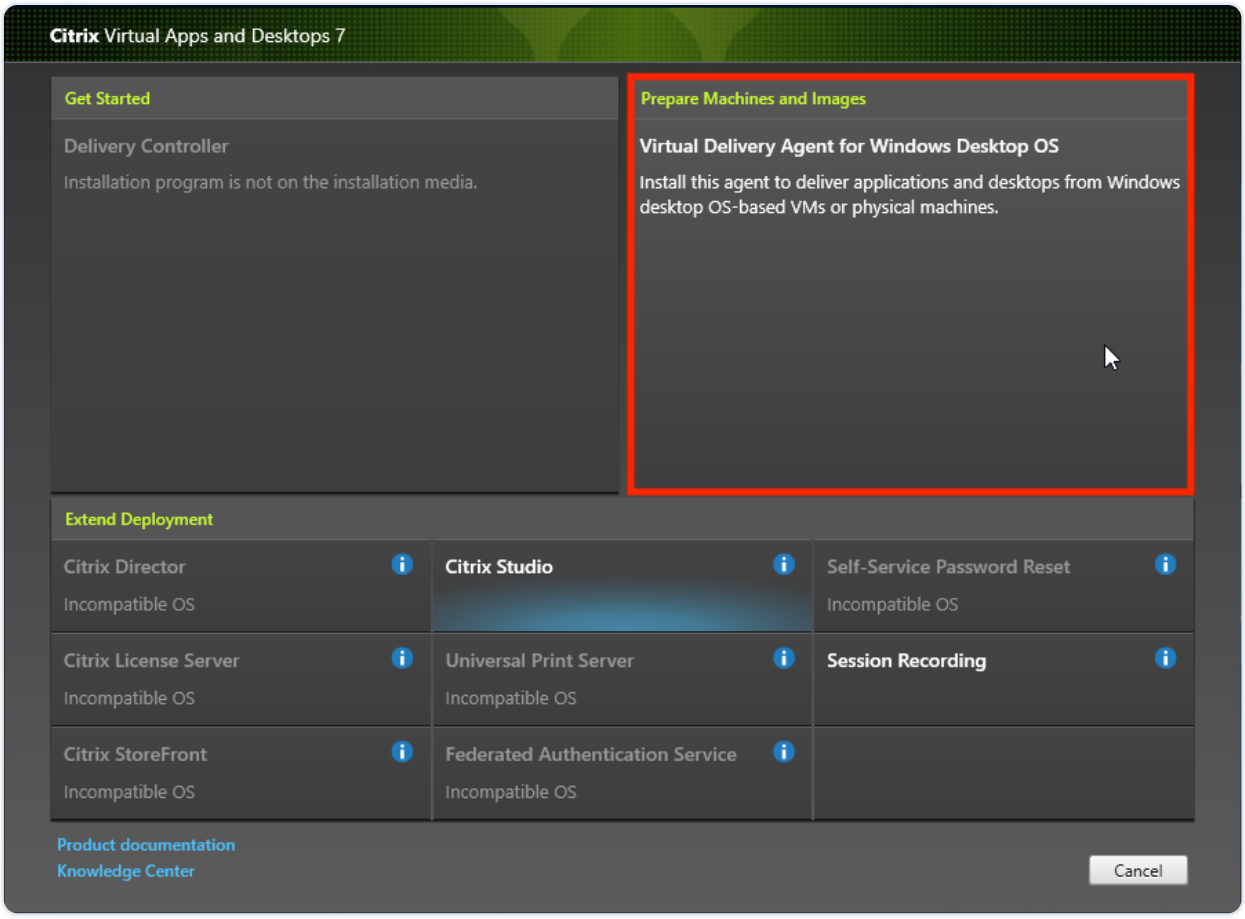
Passo 2: Prepare sua imagem mestre

Para preparar sua imagem mestre:

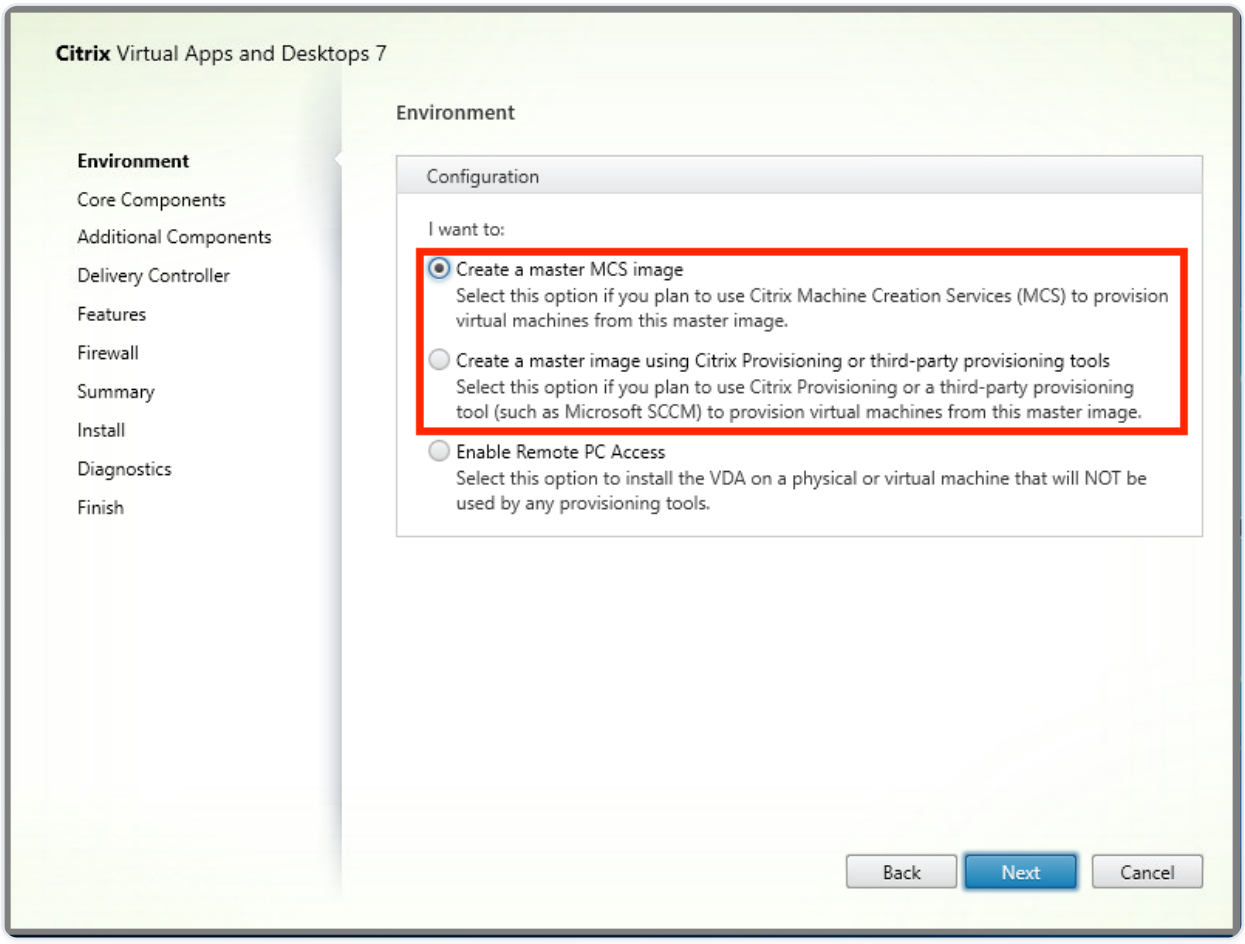
1. Localize a imagem mestre. Instale os aplicativos corporativos da sua organização e quaisquer outros aplicativos que seus usuários geralmente considerem úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Certifique-se de incluir o componente opcional, a **Camada de personalização do usuário**. Para obter detalhes, consulte as Opções de linha de comando para instalar um VDA.
3. Se você estiver usando o Windows 10, instale o Virtual Delivery Agent (VDA) 1912 ou posterior. Se uma versão mais antiga do VDA já estiver instalada, desinstale a versão antiga

primeiro. Ao instalar a nova versão, certifique-se de selecionar e instalar o componente opcional, a **Camada de Personalização do Usuário Citrix**, da seguinte forma:

a. Clique no bloco **Virtual Delivery Agent for Windows Desktop OS**:

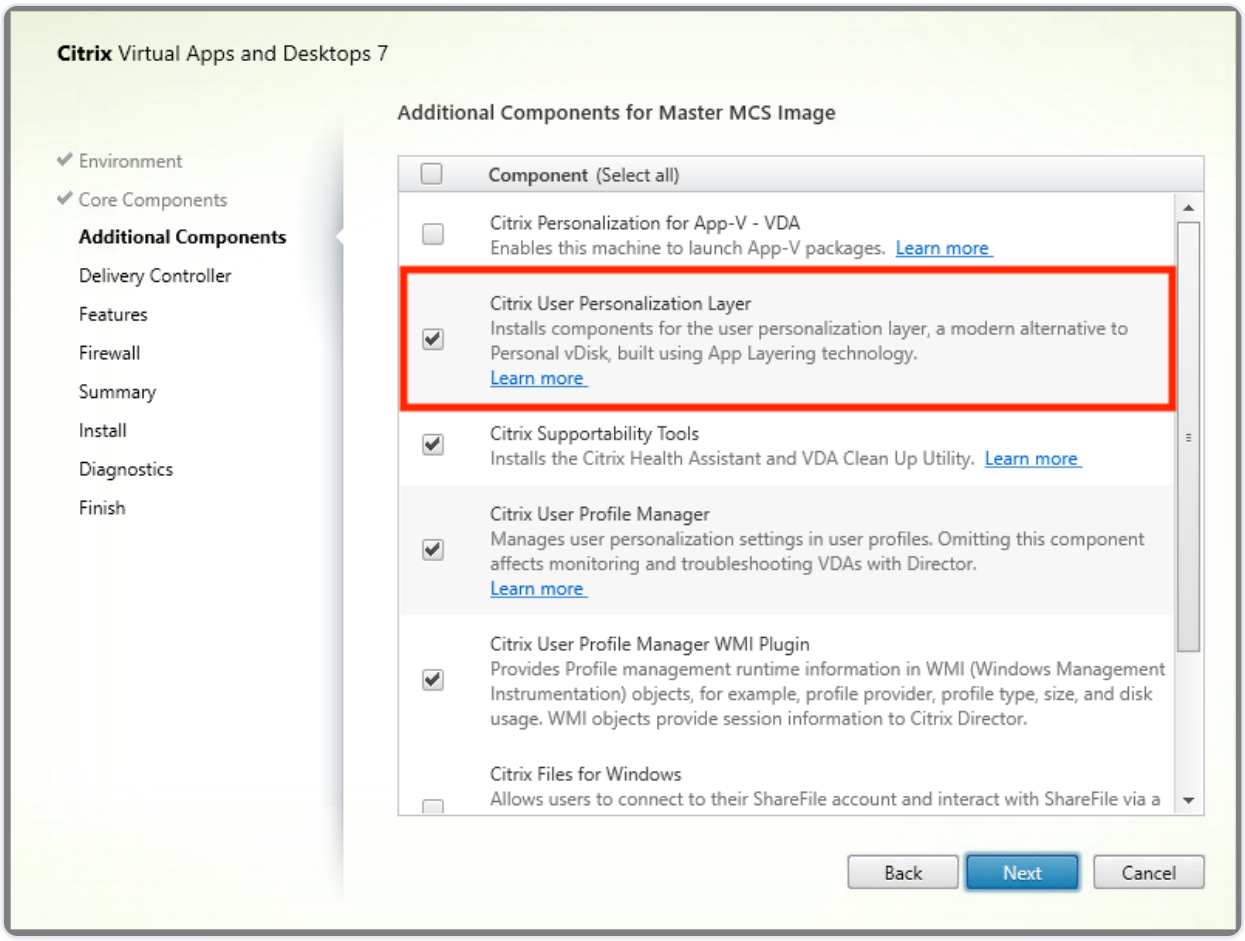


a. **Ambiente:** Selecione **Criar uma imagem mestre MCS** ou **Criar uma imagem mestre usando o Citrix Provisioning ou ferramentas de provisionamento de terceiros**.



a. **Componentes Principais:** Clique em **Avançar**.

b. **Componentes Adicionais:** Marque **Camada de Personalização do Usuário Citrix**.



a. Clique nas telas de instalação restantes, configure o VDA conforme necessário e clique em **Instalar**. A imagem reinicia uma ou mais vezes durante a instalação.

4. Deixe as **atualizações do Windows** desativadas. 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 Web Studio.

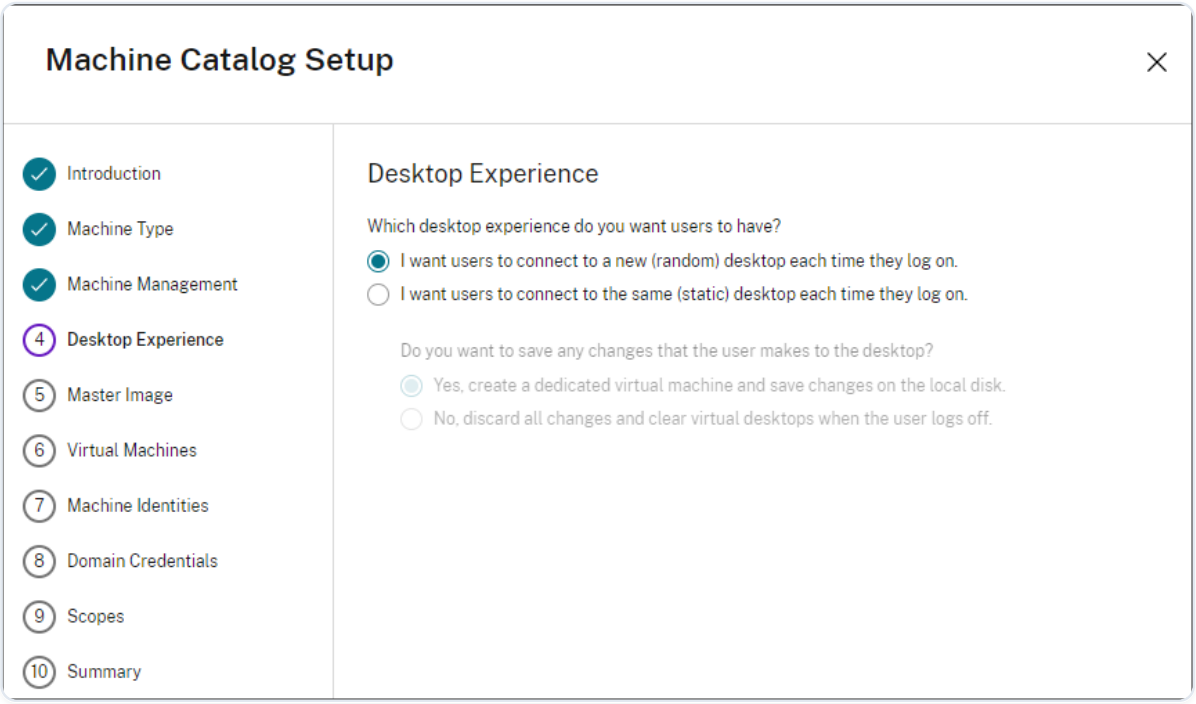
> **Observação:**
>
> Se você simplesmente deseja atualizar a camada de personalização do usuário (UPL), pode fazê-lo com uma versão mais recente da UPL e o pacote autônomo. Você não precisa atualizar o VDA.

Etapa 3: Criar um catálogo de máquinas

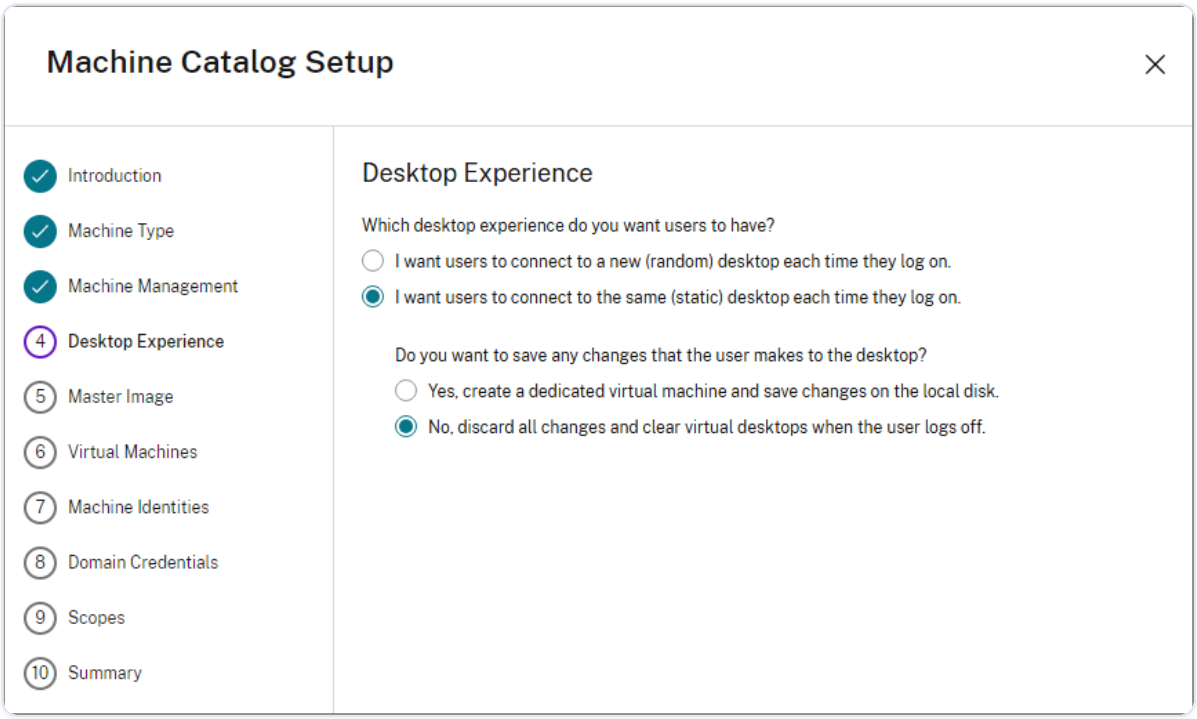
No Web Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

1. Selecione **Sistema Operacional** e defina-o como **SO de sessão única**.
2. Selecione **Gerenciamento de Máquinas** e defina-o como **Máquinas com gerenciamento de energia**. Por exemplo, máquinas virtuais ou PCs blade.
3. Selecione **Experiência de Área de Trabalho** e defina-o como tipo de catálogo **pooled-random** ou **pooled-static**, como nos exemplos a seguir:

   - **Pooled-random:**



   - **Pooled-static:** Se você selecionar pooled-static, configure as áreas de trabalho para descartar todas as alterações e limpar as áreas de trabalho virtuais quando o usuário fizer logoff, conforme mostrado na seguinte captura de tela:



Observação:

A camada de personalização do usuário não oferece suporte a catálogos pooled-static configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se você estiver usando o MCS, selecione **Imagem** e o instantâneo para a imagem criada na seção anterior.
5. Configure as propriedades restantes do catálogo conforme necessário para o seu ambiente.

Passo 4: Criar um grupo de entrega

Crie e configure um **grupo de entrega**, incluindo máquinas do catálogo de máquinas que você criou. Para obter detalhes, consulte Criar Grupos de Entrega.

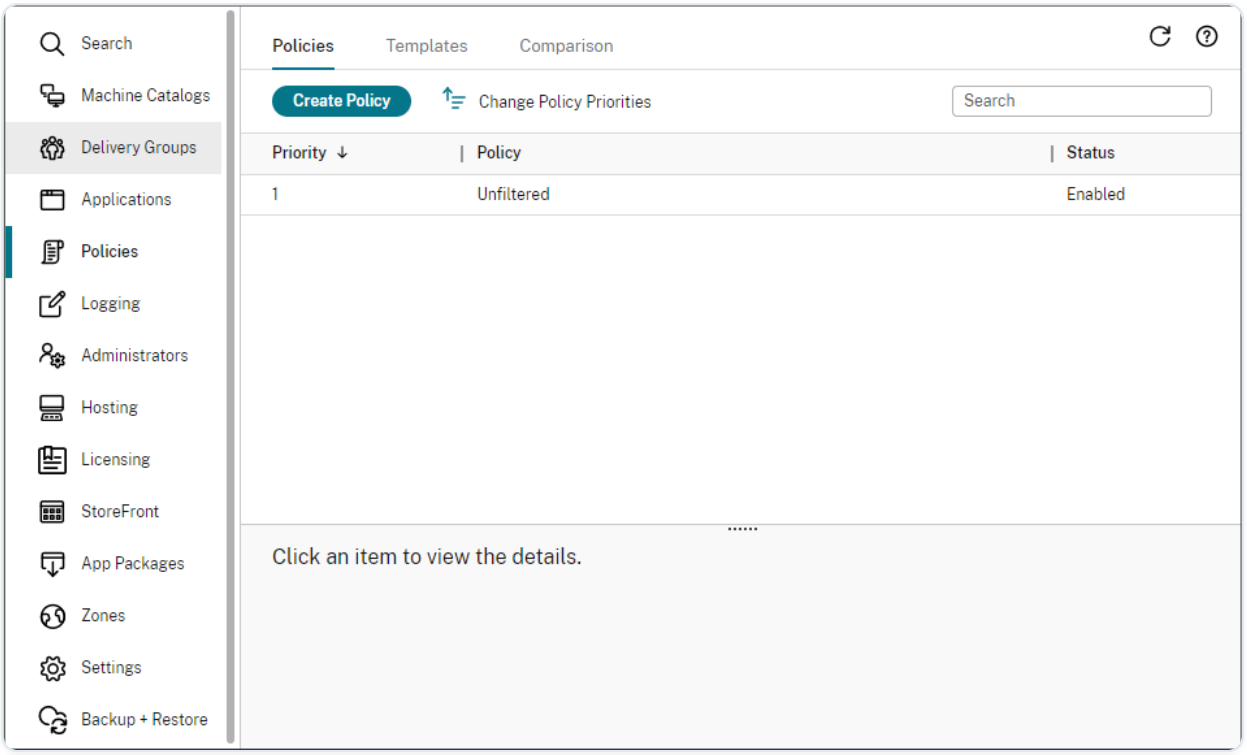
Passo 5: Criar políticas personalizadas de grupo de entrega

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, você usa os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- Qual o tamanho máximo permitido para o crescimento dos discos da camada de usuário.

Para definir os parâmetros como políticas personalizadas do Citrix no Web Studio e atribuí-los ao seu grupo de entrega.

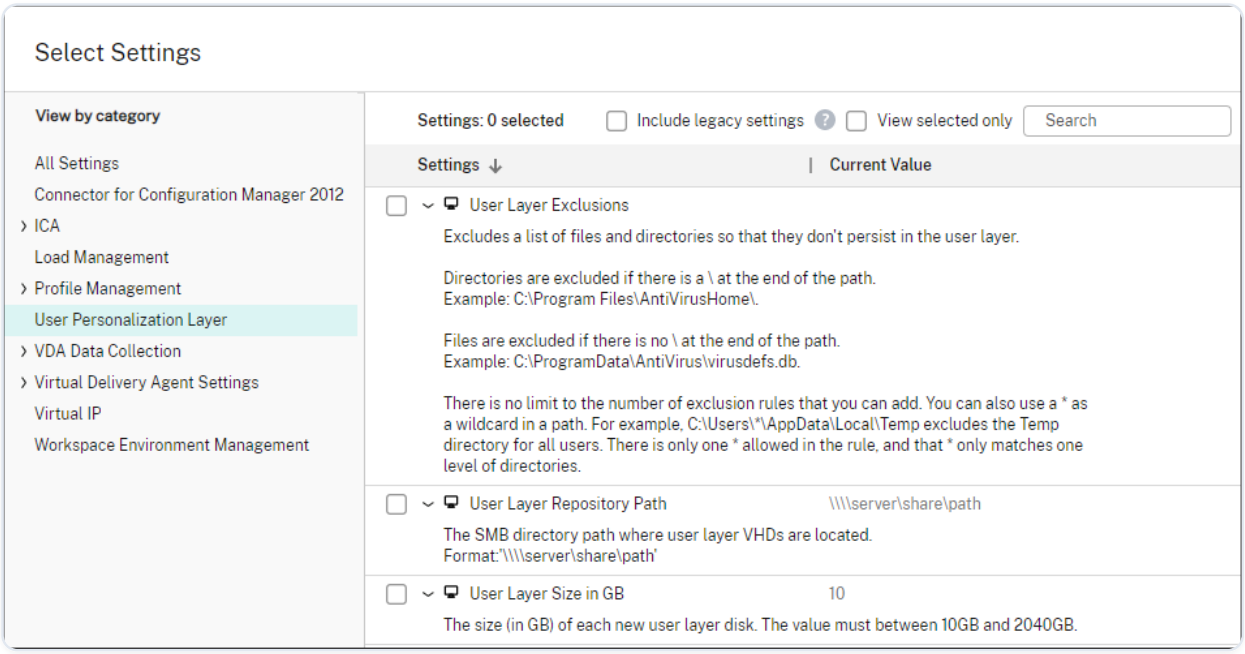
1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo:



2. Selecione **Criar Política** na barra de ações. A janela Criar Política é exibida.
3. Digite `user layer` no campo de pesquisa. As três políticas a seguir aparecem na lista de políticas disponíveis:

   - Exclusões da Camada de Usuário
   - Caminho do Repositório da Camada de Usuário
   - Tamanho da Camada de Usuário GB

   > **Observação:**
   >
   > Aumentar o tamanho afeta novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.



4. Marque a caixa de seleção ao lado de **User Layer Repository Path** e clique em **Edit**. A janela **Edit Setting** é exibida.
5. Insira um caminho no campo **Value** e clique em **Save**:

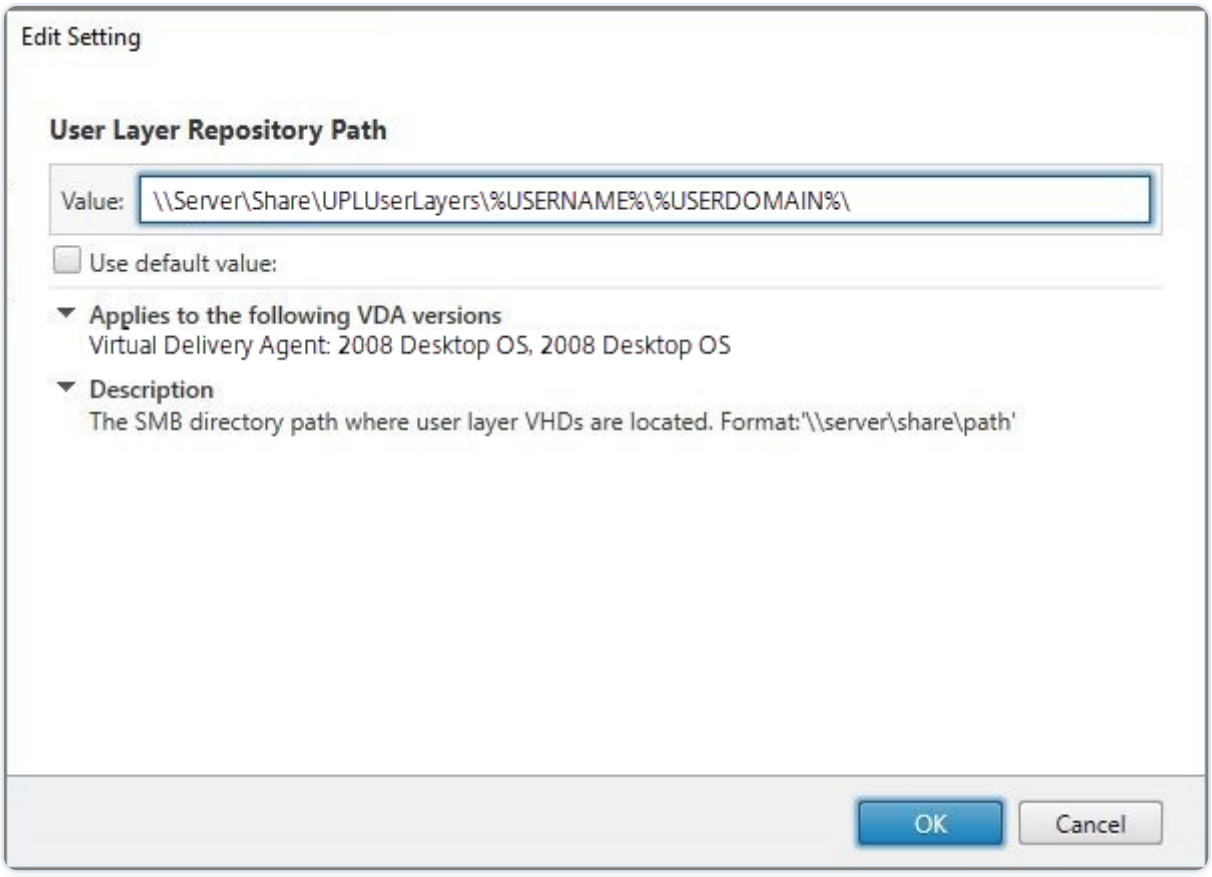
   - **Formato do caminho:** `\\server-name-or-address\share-name\folder`
   - **Exemplo de caminho:** `\\Server\Share\UPLUsers`
   - **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho é: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



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:

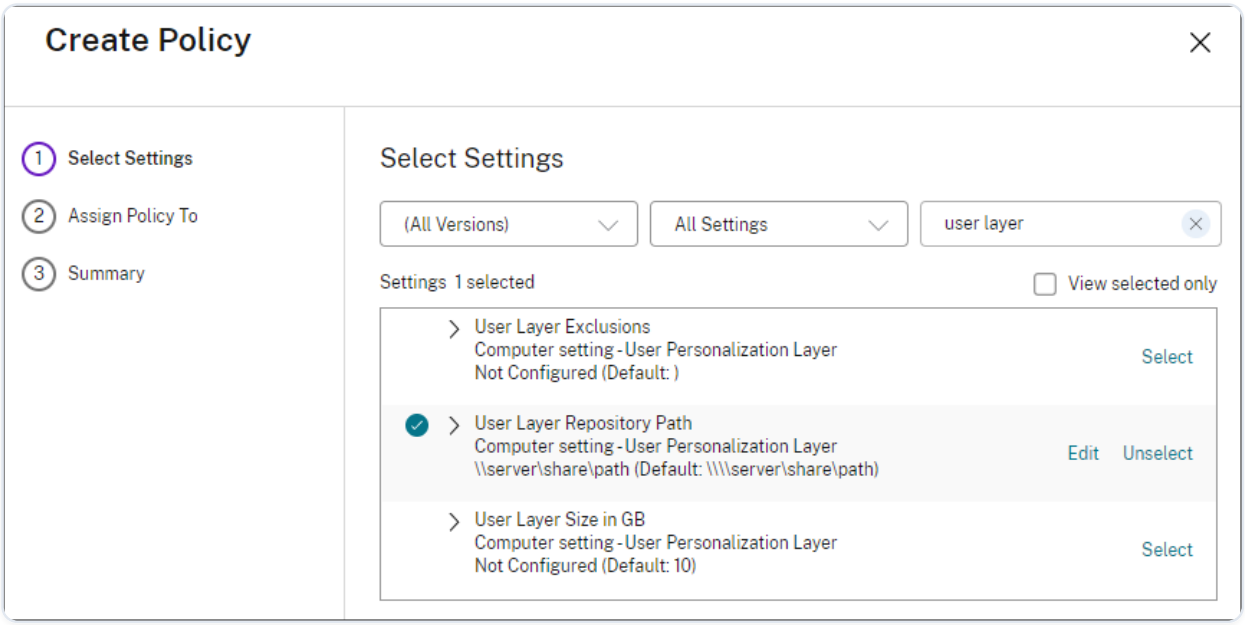
- **Formato do caminho:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Exemplo de caminho:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



Exemplo de atributos AD personalizados:

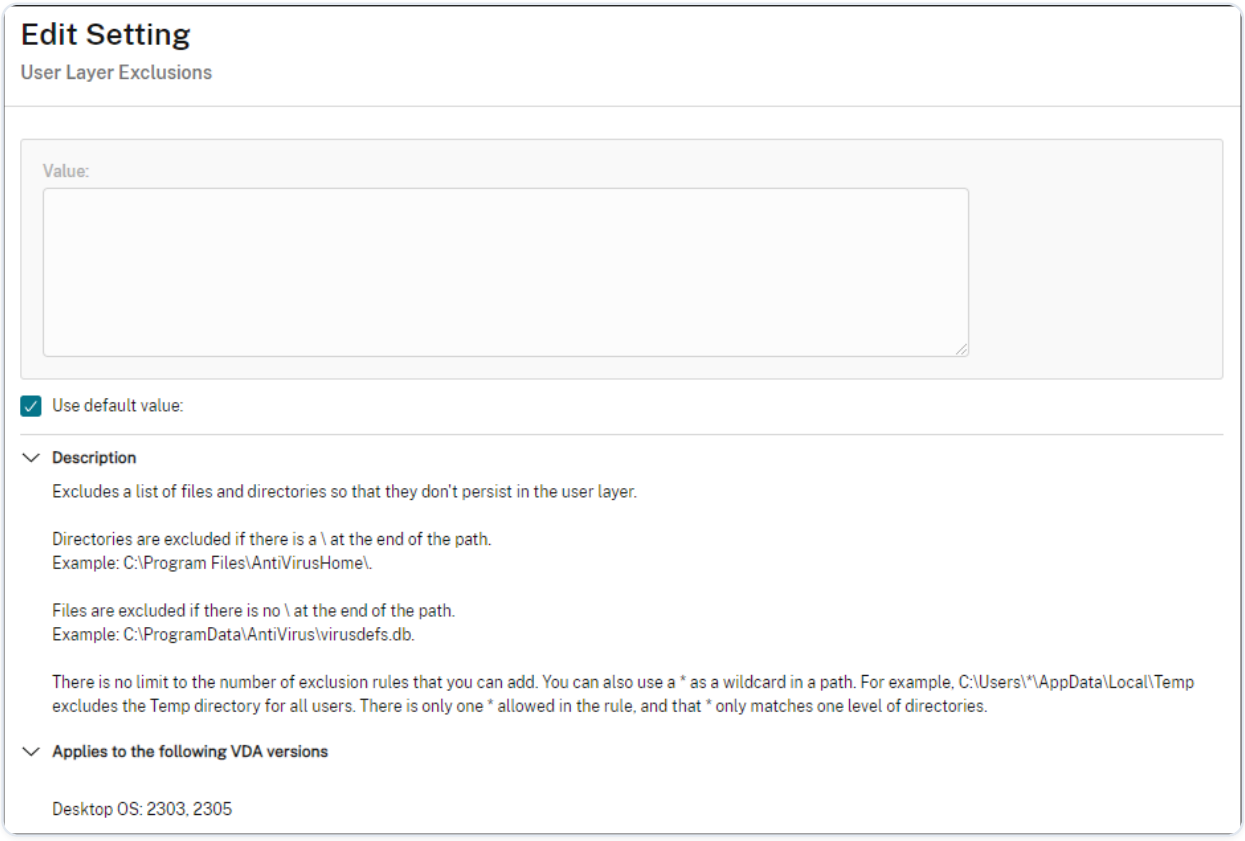
- Formato do caminho: `\\Server-name-or-address\share-name\AD-attribute`
- Exemplo de caminho: `\\Server\share#sAMAccountName#`
- Exemplo de caminhos resultantes: `\\Server\share\JohnSmith` (se #sAMAccountName# for resolvido para JohnSmith para o usuário atual)

6. Opcional: Marque a caixa de seleção ao lado de **User Layer Size in GB** e clique em **Edit**:



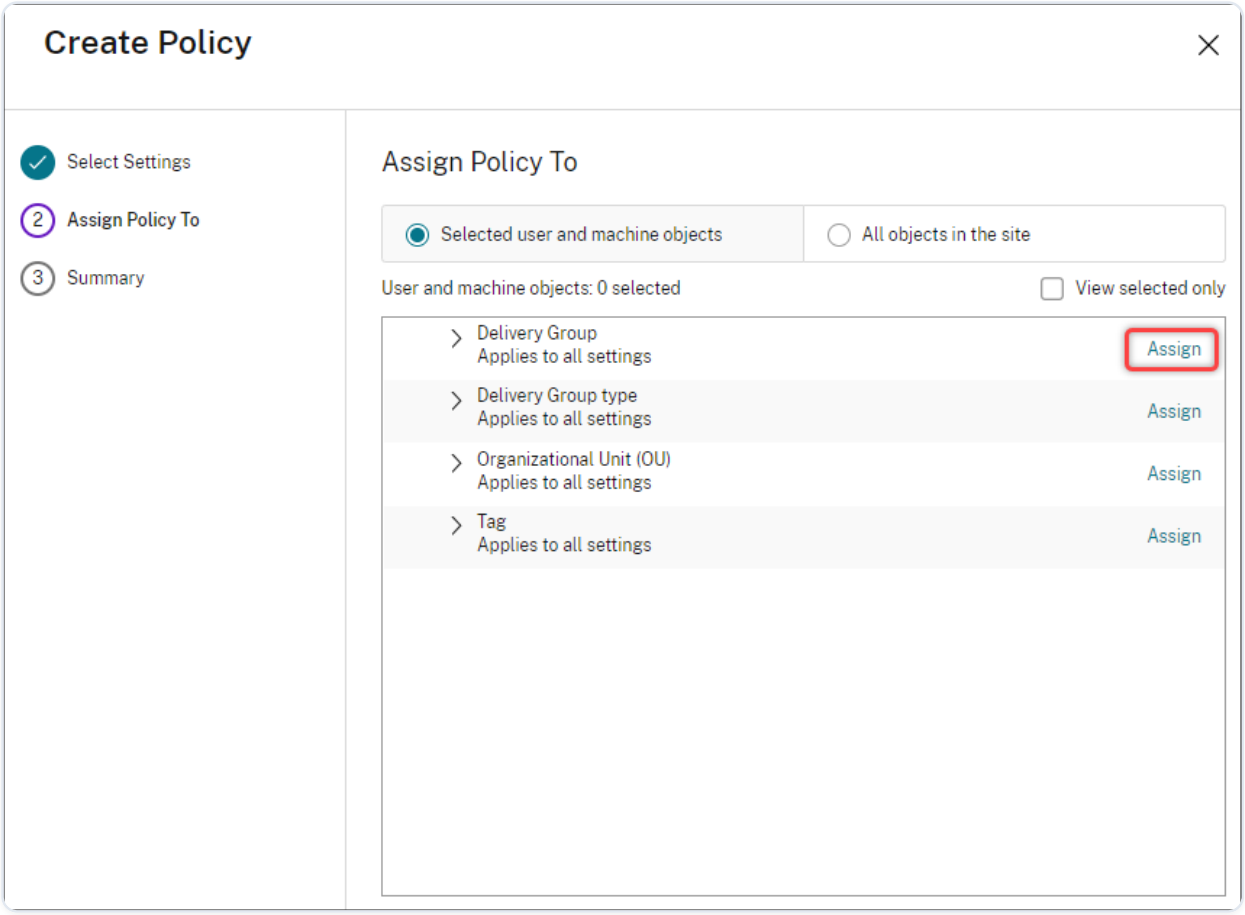
A janela Editar Configurações é exibida.

7. Opcional: Altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode atingir. Clique em **Save**.
8. Opcional: Marque a caixa de seleção ao lado de **User Layer Exclusions** e clique em **Edit**.

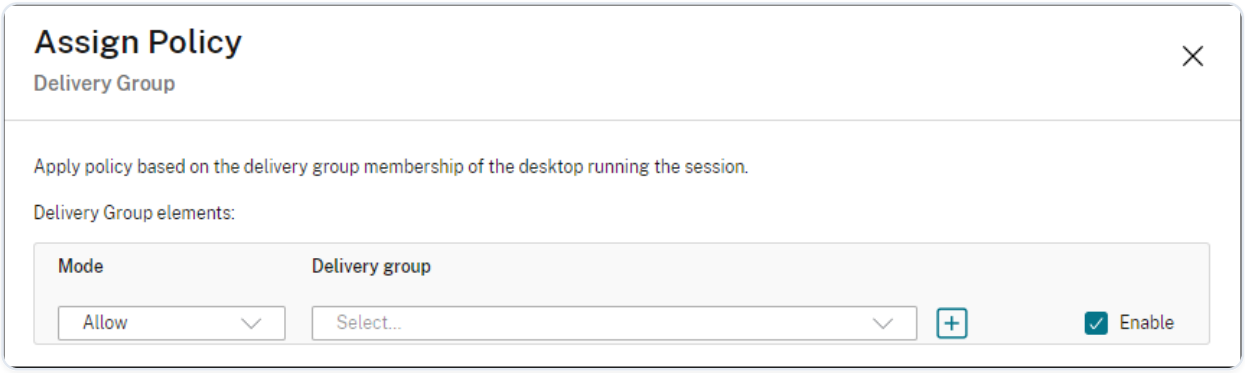


9. Opcional: Especifique os arquivos e pastas a serem excluídos e clique em **Save**. Para obter mais informações, consulte a documentação do Citrix App Layering.

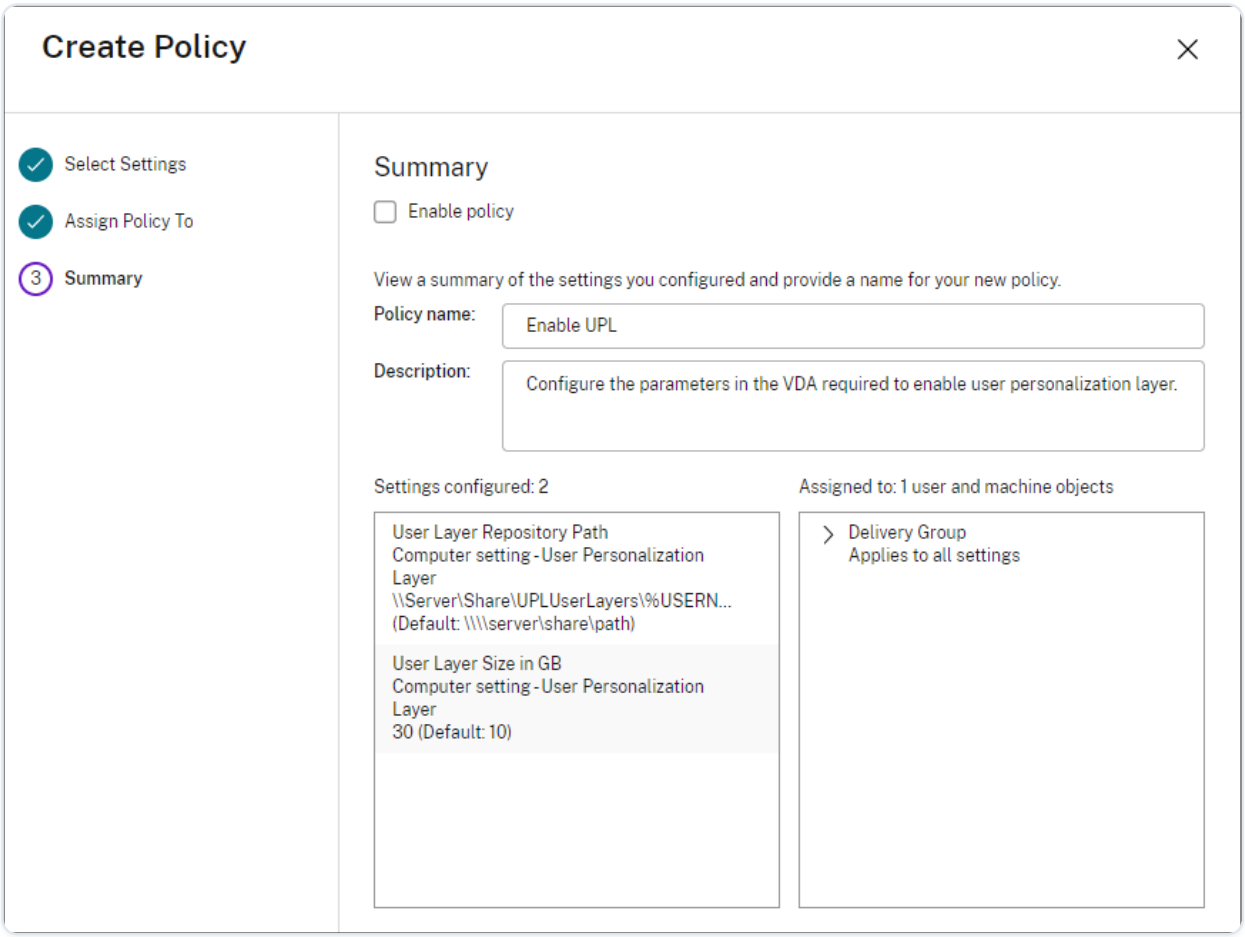
10. Clique em **Next** para configurar os usuários e máquinas aos quais você deseja atribuir. Clique no link **Delivery Group Assign** destacado nesta imagem:



11. No menu **Delivery Group**, selecione o grupo de entrega criado na seção anterior. Clique em **OK**.



12. Insira um nome para a política. Marque a caixa de seleção para habilitar a política e clique em **Finish**.



Configurar configurações de segurança na pasta da camada de usuário

Como administrador de domínio, você pode especificar mais de um local de armazenamento para suas camadas de usuário. Crie uma subpasta `\Users` para cada local de armazenamento (incluindo o local padrão). Proteja cada local usando as seguintes configurações.

NOME DA CONFIGURAÇÃO	VALOR	APLICAR A	
Criador Proprietário	Modificar	Somente Subpastas e Arquivos	
Direitos do Proprietário	Modificar	Somente Subpastas e Arquivos	
Usuários ou grupo	Criar Pasta/Anexar Dados; Atravessar Pasta/Executar Arquivo; Listar Pasta/Ler Dados; Ler Atributos	Somente Pasta Selecionada	

NOME DA CONFIGURAÇÃO	VALOR	APLICAR A	
Sistema	Controle Total	Pasta Selecionada, Subpastas e Arquivos	
Administradores de Domínio e grupo de Administradores selecionado	Controle Total	Pasta, Subpastas e Arquivos Selecionados	

Mensagens da camada de usuário

Quando um usuário não consegue acessar sua camada de usuário, ele recebe uma destas mensagens de notificação.

- **Camada de Usuário em Uso**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Camada de Usuário Indisponível**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Sistema não redefinido após o logoff do usuário**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

Arquivos de log para usar na solução de problemas

O arquivo de log, ulayersvc.log, contém a saída do software da camada de personalização do usuário onde as alterações são registradas.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

Recuperação de espaço da Camada de Usuário/UPL

Você pode usar a **recuperação de espaço da Camada de Usuário/UPL** para compactar automaticamente os arquivos VHDX toda vez que o usuário fizer logoff. Para obter mais informações, consulte Recuperação de espaço da Camada de Usuário/UPL

Limitações

Tenha as seguintes limitações em mente ao instalar e usar o recurso de camada de personalização do usuário.

- NÃO *tente* implantar o software da camada de personalização do usuário em uma camada dentro do App Layering. Implante camadas de personalização do usuário no Citrix Virtual Apps and Desktops ou habilite camadas de usuário em um modelo de imagem do 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 de máquinas com uma imagem executando uma nova instalação do SO (mesmo que seja a mesma versão do Windows 10). A melhor prática é aplicar as atualizações ao SO dentro da mesma imagem mestre usada ao criar o catálogo de máquinas.
- NÃO use *drivers* de tempo de inicialização ou qualquer outra 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 completo App Layering 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 mestre de SO diferente.
- Quando um usuário faz logoff de uma sessão e depois faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Microsoft Software Center lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Indisponível** na segunda máquina.

  Para descobrir o status real do aplicativo, instrua o usuário a selecionar o aplicativo no Software Center e clicar em **Instalar**. O SCCM então atualiza o status para o valor real.
- O Software Center ocasionalmente para imediatamente após ser iniciado em um VDA que tem o recurso de camada de personalização do usuário habilitado. Para evitar esse problema, siga

as recomendações da Microsoft para Implementar o SCCM em um ambiente VDI do XenDesktop. Além disso, certifique-se de que o serviço `ccmexec` esteja em execução antes de iniciar o Software Center.

- Nas Políticas de Grupo (Configurações do Computador), as configurações da camada de usuário substituem as configurações aplicadas à imagem mestre. Portanto, as alterações feitas nas Configurações do Computador usando uma GPO nem sempre estão presentes para o usuário no próximo login da sessão.

  Para contornar esse problema, crie um Script de Logon do Usuário que emita o comando:

  ```
  gpupdate /force
  ```

  Por exemplo, um cliente configurou o seguinte comando para ser executado em cada login de usuário:

  ```
  gpudate /Target:Computer /force
  ```

  Para obter melhores resultados, aplique as alterações nas Configurações do Computador diretamente na camada de usuário, depois que o usuário tiver feito login.
- Uma conta de usuário de domínio não deve ser o último usuário a ter feito login em uma imagem mestre. Caso contrário, as máquinas provisionadas a partir dessa imagem podem apresentar problemas.
- 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.

Remover componentes

Para remover componentes, a Citrix® recomenda usar o recurso do Windows para remover ou alterar programas. Alternativamente, você pode remover componentes usando a linha de comando ou um script na mídia de instalação.

Ao remover componentes, os pré-requisitos não são removidos e as configurações do firewall não são alteradas. Por exemplo, ao remover um Delivery Controller™, o software SQL Server e os bancos de dados não são removidos.

Se você atualizou um Controller de uma implantação anterior que incluía o Web Interface, você deve remover o componente Web Interface separadamente. Você não pode usar o instalador para remover o Web Interface.

Para obter informações sobre como remover recursos não mencionados abaixo, consulte a documentação do recurso.

Preparação

Antes de remover um Controller, remova-o do site. Para obter detalhes, consulte Remover um Controller.

Feche o Studio e o Director antes de removê-los.

Remover componentes usando o recurso do Windows para remover ou alterar programas

No recurso do Windows para remover ou alterar programas:

- Para remover um Controller, Studio, Director, License Server ou StoreFront, clique com o botão direito em **Citrix Virtual Apps *version*** ou **Citrix Virtual Apps and Desktops™ *version*** e selecione **Desinstalar**. O instalador é iniciado. Selecione os componentes a serem removidos.

  Alternativamente, você pode remover o StoreFront™ clicando com o botão direito em **Citrix StoreFront** e selecionando **Desinstalar**.
- Para remover um VDA, clique com o botão direito em **Citrix Virtual Delivery Agent *version*** e selecione **Desinstalar**. O instalador é iniciado e você pode selecionar os componentes a serem removidos. A máquina é reiniciada automaticamente após a remoção, por padrão.
- Para remover o Universal Print Server, clique com o botão direito em **Citrix Universal™ Print Server** e selecione **Desinstalar**.

Remover componentes principais usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopServerSetup.exe`.

- Para remover um ou mais componentes, especifique as opções `/remove` e `/components`.
- Para remover todos os componentes, especifique a opção `/removeall`.

Para obter detalhes de comando e parâmetro, consulte Instalar usando a linha de comando.

Por exemplo, o seguinte comando remove o Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

Remover VDAs usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopVdaSetup.exe`.

- Para remover um ou mais componentes, use as opções `/remove` e `/components`. Por exemplo, para remover o VDA e o aplicativo Citrix Workspace, use `/remove /components vda,plugin`.
- A opção `/removeall` remove apenas o VDA. Ela não remove o aplicativo Citrix Workspace.

Para obter detalhes de comandos e parâmetros, consulte Instalar usando a linha de comando.

A máquina reinicia automaticamente após a remoção, por padrão.

Para remover VDAs usando um script no Active Directory, consulte Instalar ou remover VDAs usando scripts.

Atualizar e migrar

Introdução

A atualização altera sua implantação para o Citrix Virtual Apps and Desktops™ 7 **Current Release (CR)** sem a necessidade de configurar novas máquinas ou sites. Isso é conhecido como uma atualização in-loco.

A atualização oferece acesso aos recursos e tecnologias mais recentes para os quais você é elegível. As atualizações também podem conter correções, esclarecimentos e aprimoramentos de versões anteriores.

Visão geral da atualização

1. Revise o artigo Atualizar uma implantação antes de iniciar a atualização. Esta é a principal fonte de informação para aprender como se preparar e implementar uma atualização.
2. Certifique-se de que as datas atuais dos seus Customer Success Services sejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo Licenças de renovação do Customer Success Services.
3. Conclua as orientações de preparação.
4. Execute os instaladores para atualizar os componentes principais.
5. Atualize os bancos de dados do sistema e o site.
6. Atualize os VDAs em imagens (ou diretamente nas máquinas).
7. Atualize outros componentes.

Cada etapa de preparação e atualização é detalhada em Atualizar uma implantação.

Versões que você pode atualizar

Você pode atualizar para o Citrix Virtual Apps and Desktops 2407 a partir de:

- Virtual Apps and Desktops 2203 LTSR com ou sem CUs, até e incluindo CU5
- Virtual Apps and Desktops 1912 LTSR com ou sem CUs, até e incluindo CU9
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

Você também pode consultar o Guia de Atualização do Citrix para obter uma lista das versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop) a partir das quais você pode fazer upgrade.

> Nota:
>
> - Antes de iniciar o processo de upgrade, a Citrix® recomenda que os clientes testem o upgrade em um ambiente controlado e verifiquem se ele atende aos seus requisitos específicos. Além disso, aconselhamos revisar toda a documentação relevante do produto, incluindo a lista de descontinuações e problemas conhecidos, para garantir uma transição tranquila. Essa abordagem ajuda a mitigar possíveis interrupções nos sistemas de produção e aprimora a experiência geral de upgrade.
> - O Citrix Virtual Apps and Desktops 1912 LTSR em breve atingirá sua fase de fim de vida. Para obter mais informações sobre a lista de versões suportadas, consulte Matriz de Produtos.

Perguntas frequentes

Esta seção responde a algumas perguntas frequentes sobre o upgrade do Citrix Virtual Apps and Desktops.

- **Qual é a ordem correta para fazer upgrade do meu ambiente Virtual Apps and Desktops?**

  Para uma ilustração e descrição da sequência de upgrade recomendada, consulte Sequência de upgrade e Procedimento de upgrade.

- **Meu site tem vários Delivery Controllers (em diferentes zonas). O que acontece se eu fizer upgrade apenas de alguns deles? Sou obrigado a fazer upgrade de todos os Controllers no site durante a mesma janela de manutenção?**

  A melhor prática é fazer upgrade de todos os Delivery Controllers durante a mesma janela de manutenção, pois vários serviços em cada Controller se comunicam entre si. Manter versões diferentes pode causar problemas. Durante uma janela de manutenção, recomendamos que você faça upgrade de metade dos Controllers, faça upgrade do site e, em seguida, faça upgrade dos Controllers restantes. Para obter detalhes, consulte o Procedimento de upgrade.

- **Posso ir diretamente para a versão mais recente ou preciso fazer upgrades incrementais?**

Você quase sempre pode fazer upgrade para a versão mais recente e pular lançamentos intermediários, a menos que explicitamente declarado no artigo **Novidades** para a versão para a qual você está fazendo upgrade.

- **Um cliente pode fazer upgrade de um ambiente Long Term Service Release (LTSR) para um Current Release?**

  Sim. Os clientes não são obrigados a permanecer em uma Long Term Service Release por um período prolongado. Os clientes podem mover um ambiente LTSR para uma Current Release, com base nos requisitos e recursos de negócios.

- **Versões mistas de componentes são permitidas?**

  Em cada site, a Citrix recomenda atualizar todos os componentes para a mesma versão. Embora você possa usar versões anteriores de alguns componentes, nem todos os recursos da versão mais recente podem estar disponíveis. Para obter mais informações, consulte Considerações sobre ambientes mistos.

- **Com que frequência uma Current Release deve ser atualizada?**

  As Current Releases atingem o Fim da Manutenção (EOM) 6 meses após a data de lançamento. A Citrix recomenda que os clientes adotem a Current Release mais recente. As Current Releases atingem o Fim da Vida Útil (EOL) 18 meses após a data de lançamento.

- **O que é recomendado: atualização para LTSR ou CR?**

  As Current Releases (CRs) oferecem os recursos e funcionalidades de virtualização de aplicativos, desktops e servidores mais recentes e inovadores. Isso permite que você permaneça na vanguarda da tecnologia e à frente da concorrência.

  As Long Term Service Releases (LTSRs) são ideais para grandes ambientes de produção corporativos que preferem manter a mesma versão base por um período prolongado.

```
For details, see [Servicing Options]( https://www.citrix.com/support/
citrix-customer-success-services/citrix-virtual-apps-and-desktops-
servicing-options.md).
```

- **Preciso atualizar minhas licenças?**

  Certifique-se de que a data da licença atual não expirou e é válida para a versão para a qual você está atualizando. Consulte CTX111618. Para obter informações sobre renovação, consulte Licenças de renovação dos Customer Success Services.

- **Quanto tempo leva uma atualização?**

O tempo necessário para atualizar uma implantação varia, dependendo da infraestrutura e da rede. Portanto, não podemos fornecer um tempo exato.

- **Quais são as melhores práticas?**

  Certifique-se de que você entende e segue as orientações de preparação.

- **Quais sistemas operacionais são suportados?**

  O artigo Requisitos do sistema para a versão para a qual você está atualizando lista os sistemas operacionais suportados.

  Se sua implantação atual usa sistemas operacionais que não são mais suportados, consulte Sistemas operacionais anteriores.

- **Quais versões do VMware vSphere (vCenter + ESXi) são suportadas?**

  CTX131239 lista os hosts e versões suportados, além de links para problemas conhecidos.

- **Quando minha versão chega ao fim da vida útil (EOL)?**

  Verifique a Matriz de Produtos.

- **Quais são os problemas conhecidos com a versão mais recente?**

  - Citrix Aplicativos Virtuais e Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - Aplicativo Citrix Workspace para Windows

Mais informações

As atualizações de implantação da **Long Term Service Release (LTSR)** usam Atualizações Cumulativas (CUs). Uma CU atualiza os componentes de base da LTSR, e cada CU inclui seu próprio metainstalador.

Cada CU possui documentação dedicada. Por exemplo, para a LTSR 2203, verifique o link na página **Novidades** dessa LTSR para a CU mais recente. Cada página da CU inclui informações de versão suportadas, instruções e um link para o pacote de download da CU.

Migrar

Migrar para a nuvem

Você pode usar a ferramenta de Configuração Automatizada para Citrix Virtual Apps and Desktops para migrar sua implantação local para a nuvem. Para mais informações, consulte Migrar para a Nuvem.

Migração legada

A migração move dados de uma implantação anterior para uma versão mais recente. O processo inclui a instalação de componentes mais recentes e a criação de um novo site, a exportação de dados do farm mais antigo e, em seguida, a importação dos dados para o novo site.

Não há ferramentas ou scripts suportados para migrar versões do XenApp e XenDesktop, ou migrar versões anteriores do Citrix Virtual Apps and Desktops. A *atualização* é suportada para as versões do Citrix Virtual Apps and Desktops descritas nesta documentação do produto.

Para conteúdo de migração anterior do XenApp 6.x, consulte o seguinte. Nem os scripts nem os artigos são suportados ou mantidos.

- Scripts de migração de código aberto para versões do XenApp 6.x estão disponíveis em `<https://github.com/citrix/xa65migrationtool>`. A Citrix não oferece suporte nem mantém esses scripts de migração
- Para **Alterações no 7.x**, **Atualizar um worker do XenApp 6.5 para um novo VDA** e **Migrar XenApp 6.x**, consulte o arquivo legado do Citrix Virtual Apps and Desktops em `<https://docs.citrix.com/pt-br/legacy-archive/citrix-virtual-apps-and-desktops.html>`.

Atualizar uma implantação

Introdução

Você pode atualizar certas implantações para versões mais recentes sem precisar configurar novas máquinas ou sites primeiro. Isso é chamado de atualização in-loco.

Para saber quais versões do Citrix Virtual Apps and Desktops você pode atualizar, consulte as Versões que você pode atualizar.

Antes de atualizar para qualquer uma das versões do Citrix Virtual Apps and Desktops, certifique-se de que suas datas atuais de Customer Success Services sejam válidas e não tenham expirado.

Para obter mais informações, consulte o artigo Licenças de renovação do Customer Success Services.

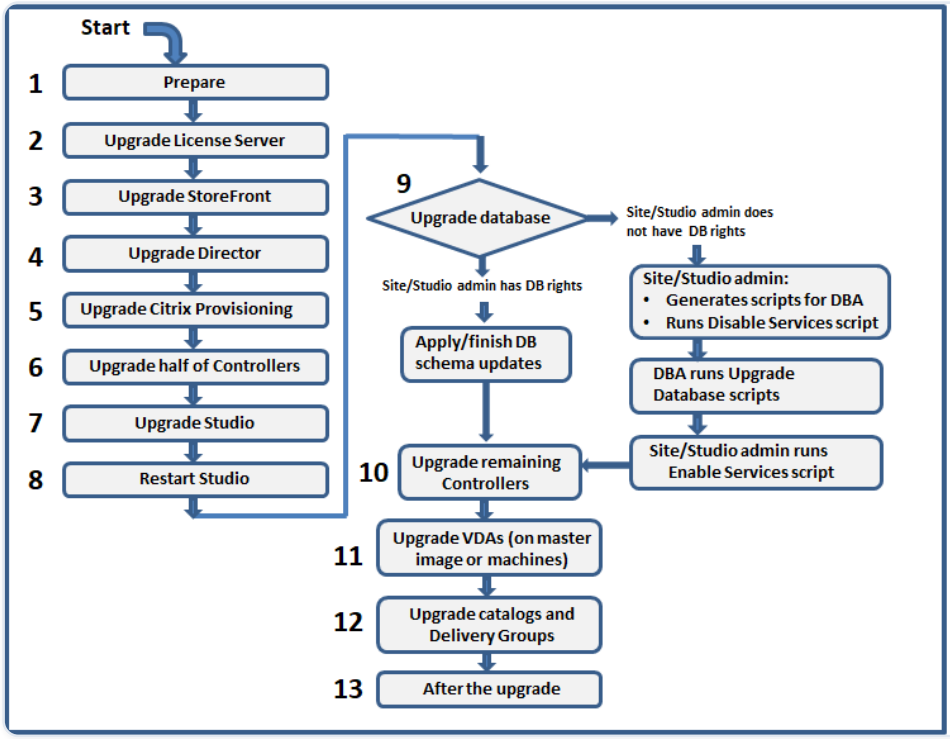
Para iniciar uma atualização, você executa o instalador da nova versão para atualizar os componentes principais, VDAs e outros componentes instalados anteriormente. Em seguida, você atualiza o banco de dados e o site.

Você pode atualizar qualquer componente que possa ser instalado com o instalador completo do produto (e os instaladores VDA autônomos), se houver uma versão mais recente disponível. Para outros componentes que não são instalados com o instalador completo do produto (como Citrix Provisioning™ e Profile Management), consulte a documentação desse componente para obter orientação. Para atualizações de host, consulte a documentação apropriada.

Revise todas as informações neste artigo antes de iniciar uma atualização.

Sequência de atualização

O diagrama a seguir mostra as etapas da sequência de atualização. Procedimento de atualização contém detalhes de cada etapa no diagrama.



Observação:

Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer uma das tarefas relacionadas ao provisionamento e ao grupo de

entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

Licenças de Direitos Híbridos

As licenças de Direitos Híbridos são licenças de assinatura baseadas em termo que são fornecidas, além da assinatura do serviço em nuvem, quando um cliente faz a transição ou upgrade de uma licença perpétua para uma assinatura de serviço em nuvem. Você também pode adquirir um complemento de Direitos Híbridos com suas assinaturas DaaS.

Se você tiver uma licença de Direitos Híbridos com um atributo SaaS, ao atualizar para o Citrix Virtual Apps and Desktops™ LTSR 2203 e posterior, você se tornará elegível para acessar recursos não disponíveis com o Citrix Virtual Apps and Desktops LTSR 1912. Esses recursos incluem provisionamento e hospedagem de cargas de trabalho em nuvens públicas, como Microsoft Azure, AWS EC2 e Google Cloud. Antes de implantar o novo arquivo de licença, atualize seu License Server para a versão mais recente.

Se você tiver acesso a uma licença de Direitos Híbridos sem atributo SaaS, siga estas etapas para obter acesso à nova licença de Direitos Híbridos com atributo SaaS:

Observação:

- Você recebe um e-mail com um novo código de licença. Para obter mais informações, consulte, Usar código de acesso de licença.
- Suas licenças existentes são revogadas. As licenças revogadas devem ser excluídas dos Servidores de Licença, seguidas pela instalação de novas licenças. Para obter mais informações, consulte Excluir arquivos de licença.

1. Vá para o portal citrix.com Gerenciar Licenças e baixe o novo arquivo de licença Hybrid Rights com os direitos de provisionamento de nuvem ativados (atributo SaaS). Para obter mais informações, consulte Baixar licenças. A imagem a seguir mostra o arquivo de licença Hybrid Rights com o atributo SaaS na seção Increments.



2. Instale o arquivo de licença Hybrid Rights no Servidor de Licenças. Para obter mais informações, consulte Instalar licenças.
3. Se houver uma alteração nas edições ou no modelo da licença, certifique-se de executar o comando do broker para definir a edição e o modelo e, em seguida, iniciar a atualização in-loco. Para obter mais informações sobre os comandos do Broker, consulte a seção Broker PowerShell SDK.

Para obter mais informações sobre o suporte a nuvem pública com o Citrix Virtual Apps and Desktops Current Releases e Long Term Service Releases, consulte CTX270373.

Procedimento de atualização

A maioria dos principais componentes do produto pode ser atualizada executando o instalador do produto na máquina que contém o componente.

Se uma máquina contiver mais de um componente (por exemplo, Studio e Servidor de Licenças), todos os componentes dessa máquina serão atualizados, se a mídia do produto contiver versões mais recentes do software.

Para usar os instaladores:

- Para executar a interface gráfica do instalador completo do produto, faça logon na máquina e, em seguida, insira a mídia ou monte a unidade ISO para a nova versão. Clique duas vezes em **AutoSelect**.
- Para usar a interface de linha de comando, emita o comando apropriado. Consulte Instalar usando a linha de comando.

Etapa 1: Preparar

Antes de iniciar uma atualização, certifique-se de estar pronto. Leia e conclua todas as tarefas necessárias:

- Remover PVD, AppDisks™ e hosts não suportados(#remove-pvd-appdisks-and-unsupported-hosts)
- VDAs que possuem componentes PvD ou AppDisk(#vdas-that-have-pvd-or-appdisks-components)
- Limitações
- Considerações sobre ambiente misto(#mixed-environment-considerations)
- Sistemas operacionais anteriores(#earlier-operating-systems)

- Preparação(#preparation)
- Testes preliminares do site(#preliminary-site-tests)
- Verificação da versão do SQL Server(#sql-server-version-check)

Etapa 2: Atualizar o License Server

Se a instalação tiver uma nova versão do software Citrix License Server, atualize este componente primeiro, antes de qualquer outro componente.

Se você ainda não determinou se o seu License Server é compatível com a nova versão, é essencial que você execute o instalador no License Server antes de atualizar quaisquer outros componentes principais.

Etapa 3: Atualizar o StoreFront™

Se a mídia de instalação contiver uma nova versão do software StoreFront, execute o instalador na máquina que contém o servidor StoreFront.

- Na interface gráfica, escolha **Citrix StoreFront** na seção **Estender implantação**.
- Na linha de comando, execute `CitrixStoreFront-x64.exe`, que está disponível na pasta `x64` da mídia de instalação do Citrix Virtual Apps and Desktops.

Etapa 4: Atualizar o Director

Se a mídia de instalação contiver uma nova versão do software Director, execute o instalador na máquina que contém o Director.

Etapa 5: Atualizar o Citrix Provisioning

A mídia de instalação do Citrix Provisioning está disponível separadamente da mídia de instalação do Citrix Virtual Apps and Desktops. Para saber como instalar e atualizar o servidor Citrix Provisioning e o software do dispositivo de destino, consulte a documentação do produto Citrix Provisioning.

Etapa 6: Atualizar metade dos Delivery Controllers

Por exemplo, se o seu site tiver quatro Controllers, execute o instalador em dois deles.

Deixar metade dos Controllers ativos permite que os usuários acessem o site. Os VDAs podem se registrar nos Controllers restantes. Pode haver momentos em que o site tenha capacidade reduzida porque menos Controllers estão disponíveis. A atualização causa apenas uma breve interrupção no estabelecimento de novas conexões de cliente durante as etapas finais de

atualização do banco de dados. Os Controllers atualizados não podem processar solicitações até que todo o site seja atualizado.

Se o seu site tiver apenas um Controller, ele ficará inoperável durante a atualização.

Testes preliminares do site são executados no primeiro Controller, antes do início da atualização real. Para obter detalhes, consulte Testes preliminares do site.

Etapa 7: Atualizar o Studio

Se você ainda não atualizou o Web Studio (porque ele estava na mesma máquina que outro componente), execute o instalador na máquina que contém o Studio.

> **Observação:**
>
> Depois de atualizar o Web Studio, as informações de versão podem não ser atualizadas imediatamente. Você pode ser solicitado a atualizar o Web Studio mesmo que ele já esteja atualizado. Para resolver o problema, vá para o servidor Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegar para Página Inicial > Sites > Site Padrão, e selecione **Reiniciar** no painel **Gerenciar Site**.

Etapa 8: Reiniciar o Studio

Reinicie o Web Studio atualizado. O processo de atualização é retomado automaticamente.

Etapa 9: Atualizar banco de dados e site

> **Observação:**
>
> Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer uma das tarefas relacionadas ao provisionamento e grupo de entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

> Verifique Preparação para as permissões necessárias para atualizar o esquema dos bancos de dados do SQL Server.

- Se você tiver permissão suficiente para atualizar o esquema do banco de dados do SQL Server, poderá iniciar uma atualização automática do banco de dados. Continue com Atualizar o banco de dados e o site automaticamente.
- Se você não tiver permissões de banco de dados suficientes, poderá iniciar uma atualização manual que usa scripts e prosseguir com a ajuda do seu administrador de banco de dados (alguém que tenha as permissões necessárias). Para uma atualização manual, o usuário do Studio gera os scripts e, em seguida, executa os scripts que habilitam e desabilitam os serviços. O administrador do banco de dados executa outros scripts que atualizam o esquema do banco de dados, usando o utilitário SQLCMD ou o SQL Server Management Studio no modo SQLCMD. Continue com Atualizar o banco de dados e o site manualmente.
- Se você tiver uma implantação multizona e quiser atualizar o banco de dados e o site automaticamente, a Citrix recomenda que a atualização do dbschema seja realizada na mesma zona que hospeda os bancos de dados do SQL Server do site. Caso contrário, a atualização automática do banco de dados e do site poderá falhar.

A Citrix recomenda fortemente que você faça backup do banco de dados antes de atualizar. Consulte CTX135207. Durante uma atualização de banco de dados, os serviços do produto são desabilitados. Durante esse período, os Controllers não podem intermediar novas conexões para o site, portanto, planeje cuidadosamente.

Atualizar o banco de dados e o site automaticamente

1. Inicie o Studio recém-atualizado.
2. Indique que você deseja iniciar a atualização do site automaticamente e confirme que está pronto.

A atualização do banco de dados e do site prossegue.

Atualizar o banco de dados e o site manualmente

1. Inicie o Studio recém-atualizado.
2. Indique que você deseja atualizar o site manualmente. O assistente verifica a compatibilidade do License Server e solicita confirmação.
3. Confirme que você fez backup do banco de dados.

   O assistente gera e exibe os scripts e uma lista de verificação das etapas de atualização. Se o esquema de um banco de dados não tiver sido alterado desde a versão do produto que está sendo atualizada, esse script não será gerado. Por exemplo, se o esquema do banco de dados de log não for alterado, o script `UpgradeLoggingDatabase.sql` não será gerado.

4. Execute os seguintes scripts na ordem mostrada.

    - `DisableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para desabilitar os serviços do produto.
    - `UpgradeSiteDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Site
    - `UpgradeMonitorDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados do Monitor.
    - `UpgradeLoggingDatabase.sql`: O administrador do banco de dados executa este script SQL no servidor que contém o banco de dados de Log de Configuração. Execute este script somente se este banco de dados for alterado (por exemplo, após aplicar um hotfix).
    - `EnableServices.ps1`: O usuário do Studio executa este script PowerShell em um Controller para habilitar os serviços do produto.

    Após a conclusão da atualização do banco de dados e a habilitação dos serviços do produto, o Studio testa automaticamente o ambiente e a configuração e, em seguida, gera um relatório HTML. Se problemas forem identificados, você poderá restaurar o backup do banco de dados. Após resolver os problemas, você pode atualizar o banco de dados novamente.

5. Após concluir as tarefas da lista de verificação, clique em **Concluir atualização**.

Etapa 10: Atualizar os Delivery Controllers restantes

No Studio recém-atualizado, selecione **Citrix Studio** *nome-do-site* no painel de navegação. Na guia **Tarefas Comuns**, selecione **Atualizar os Delivery Controllers restantes**.

> **Observação:**

> Para que **Atualizar os Delivery Controllers restantes** esteja disponível, crie pelo menos um catálogo de máquinas e um grupo de entrega para o site.

> Após concluir a atualização e confirmar a conclusão, feche e reabra o Studio. O Studio pode solicitar uma atualização extra do site para registrar os serviços do Controller no site ou para criar um ID de zona, se ele não existir.

Etapa 11: Atualizar VDAs

> **Importante:**

> Se você estiver atualizando um VDA para a versão 1912 ou posterior, consulte Atualizando VDAs para 1912 ou posterior.

> Execute o instalador do produto nas máquinas que contêm VDAs.

Se você usou o Machine Creation Services™ e uma imagem mestre para criar máquinas, vá para o seu host e atualize o VDA na imagem mestre. Você pode usar qualquer um dos instaladores de VDA disponíveis.

- Para obter orientação sobre a interface gráfica, consulte Instalar VDAs.
- Para obter orientação sobre a linha de comando, consulte Instalar usando a linha de comando.

Se você usou o Citrix Provisioning para criar máquinas, consulte a documentação do produto Citrix Provisioning para obter orientação sobre a atualização.

Etapa 12: Atualizar catálogos de máquinas e Delivery Groups

- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Atualizar Delivery Groups que usam máquinas com VDAs atualizados.

Etapa 13: Após a atualização

Atualize outros componentes em sua implantação. Para obter orientação, consulte a seguinte documentação do produto:

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Gerenciamento do Ambiente de Trabalho

Se você precisar substituir o software Microsoft SQL Server Express LocalDB por uma versão posterior, consulte Substituir SQL Server Express LocalDB.

Atualização do dbschema

Ao atualizar sua implantação, vários esquemas de banco de dados podem ser atualizados. A tabela a seguir lista quais esquemas de banco de dados são atualizados no processo:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

Definição de termos:

- Site: Datastore do Site. A atualização do dbschema é feita no Datastore do Site.
- Monitor: Datastore do Monitor. A atualização do dbschema é feita no Datastore do Monitor.
- Config: Tabela de Configuração. A versão do Desktop Studio, as informações de Licenciamento ou ambos são atualizados na tabela de Configuração.
- Logging: Datastore de Log. A atualização do dbschema é feita no Datastore de Log.

Atualizar VDAs para 2203 ou posterior

Se o componente Personal vDisk (PvD) foi instalado em um VDA, esse VDA não pode ser atualizado para a versão 2203 ou posterior. Para usar o novo VDA, você deve desinstalar o VDA atual e, em seguida, instalar o novo VDA.

Esta instrução se aplica mesmo 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 **Componentes Adicionais**.
- Na linha de comando, a opção `/baseimage` instalou o PvD. Se você especificou esta opção ou usou um script que continha esta opção, o PvD foi instalado.

Se você não souber se o seu VDA tem o PvD instalado, execute o instalador do novo VDA (2203 ou posterior) na máquina ou imagem.

- Se o PvD estiver instalado, uma mensagem será exibida, indicando que há um componente incompatível.
  - Na interface gráfica, clique em **Cancelar** na página que contém a mensagem e, em seguida, confirme que deseja fechar o instalador.
  - Na CLI, o comando simplesmente falha com a mensagem exibida.

- Se o PvD não estiver instalado, a atualização prossegue.

O que fazer

Se o VDA não tiver o PvD instalado, siga o procedimento de atualização usual.

Se o VDA tiver o PvD instalado:

1. Desinstale o VDA atual.
2. Instale o novo VDA.

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.

> **Observação:**

> *Posso usar o Personal vDisk com desktops Windows 7 no XenApp e XenDesktop 7.15 LTSR?*

> A Citrix excluiu o Personal vDisk (PvD) do XenApp e XenDesktop 7.6 LTSR, que foi anunciado em janeiro de 2016. Além disso, a Citrix anunciou a descontinuação da tecnologia PvD e recomenda que os clientes comecem a usar o Citrix App Layering daqui para frente. O Citrix App Layering (versão 4.4 e posterior) é um componente compatível do XenApp e XenDesktop 7.15 LTSR. No entanto, para ajudar os clientes com implantações existentes de PvD no Windows 7 a migrar para a tecnologia Citrix App Layering, a Citrix decidiu fornecer suporte por tempo limitado para implantações de PvD para desktops Windows 7 por meio das Atualizações Cumulativas (CUs) do XenApp e XenDesktop 7.15 LTSR até Jan 14, 2020. O componente PvD será removido das CUs do LTSR e não será suportado após Jan 14, 2020. Além disso, o uso de PvD para Windows 7 após Jan 14, 2020 tornará os sites LTSR não conformes. Além disso, o PvD para Windows 10 permanece excluído do 7.15 LTSR. Portanto, os clientes não devem usá-lo com seus sites 7.15 LTSR.

Remover PvD, AppDisks e hosts não suportados

As seguintes tecnologias e tipos de host não são suportados em implantações do Citrix Virtual Apps and Desktops 7 Current Release:

- **Personal vDisks (PvD)** para armazenar dados próximos às VMs dos usuários em catálogos. O recurso de camada de personalização do usuário agora lida com a persistência do usuário.

- **AppDisks** para gerenciar aplicativos usados em Delivery Groups.
- **Tipos de host:** Azure Classic, CloudPlatform (o produto Citrix original).
    - Para tipos de host suportados nesta versão, consulte Requisitos do sistema.
    - Para obter informações sobre maneiras alternativas de continuar usando ARM e AWS, consulte CTX270373.

Se sua implantação atual usa PvDs ou AppDisks, ou tem conexões com tipos de host não suportados (por exemplo, Microsoft Azure Classic), você pode atualizar para a versão 2006 (ou versões suportadas posteriores) somente após remover os itens que usam essas tecnologias. Se sua implantação atual usa conexões de host de nuvem pública (por exemplo, AWS), certifique-se de ter a Hybrid Rights License antes de atualizar. Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Hybrid Rights License, a atualização pausa ou para, e uma mensagem explicativa aparece. Os logs do instalador contêm detalhes.

Para ajudar a garantir uma atualização bem-sucedida, revise e siga as orientações aplicáveis para remover os itens não suportados.

- Remover PvD
- Remover AppDisks
- Remover itens de host não suportados

Mesmo que você não tenha usado PvD ou AppDisks em sua implantação, MSIs relacionados podem ter sido incluídos em uma instalação ou atualização anterior do VDA. Antes de poder atualizar seus VDAs para a versão 2006 (ou uma versão suportada posterior), você deve remover esse software, mesmo que nunca o tenha usado. Ao usar a interface gráfica, essa remoção pode ser feita para você, ou você pode incluir opções de remoção ao usar a CLI. Para detalhes, consulte Atualizando VDAs que possuem componentes PvD ou AppDisks.

Remover PvD

Uma atualização de implantação não pode ser bem-sucedida até que você remova todas as máquinas configuradas para usar PvD. Isso afeta catálogos e Delivery Groups.

Para remover PvD de grupos e catálogos:

1. No Studio, se um Grupo de Entrega contiver máquinas de um catálogo que usa PvD, remova essas máquinas do grupo.
2. No Studio, exclua todos os catálogos que contêm máquinas que usam PvD.

Atualizações de VDA: A atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA detectam. Para obter detalhes, consulte VDAs que têm componentes PvD ou AppDisks.

Se você planeja usar o App Layering em vez de PvD, consulte Migrando PvD para App Layering para obter informações sobre como mover dados.

Remover AppDisks

Uma atualização de implantação não pode prosseguir até que você remova os AppDisks de todos os Grupos de Entrega que os utilizam e, em seguida, remova os próprios AppDisks.

1. Selecione **Grupos de Entrega** no painel de navegação do Studio.
2. Selecione um grupo e clique em **Gerenciar AppDisks** no painel Ações.
3. Clique na ação que remove o AppDisk do grupo.
4. Repita as etapas 2 e 3 para cada Grupo de Entrega que usa AppDisks.
5. Selecione **AppDisks** no painel de navegação do Studio.
6. Selecione um AppDisk e clique na ação que exclui o AppDisk.
7. Repita as etapas 5 e 6 para cada AppDisk.

Atualizações de VDA: A atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA detectam. Para obter detalhes, consulte VDAs que têm componentes PvD ou AppDisks.

Remover itens de host não suportados

Uma atualização de implantação para a versão 2006 (ou versão posterior compatível) não pode prosseguir se o site tiver conexões com tipos de host não suportados, como Citrix CloudPlatform ou Microsoft Azure Classic. Conclua as seguintes tarefas antes de tentar uma atualização.

No Studio:

- Exclua todas as conexões para hosts não suportados.
- Se um Grupo de Entrega contiver máquinas de um catálogo criado com uma imagem mestre de um host não suportado, remova essas máquinas do grupo.
- Exclua todos os catálogos que foram criados usando uma imagem mestre de um host não suportado.

VDAs que possuem componentes PvD ou AppDisks

Se os componentes que habilitam as tecnologias PvD e AppDisks estiverem instalados em um VDA, esse VDA não poderá ser atualizado até que esses componentes sejam removidos.

> **Observação:**
>
> Ao atualizar para a versão 1912, você precisava desinstalar o VDA atual e, em seguida, instalar o novo VDA. Nesta versão, é perguntado se você deseja que a Citrix remova o componente e continue a atualização.
>
> Os componentes AppDisk e PvD podem ter sido instalados em versões anteriores do VDA, mesmo que você nunca tenha usado essas tecnologias:

- Interface gráfica: Nos instaladores do VDA, a página **Componentes Adicionais** continha a opção **Citrix AppDisk / Personal vDisk**. As versões 7.15 LTSR e anteriores 7.x habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou habilitou explicitamente a opção em qualquer versão que a oferecesse), esse componente foi instalado.
- CLI: A especificação da opção `/baseimage` instalou o componente.

O que fazer

Se o instalador do VDA não detectar os componentes AppDisks ou PvD no VDA atualmente instalado, a atualização prossegue normalmente.

Se o instalador detectar componentes AppDisks ou PvD no VDA atualmente instalado:

- Interface gráfica: A atualização é pausada. Uma mensagem pergunta se você deseja que os componentes não suportados sejam removidos automaticamente. Se você clicar em **OK**, os componentes são removidos automaticamente e a atualização prossegue.
- CLI: Para evitar falha no comando, inclua as seguintes opções no comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

Limitações

As seguintes limitações se aplicam às atualizações:

- **Instalação seletiva de componentes:** Se você instalar ou atualizar quaisquer componentes para a nova versão, mas optar por não atualizar outros componentes (em máquinas diferentes) que exijam atualização, o Studio o lembrará. Por exemplo, digamos que uma atualização inclua novas versões do Controller e do Studio. Você atualiza o Controller, mas não executa o instalador na máquina onde o Studio está instalado. O Studio não permitirá que você continue a gerenciar o site até que você atualize o Studio.

  Você não precisa atualizar os VDAs, mas a Citrix recomenda atualizar todos os VDAs para permitir que você use todos os recursos disponíveis.
- **Versões de Lançamento Antecipado ou Technology Preview:** Você não pode atualizar a partir de uma versão de Lançamento Antecipado, Technology Preview ou de pré-visualização.
- **Componentes em sistemas operacionais anteriores:** Você não pode instalar VDAs atuais em sistemas operacionais que não são mais suportados pela Microsoft ou Citrix. Para obter mais informações, consulte Sistemas operacionais anteriores.
- **Ambientes/sites mistos:** Se você precisar continuar a executar sites de versões anteriores e sites de versões atuais, consulte Considerações sobre ambientes mistos.
- **Seleção de produto:** Ao atualizar de uma versão anterior, você não escolhe ou especifica o produto (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) que foi definido durante a instalação.

Considerações sobre ambientes mistos

Ao atualizar, a Citrix recomenda que você atualize todos os componentes e VDAs para que possa acessar todos os recursos novos e aprimorados em sua edição e versão.

Por exemplo, embora você possa usar VDAs atuais em implantações que contêm versões anteriores do Controller, novos recursos na versão atual podem não estar disponíveis. Problemas de registro de VDA também podem ocorrer ao usar versões não atuais.

Em alguns ambientes, talvez você não consiga atualizar todos os VDAs para a versão mais atual. Nesse caso, ao criar um catálogo de máquinas, você pode especificar a versão do VDA instalada nas máquinas. (Isso é chamado de nível funcional.) Por padrão, essa configuração especifica a versão mínima recomendada do VDA. O valor padrão é suficiente para a maioria das implantações. Considere alterar a configuração para uma versão anterior somente se o catálogo contiver VDAs anteriores ao padrão. Não é recomendável misturar versões de VDA em um catálogo de máquinas.

Se um catálogo for criado com a configuração padrão de versão mínima do VDA, e uma ou mais máquinas tiverem um VDA anterior à versão padrão, essas máquinas não poderão se registrar no Controller e não funcionarão.

Para obter mais informações, consulte Versões de VDA e níveis funcionais.

Vários sites com versões diferentes

Quando seu ambiente contém sites com diferentes versões de produto (por exemplo, um site XenDesktop 7.18 e um site Citrix Virtual Apps and Desktops 1909), a Citrix recomenda usar o StoreFront para agregar aplicativos e desktops de diferentes versões de produto. Para obter detalhes, consulte a documentação do StoreFront.

Em um ambiente misto, continue usando as versões do Studio e do Director para cada lançamento, mas certifique-se de que as diferentes versões estejam instaladas em máquinas separadas.

Sistemas operacionais anteriores

Digamos que você instalou uma versão anterior de um componente em uma máquina que estava executando uma versão de sistema operacional (SO) suportada. Agora, você deseja usar uma versão mais recente do componente, mas esse SO não é mais suportado para a versão atual do componente.

Por exemplo, suponha que você instalou um VDA de servidor em uma máquina Windows Server 2016. Agora você deseja atualizar esse VDA para a versão atual, mas o Windows Server 2016 não é suportado na versão atual para a qual você está atualizando.

Se você tentar instalar ou atualizar um componente em um sistema operacional que não é mais permitido, uma mensagem de erro será exibida, como "Não pode ser instalado neste sistema operacional".

Essas considerações se aplicam à atualização das versões Current Release e Long Term Service Release. (Não afeta a aplicação de CUs a uma versão LTSR.)

Siga os links para saber quais SOs são suportados:

- Citrix Virtual Apps and Desktops (Versão Atual):
  - Delivery Controller, Studio, Director, VDAs, Universal Print Server
  - Federated Authentication Service

  - Para StoreFront, Self-Service Password Reset e Session Recording, consulte o artigo de requisitos do sistema para a versão atual.

- Para LTSRs, consulte as listas de componentes para sua versão LTSR e CU. (Selecione sua versão LTSR na página principal de documentação do produto Citrix Virtual Apps and Desktops.)

Sistemas operacionais inválidos

A tabela a seguir lista os sistemas operacionais anteriores que não são válidos para instalar/atualizar componentes na versão atual. Ela indica a versão mais recente do componente válida suportada para cada SO listado e a versão do componente quando a instalação e a atualização se tornaram inválidas.

Os sistemas operacionais na tabela incluem service packs e atualizações.

SISTEMA OPERACIONAL	COMPONENTE/ RECURSO	VERSÃO VÁLIDA MAIS RECENTE	INSTALAÇÃO/ ATUALIZAÇÃO NÃO É POSSÍVEL A PARTIR DA VERSÃO
Windows 7 e Windows 8	VDA	7.15 LTSR	7.16
Windows 7 e Windows 8	Outros componentes do instalador	7.17	7.18
Versões do Windows 10 anteriores a 1607	VDA	7.15 LTSR	7.16
Versão do Windows 10 x86	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Outros componentes do instalador	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16

SISTEMA OPERACIONAL	COMPONENTE/ RECURSO	VERSÃO VÁLIDA MAIS RECENTE	INSTALAÇÃO/ ATUALIZAÇÃO NÃO É POSSÍVEL A PARTIR DA VERSÃO
Windows Server 2012	Outros componentes do instalador	7.17	7.18
Windows Server 2012 R2	Outros componentes do instalador *	1912 LTSR	2003
Windows Server 2012 R2	VDI de Servidor	7.15 LTSR	7.16
Windows Server 2016	VDI de Servidor	7.15 LTSR	7.16

Windows XP e Windows Vista não são válidos para nenhum componente ou tecnologia 7.x.

* Aplica-se a Delivery Controller, Studio, Director e VDAs.

O que você pode fazer

Você tem opções. Você pode:

- Continuar com o SO atual
- Reimagear ou atualizar a máquina
- Adicionar novas máquinas e depois remover as máquinas antigas(#add-new-machines-and-then-remove-old-machines)

Continuar com o SO atual

Esses métodos são viáveis para VDAs. Se você quiser continuar usando máquinas com o SO anterior, pode escolher uma das seguintes opções:

- Continuar usando a versão do componente instalada.
- Baixe a versão mais recente válida do componente e, em seguida, atualize o componente para essa versão. (Isso pressupõe que a versão mais recente válida do componente ainda não esteja instalada.)

Por exemplo, você tem um VDA 7.14 em uma máquina Windows 7 SP1. A versão VDA válida mais recente em máquinas com SO Windows 7 é XenApp e XenDesktop 7.15 LTSR. Você pode

continuar usando o 7.14 ou baixar um VDA 7.15 LTSR e, em seguida, atualizar seu VDA para essa versão. Essas versões VDA anteriores funcionam em implantações que contêm Delivery Controllers com versões mais recentes. Por exemplo, um VDA 7.15 LTSR pode se conectar a um Citrix Virtual Apps and Desktops 7 1808 Controller.

Reimagear ou atualizar a máquina

Esses métodos são viáveis para VDAs e outras máquinas que não possuem componentes principais (como Delivery Controllers) instalados. Escolha uma das seguintes opções:

- Depois de desativar a máquina (ativando o modo de manutenção e permitindo que todas as sessões sejam encerradas), você pode reimaginá-la para uma versão de SO Windows compatível e, em seguida, instalar a versão mais recente do componente.
- Para atualizar o SO em uma máquina VDA sem reimaginá-la, você deve primeiro instalar a versão do VDA compatível com o SO para o qual você está atualizando ou atualizar o VDA após a atualização do SO. Caso contrário, o software Citrix não será compatível. Você pode atualizar para as seguintes versões mínimas de SO ao realizar uma atualização in-loco sem desinstalar o VDA:
  - Windows 11 com Atualização Cumulativa de 2023-07 para Windows 11 (KB5028185) ou posterior instalado (compilação 22621.1992 ou posterior).
  - Windows 10 com Atualização Dinâmica de 2023-07 para Windows 10 (KB5028311) instalado.
- Se a versão do Windows para a qual você planeja atualizar não estiver alinhada com a diretriz mencionada, você deve desinstalar o VDA antes de atualizar o SO e, em seguida, instalar uma versão VDA compatível após a conclusão da atualização do SO.

Adicionar novas máquinas e depois remover as máquinas antigas

Este método é viável se você precisar atualizar o SO em máquinas que contêm um Delivery Controller™ ou outro componente principal.

A Citrix recomenda que todos os Controllers em um site tenham o mesmo SO. A seguinte sequência de atualização minimiza o intervalo em que diferentes Controllers têm SOs diferentes.

1. Crie um snapshot de todos os Delivery Controllers no site e, em seguida, faça backup do banco de dados do site.
2. Instale novos Delivery Controllers em servidores limpos com sistemas operacionais compatíveis.
3. Adicione os novos Controllers ao site.

4. Remova os Controllers que estão sendo executados em sistemas operacionais que não são válidos para a versão atual. Siga as recomendações para remover Controllers em Delivery Controllers.

Preparação

Antes de iniciar uma atualização, revise as seguintes informações e conclua as tarefas necessárias.

> **Observação:**
>
> Embora a atualização de VDAs ocorra mais tarde na sequência de atualização, é uma boa ideia escolher um instalador e revisar o procedimento antes de iniciar a atualização, para que você saiba o que esperar.

Escolha um instalador e interface

Use o instalador completo do produto a partir da ISO do produto para atualizar componentes. Você pode atualizar VDAs usando o instalador completo do produto ou um dos instaladores VDA autônomos. Todos os instaladores oferecem interfaces gráficas e de linha de comando.

Para obter mais informações, consulte Instaladores.

Especificidades da instalação: Depois de concluir qualquer trabalho de preparação e estiver pronto para iniciar o instalador, o artigo de instalação mostra o que você verá (se estiver usando a interface gráfica) ou o que digitar (se estiver usando a interface de linha de comando).

- Instalar/atualizar componentes principais usando a interface gráfica
- Instalar/atualizar componentes principais usando a linha de comando
- Instalar/atualizar VDAs usando a interface gráfica
- Instalar/atualizar VDAs usando a linha de comando

Se você instalou originalmente um VDA de sessão única com o instalador `VDAWorkstationCoreSetup.exe`, a Citrix recomenda usar esse instalador para atualizá-lo. Se você usar o instalador VDA de produto completo ou o instalador `VDAWorkstationSetup.exe` para atualizar o VDA, os componentes que foram originalmente excluídos podem ser instalados, a menos que você os omita/exclua expressamente da atualização.

Ao atualizar um VDA para a versão atual, uma reinicialização da máquina ocorre durante o processo de atualização. (Este requisito começou com a versão 7.17.) Isso não pode ser evitado. A atualização é retomada automaticamente após a reinicialização (a menos que você especifique `/noresume` na linha de comando).

Ações do banco de dados

Faça backup dos bancos de dados de site, monitoramento e registro de configuração. Siga as instruções em CTX135207. Se algum problema for descoberto após a atualização, você poderá restaurar o backup.

Para obter informações sobre como atualizar versões do SQL Server que não são mais suportadas, consulte Verificação de versão do SQL Server. (Isso se refere ao SQL Server usado para os bancos de dados de site, monitor e registro de configuração.)

O Microsoft SQL Server Express LocalDB é instalado automaticamente, para uso com o Local Host Cache. Se você precisar substituir uma versão anterior, a nova versão deve ser o SQL Server Express LocalDB 2019. Para obter detalhes sobre como substituir o SQL Server Express LocalDB pela nova versão depois de atualizar os componentes e o site, consulte Substituir SQL Server Express LocalDB.

Certifique-se de que seu licenciamento Citrix esteja atualizado

Para uma visão abrangente do gerenciamento de licenciamento Citrix, consulte Ativar, atualizar e gerenciar licenças Citrix.

Você pode usar o instalador completo do produto para atualizar o License Server. Ou, você pode baixar e atualizar os componentes da licença separadamente. Consulte Atualizar.

Antes de atualizar, certifique-se de que sua data de Customer Success Services / Software Maintenance / Subscription Advantage seja válida para a nova versão do produto. A data deve ser pelo menos 15/11/2021.

Certifique-se de que seu Citrix License Server seja compatível

Certifique-se de que seu Citrix License Server seja compatível com a nova versão. Existem duas maneiras de fazer isso:

- Antes de atualizar quaisquer outros componentes Citrix, execute o instalador `XenDesktopServerSetup.exe` do layout ISO na máquina que contém um Delivery Controller. Se houver algum problema de incompatibilidade, o instalador o relatará com as etapas recomendadas para resolver os problemas.

- No diretório `XenDesktop Setup` na mídia de instalação, execute o comando: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. A exibição indica se o License Server é compatível. Se o License Server for incompatível, atualize o servidor de licenças.

Faça backup de quaisquer modificações do StoreFront

Antes de iniciar uma atualização, se você modificou arquivos em `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como *default.ica* e *usernamepassword.tfrm*, faça backup deles para cada loja. Após a atualização, você pode restaurá-los para restabelecer suas modificações.

Fechar aplicativos e consoles

Antes de iniciar uma atualização, feche todos os programas que possam causar bloqueios de arquivo, incluindo consoles de administração e sessões do PowerShell.

Reiniciar a máquina garante que quaisquer bloqueios de arquivo sejam liberados e que não haja atualizações pendentes do Windows.

Antes de iniciar uma atualização, pare e desative quaisquer serviços de agente de monitoramento de terceiros.

Certifique-se de ter as permissões adequadas

Além de ser um usuário de domínio, você deve ser um administrador local nas máquinas onde está atualizando os componentes do produto.

O banco de dados do site e o site podem ser atualizados automaticamente ou manualmente. Para uma atualização automática do banco de dados, as permissões do usuário do Studio devem incluir a capacidade de atualizar o esquema do banco de dados do SQL Server (por exemplo, a função de banco de dados `db_securityadmin` ou `db_owner`). Para obter detalhes, consulte Bancos de dados.

Se o usuário do Studio não tiver essas permissões, iniciar uma atualização manual do banco de dados gera scripts. O usuário do Studio executa alguns dos scripts a partir do Studio. O administrador do banco de dados executa outros scripts, usando uma ferramenta como o SQL Server Management Studio.

Outras tarefas de preparação

- Faça backup dos modelos e atualize os hipervisores, se necessário

- Conclua quaisquer outras tarefas de preparação ditadas pelo seu plano de continuidade de negócios.

Testes preliminares do site

Ao atualizar os Delivery Controllers e um site, testes preliminares do site são executados antes do início da atualização real. Esses testes verificam:

- O banco de dados do site pode ser acessado e foi feito backup
- As conexões com os serviços essenciais da Citrix estão funcionando corretamente
- O endereço do Citrix License Server está disponível
- O banco de dados de log de configuração pode ser acessado
- Certifique-se de ter a Licença de Direitos Híbridos se quiser adicionar conexões de host de nuvem pública (por exemplo, AWS). Caso contrário, o teste preliminar do site pausa ou para, e uma mensagem explicativa aparece.

Após a execução dos testes, você pode visualizar um relatório dos resultados. Em seguida, você pode corrigir quaisquer problemas detectados e executar os testes novamente. A falha em executar os testes preliminares do site e, em seguida, resolver quaisquer problemas pode afetar o funcionamento do seu site.

O relatório contendo os resultados do teste é um arquivo HTML (`PreliminarySiteTestResult.html`) no mesmo diretório dos logs de instalação. Esse arquivo é criado se não existir. Se o arquivo existir, seu conteúdo será sobrescrito.

Executar os testes

- Ao usar a interface gráfica do instalador para atualizar, o assistente inclui uma página onde você pode iniciar os testes e, em seguida, exibir o relatório. Após a execução dos testes e a visualização do relatório e a resolução de quaisquer problemas encontrados, você pode executar os testes novamente. Quando os testes forem concluídos com sucesso, clique em Avançar para continuar com o assistente.
- Ao usar a interface de linha de comando para atualizar, os testes são executados automaticamente. Por padrão, se um teste falhar, a atualização não será realizada. Depois de visualizar o relatório e resolver os problemas, execute o comando novamente.

A Citrix recomenda sempre executar os testes preliminares do site e, em seguida, resolver quaisquer problemas antes de continuar a atualização do Controller e do site. O benefício

potencial vale bem os poucos momentos para executar os testes. No entanto, você pode substituir esta ação recomendada.

- Ao atualizar com a interface gráfica, você pode optar por pular os testes e continuar com a atualização.
- Ao atualizar pela linha de comando, você não pode pular os testes. Por padrão, um teste de site com falha faz com que o instalador falhe, sem realizar a atualização. Geralmente, se você incluir a opção `/ignore_site_test_failure`, quaisquer falhas de teste são ignoradas e a atualização prossegue. (Consulte Verificação da versão do SQL Server para exceções.)

Ao atualizar vários Controllers

Ao iniciar uma atualização em um Controller e, em seguida, iniciar uma atualização de outro Controller no mesmo site (antes que a primeira atualização seja concluída):

- Se os testes preliminares do site forem concluídos no primeiro Controller, a página de testes preliminares do site não aparecerá no assistente no outro Controller.
- Se os testes no primeiro Controller estiverem em andamento quando você iniciar a atualização no outro Controller, a página de testes do site aparecerá no assistente no outro Controller. No entanto, se os testes no primeiro Controller terminarem, apenas os resultados dos testes do primeiro Controller serão retidos.

Falhas de teste não relacionadas à integridade do site

- Se os testes preliminares do site falharem devido a memória insuficiente, disponibilize mais memória e execute os testes novamente.
- Se você tiver permissão para atualizar, mas não para executar testes de site, os testes preliminares do site falharão. Para resolver isso, execute o instalador novamente com uma conta de usuário que tenha permissão para executar os testes.

Verificação da versão do SQL Server

Uma implantação bem-sucedida do Citrix Virtual Apps and Desktops requer uma versão compatível do Microsoft SQL Server para os bancos de dados de site, monitoramento e registro de configuração. A atualização de uma implantação Citrix com uma versão do SQL Server que não é mais compatível pode resultar em problemas de funcionalidade, e o site não será compatível.

Para saber quais versões do SQL Server são compatíveis com a versão do Citrix para a qual você está atualizando, consulte o artigo Requisitos do sistema para essa versão.

Ao atualizar um Controller, o instalador Citrix verifica a versão do SQL Server atualmente instalada usada para os bancos de dados de site, monitoramento e registro de configuração.

- Se a verificação determinar que a versão do SQL Server atualmente instalada não é uma versão compatível na versão do Citrix para a qual você está atualizando:
  - Interface gráfica: A atualização é interrompida com uma mensagem. Clique em **Entendi** e depois em **Cancelar** para fechar o instalador Citrix. (Você não pode continuar com a atualização.)
  - Interface de linha de comando: o comando falha (mesmo que você tenha incluído a opção `/ignore_db_check_failure` com o comando).

  Atualize a versão do SQL Server e, em seguida, inicie a atualização do Citrix novamente.
- Se a verificação não conseguir determinar qual versão do SQL Server está atualmente instalada, verifique se a sua versão atualmente instalada é compatível com a versão para a qual você está atualizando (Requisitos do sistema).
  - Interface gráfica: A atualização é interrompida com uma mensagem.
    - Se a versão do SQL Server atualmente instalada for compatível, clique em **Entendi** para fechar a mensagem e, em seguida, clique em **Avançar** para continuar com a atualização do Citrix.
    - Se a versão do SQL Server atualmente instalada não for suportada, clique em **Entendi** para fechar a mensagem e, em seguida, clique em **Cancelar** para encerrar a atualização do Citrix. Atualize seu SQL Server para uma versão suportada e, em seguida, inicie a atualização do Citrix novamente.
  - Interface de linha de comando: O comando falha com uma mensagem. Após fechar a mensagem:
    - Se a versão do SQL Server atualmente instalada for suportada, execute o comando novamente com a opção `/ignore_db_check_failure`.
    - Se a versão do SQL Server atualmente instalada não for suportada, atualize seu SQL Server para uma versão suportada. Execute o comando novamente para iniciar a atualização do Citrix.

Atualizando o SQL Server

Se você configurar novos servidores SQL Server e migrar o banco de dados do site, as cadeias de conexão deverão ser atualizadas.

Se o site atualmente usa SQL Server Express para o banco de dados do site (que o Citrix instalou automaticamente durante a criação do site):

1. Instale a versão mais recente do SQL Server Express.
2. Desanexe o banco de dados.
3. Anexe o banco de dados ao novo SQL Server Express.
4. Migre as cadeias de conexão.

Para obter mais informações, consulte Configurando cadeias de conexão e a documentação do produto Microsoft SQL Server.

Substituir SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o Local Host Cache usa de forma autônoma. O Local Host Cache não requer nenhum componente do SQL Server Express além do SQL Server Express LocalDB.

O Citrix não atualiza automaticamente o SQL Server Express LocalDB. Para atualizar a versão do SQL Server Express LocalDB, siga as orientações nesta seção.

- Ao atualizar os Delivery Controllers para o Citrix Virtual Apps and Desktops versão 2203 LTSR ou versões posteriores, a versão suportada é SQL Server Express LocalDB 2019 ou SQL Server Express LocalDB 2022.

O que você precisa:

- A mídia de instalação do Citrix Virtual Apps and Desktops.
- A ferramenta PsExec da caixa de ferramentas do Windows Sysinternals.

Procedimento:

1. Conclua a atualização dos componentes, bancos de dados e site do Citrix Virtual Apps and Desktops. (Essas atualizações de banco de dados afetam os bancos de dados de site, monitoramento e registro de configuração. Elas não afetam o banco de dados Local Host Cache que usa SQL Server Express LocalDB.)
2. Faça logon no Delivery Controller, onde você gostaria de atualizar o SQL Server Express LocalDB.
3. Baixe o PsExec da Microsoft e coloque-o em um local de fácil acesso nesse Delivery Controller, como C:\Temp.

4. Pare o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
5. Abra o Prompt de Comando no Delivery Controller, navegar até o local com o PsExec (exemplo, `C:\Temp`), e então execute o seguinte comando para elevar o prompt de comando com a conta de Serviço de Rede:

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. Execute `whoami` para confirmar que o prompt de comando está sendo executado como a conta de Serviço de Rede. Você deve obter a seguinte saída: `nt authority\networkservice`.
7. Use o prompt de comando para navegar até a instância do SQL LocalDB:
   - Se estiver atualizando do SQL LocalDB 2014:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2017:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - Se estiver atualizando do SQL LocalDB 2019:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. Parar e excluir a instância do SQL LocalDB: `CitrixHA`.

   ```
   SqlLocalDB stop CitrixHA



   SqlLocalDB delete CitrixHA
   ```

9. Remova os seguintes arquivos do Delivery Controller:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. Desinstale seu SQL LocalDB SQL Server Express existente do Delivery Controller usando o recurso nativo do Windows para remover programas.
11. Reinicie o Delivery Controller após a conclusão da desinstalação.
12. Pare o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
13. Monte a mídia de instalação do Citrix Virtual Apps and Desktops no seu Delivery Controller.
14. Instale o SQL Server Express LocalDB 2022 como administrador no Delivery Controller.
    a. Use o arquivo `sqllocaldb.msi` na pasta `Support > SQLLocalDB` da mídia de instalação do Citrix Virtual Apps and Desktops. Por exemplo, se a mídia de instalação estiver montada na letra `E drive`, o arquivo pode ser encontrado em `E:\Support\SQLLocalDB\sqllocaldb.msi`. É necessário reiniciar para concluir a instalação.
    b. O novo SQL LocalDB deve estar em `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`.
15. Inicie o Serviço de Alta Disponibilidade do Citrix no Delivery Controller a partir dos Serviços do Sistema Windows.
16. No Prompt de Comando do Delivery Controller, navegar para `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` e execute `SqlLocalDB i` para confirmar que a instância CitrixHA foi criada. O `CitrixHA` deve ser incluído na lista de instâncias retornadas.

> **Observação:**
>
> Pode levar até 15 minutos para que o banco de dados CitrixHA seja criado após o início do Serviço de Alta Disponibilidade do Citrix.

17. Certifique-se de que os arquivos do banco de dados do Cache de Host Local sejam criados para confirmar que o Serviço de Alta Disponibilidade (broker secundário) pode assumir o controle, se necessário.
    a. No Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
    b. Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.
18. Repita as etapas nos Delivery Controllers restantes.

Suporte a Proxy para o Agente de Atualização do VDA

O Suporte a Proxy para o Agente de Atualização do VDA foi adicionado no VDA 2311.

O Agente de Atualização do VDA do VDA 2311, ou seja, Versão: 7.40, pode reconhecer e enviar tráfego através do Proxy.

O Agente de Atualização do VDA (VUA) suporta Proxy na forma de Hostname:Porta (IP:Porta) e arquivo PAC.

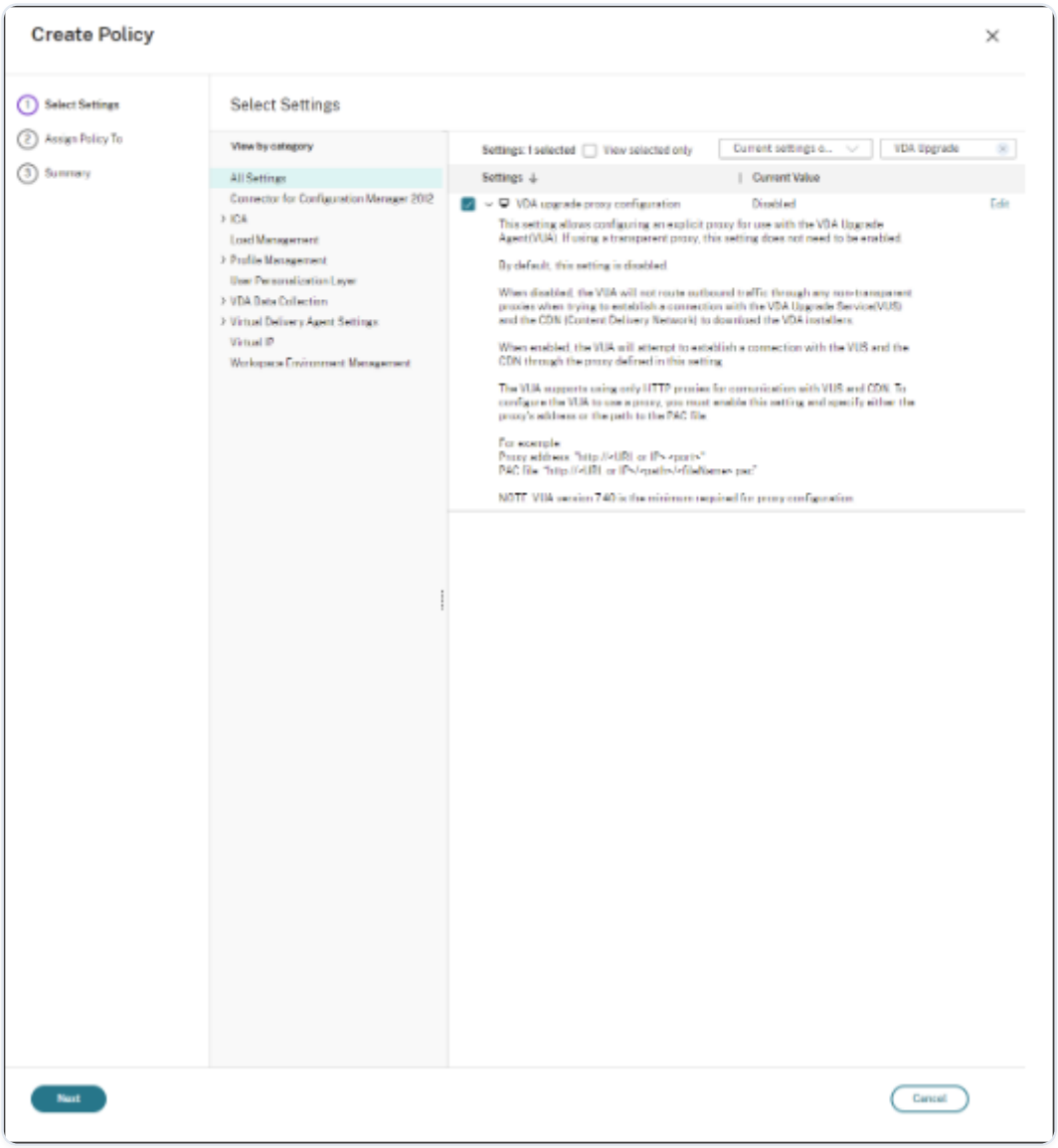
Apenas proxies HTTP são suportados. A descriptografia e inspeção de pacotes não são suportadas.

A autenticação de proxy não é suportada. SOCKS5 não é suportado.

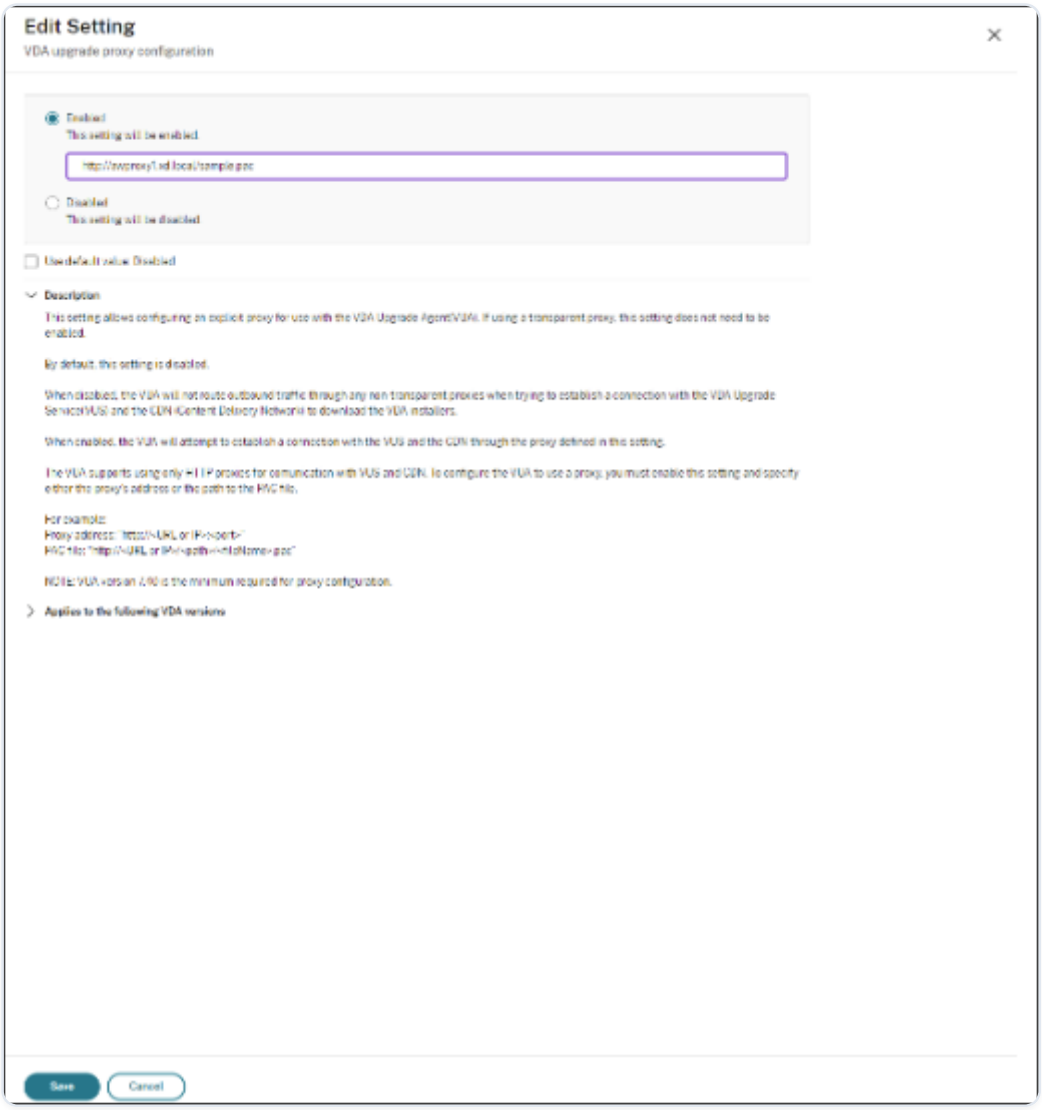
Configurando o Proxy do Agente de Atualização do VDA

O Proxy do Agente de Atualização do VDA pode ser configurado de 2 maneiras:

1. **Configurando a Política do Agente de Atualização do VDA** usando a **Política do Webstudio**.
2. Selecione **configuração de proxy de atualização do VDA** em **Configurações** na página **Criar Política**.



3. Habilite a configuração. Por padrão, a configuração está desabilitada.



4. Configurando o Agente de Atualização do VDA usando a Chave de Registro.

   A Chave de Registro é definida para o Meta-Instalador durante a Instalação do VDA.

   Registro:

   Chave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

   Tipo de valor: String

   Nome do valor: ProxySettings

   Dados do valor: Endereço do proxy ou caminho para o arquivo pac.

   Por exemplo:

   a. Endereço do proxy: `http://<URL or IP>:<port>`
   b. Arquivo Pac: `http://<URL or IP>/<path/<filename>.pac`

Fazer backup ou migrar sua configuração

Este recurso ajuda você a fazer backup de suas configurações DaaS. Os backups facilitam o processo de migração das configurações de um site em nuvem para outro. Também facilita a recuperação imediata de um site em caso de emergências. Você pode usar os seguintes métodos para fazer backups:

1. Backup + Restauração
    a. Integrado com o WebStudio.
2. Ferramenta de Configuração Automatizada (ACT)
    a. Ferramenta baseada em Powershell. Instale a ferramenta para usá-la.

Os backups podem ser usados para:

1. Restauração
2. Migração

A Citrix® recomenda as seguintes ferramentas para os cenários descritos.

Backup

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
DaaS	Backups sob demanda e agendados	Backup + Restauração	A Citrix mantém o backup e o usuário pode baixá-lo se necessário	Backup + Restauração no Studio
No local	Backups sob demanda	ACT	O usuário mantém o backup	Backup e Restauração usando a Ferramenta de Configuração Automatizada

Migração

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
No local para a nuvem	Migrar um site local para DaaS	ACT		Migrar do local para a nuvem
	Consolidar vários sites locais em um site DaaS	ACT	Fusão de sites	Mesclar vários sites locais em um único site na nuvem
No local para no local	Migrar um site local para outro site local	ACT		Guia de POC:Ferramenta de Configuração Automatizada - Migração local para local
	Consolidar vários sites locais em outro site local	ACT	Fusão de sites	Guia de POC:Ferramenta de Configuração Automatizada Migração local para local
				Mesclar vários sites locais em um único site na nuvem
Nuvem para nuvem	Migrar um site DaaS para outro site DaaS	ACT		Migrar da nuvem para a nuvem(/pt-br/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
				migrating-your-configuration)
Consolidar vários sites DaaS em um único site DaaS	ACT	Fusão de sites		Migrar da nuvem para a nuvem(/pt-br/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration)
				Migrar vários sites locais para um único site na nuvem(/pt-br/citrix-daas/migrate/multi-site-merge.html)

Seguro

O Citrix Virtual Apps and Desktops™ oferece uma solução segura por design que permite adaptar seu ambiente às suas necessidades de segurança.

Uma preocupação de segurança que a TI enfrenta com trabalhadores móveis é a perda ou roubo de dados. Ao hospedar aplicativos e desktops, o Citrix Virtual Apps and Desktops separa com segurança dados sensíveis e propriedade intelectual de dispositivos de endpoint, mantendo todos os dados em um data center. Quando as políticas são habilitadas para permitir a transferência de dados, todos os dados são criptografados.

Os data centers do Citrix Virtual Apps and Desktops também facilitam a resposta a incidentes com um serviço centralizado de monitoramento e gerenciamento. O Director permite que a TI monitore e analise os dados que estão sendo acessados na rede, e o Studio permite que a TI corrija e remedie a maioria das vulnerabilidades no data center, em vez de resolver os problemas localmente em cada dispositivo do usuário final.

O Citrix Virtual Apps and Desktops também simplifica auditorias e conformidade regulatória, pois os investigadores podem usar um registro de auditoria centralizado para determinar quem acessou quais aplicativos e dados. O Director coleta dados históricos sobre atualizações do sistema e uso de dados do usuário acessando o Log de Configuração e a API OData.

A administração delegada permite configurar funções de administrador para controlar o acesso ao Citrix Virtual Apps and Desktops em um nível granular. Isso permite flexibilidade em sua organização para conceder a certos administradores acesso total a tarefas, operações e escopos, enquanto outros administradores têm acesso limitado.

O Citrix Virtual Apps and Desktops oferece aos administradores controle granular sobre os usuários, aplicando políticas em diferentes níveis da rede - do nível local ao nível da Unidade Organizacional. Esse controle de políticas determina se um usuário, dispositivo ou grupos de usuários e dispositivos podem se conectar, imprimir, copiar/colar ou mapear unidades locais, o que pode minimizar preocupações de segurança com trabalhadores temporários de terceiros. Os administradores também podem usar o recurso Bloqueio de Área de Trabalho para que os usuários finais possam usar apenas a área de trabalho virtual, impedindo qualquer acesso ao sistema operacional local do dispositivo do usuário final.

Os administradores podem aumentar a segurança no Citrix Virtual Apps ou Citrix Virtual Desktops configurando o Site para usar o protocolo Transport Layer Security (TLS) do Controller ou entre usuários finais e Virtual Delivery Agents (VDA). O protocolo também pode ser habilitado em um Site para fornecer autenticação de servidor, criptografia de fluxo de dados e verificações de integridade de mensagens para uma conexão TCP/IP.

O Citrix Virtual Apps and Desktops também oferece suporte à autenticação multifator para Windows ou um aplicativo específico. A autenticação multifator também pode ser usada para gerenciar todos os recursos entregues pelo Citrix Virtual Apps and Desktops. Esses métodos incluem:

- Tokens
- Cartões inteligentes
- RADIUS
- Kerberos
- Biometria

O Citrix Virtual Desktops pode ser integrado com muitas soluções de segurança de terceiros, desde gerenciamento de identidade até software antivírus. Uma lista de produtos suportados pode ser encontrada em `<http://www.citrix.com/ready>`.

Algumas versões do Citrix Virtual Apps and Desktops são certificadas para o padrão Common Criteria. Para obter uma lista desses padrões, acesse `<https://www.commoncriteriaportal.org/cc/>`.

Serviço de Autenticação Federada

O Citrix Federated Authentication Service (FAS) permite o logon único (SSO) em desktops e aplicativos virtuais Citrix em ambientes onde os usuários autenticar por meio de provedores de identidade modernos, como SAML ou OpenID Connect (OIDC), que não fornecem uma senha do Windows, garantindo acesso contínuo a hosts de sessão unidos a um domínio do Active Directory.

Para obter mais informações sobre como proteger sua implantação com o Serviço de Autenticação Federada, consulte a documentação Federated Authentication Service em seu próprio documento.

Autenticação FIDO2

Autorização local e autenticação virtual usando FIDO2 e WebAuthn

Os usuários podem autenticar em aplicativos que utilizam FIDO2 ou WebAuthn em sua sessão virtual usando chaves de segurança FIDO2 e dispositivos biométricos integrados com TPM 2.0 e Windows Hello.

Para obter mais informações sobre FIDO2, consulte FIDO2: WebAuthn & CTAP.

Para obter informações sobre como usar este recurso, consulte Redirecionamento FIDO2.

> **NOTA**
>
> Observe que este recurso não oferece suporte ao login na sessão virtual usando WebAuthn ou FIDO2. Este recurso permite apenas o uso desses métodos de autenticação em aplicativos dentro da sessão virtual.

> Este recurso não é suportado em cenários de double-hop.

Matriz de suporte

SISTEMA OPERACIONAL DO HOST DA SESSÃO	AUTENTICAÇÃO DE APLICATIVO WEB	AUTENTICAÇÃO DE APLICATIVO UWP
Windows Server 2016	Suportado via redirecionamento USB	Não suportado
Windows Server 2019	Suportado	Não suportado
Windows Server 2022	Compatível	Compatível
Windows 10	Compatível	Compatível
Windows 11	Compatível	Compatível

Para informações adicionais, revise os requisitos abaixo.

Autenticação de aplicativo web

Requisitos

A seguir estão os requisitos para usar a autenticação FIDO2 e WebAuthn com aplicativos web:

Plano de controle Citrix®

- Citrix Virtual Apps and Desktops™ 2009 ou posterior

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2019 ou posterior
- VDA
  - Windows: versão 2009 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux
- Aplicativo Workspace
  - Windows: versão 2009.1 ou posterior
  - Linux: 2303 ou posterior

Requisitos do navegador web

- Navegadores de 32 bits e 64 bits

Métodos de autenticação suportados

- Chave de Segurança FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial

    - Leitor de impressão digital
  - WebAuthn

Autenticação de aplicativo UWP

Com o lançamento do Citrix Virtual Apps and Desktops 2112, a Citrix oferece suporte à autenticação WebAuthn e FIDO2 em aplicativos UWP.

Aplicativos como Microsoft Teams, Microsoft Outlook para Office 365 e OneDrive usam um aplicativo UWP para autenticação como um link para o Azure Active Directory. A Citrix agora oferece suporte ao uso do FIDO2 para autenticar esses aplicativos.

Requisitos

A seguir estão os requisitos para usar a autenticação FIDO2 e WebAuthn com aplicativos UWP:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 2112 ou posterior

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2022 ou posterior
- VDA
  - Windows: versão 2112 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux
- Aplicativo Workspace
  - Windows: versão 2009.1 ou posterior
  - Linux: 2303 ou posterior

REQUISITOS DO APLICATIVO UWP

- Aplicativos de 32 e 64 bits

Métodos de autenticação suportados

- Chave de Segurança FIDO2
- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial
    - Leitor de impressão digital
  - WebAuthn

Observação:

Em cenários onde o redirecionamento FIDO2 não está disponível porque o recurso não é suportado pelo cliente, VDA ou sistema operacional, as chaves FIDO2 baseadas em USB podem ser redirecionadas usando o redirecionamento USB. Também é possível usar o redirecionamento USB para redirecionar chaves FIDO2 baseadas em USB em cenários onde o redirecionamento FIDO2 está disponível. Neste caso, você deve desabilitar o redirecionamento FIDO2 e configurar as regras de redirecionamento USB apropriadas. Consulte a documentação de regras de dispositivo de redirecionamento USB para obter detalhes sobre como configurar chaves FIDO2 usando regras de redirecionamento USB.

Configuração avançada para aplicativos baseados em msedgewebview2.exe

Observação:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> Para empresas que possuem aplicativos web baseados em msedgewebview2.exe, valores adicionais de registro precisam ser adicionados no VDA para que o redirecionamento FIDO2 funcione dentro das sessões HDX -

Anexe o caminho completo do msedgewebview2.exe no valor de registro AllowedProcesses:

- Chave: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- Nome do valor: AllowedProcesses
- Tipo de valor: REG_MULTISZ
- Dados do valor: `<add full path of the msedgewebview2.exe here >`

Para aplicativos de 64 bits, os seguintes valores precisam ser definidos:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: FilePathName
- Tipo de valor: REG_SZ
- Dados do valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: Flag
- Tipo de valor: DWORD
- Dados do valor: 00000002

Para aplicativos de 32 bits, os seguintes valores precisam ser definidos:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\
- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: FilePathName
- Tipo de valor: REG_SZ
- Dados do valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nome do valor: Flag
- Tipo de valor: DWORD
- Dados do valor: 00000002

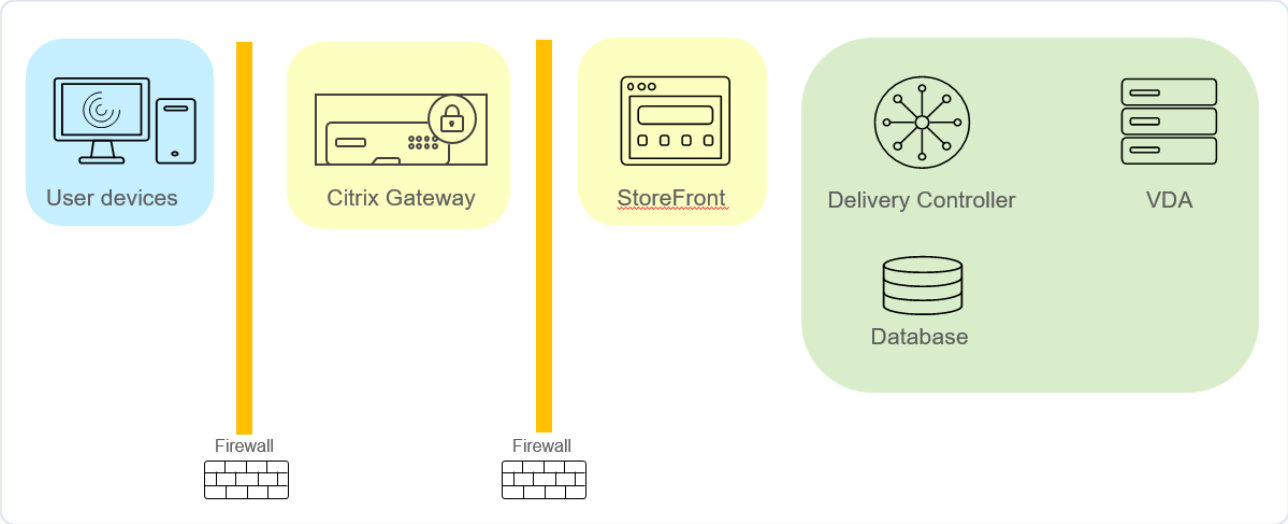
Reinicie o VDA depois de definir os valores do registro para que o redirecionamento FIDO2 seja habilitado para aplicativos baseados em msedgewebview2.exe.

Integrar Citrix Virtual Apps and Desktops™ com Citrix Gateway

Servidores StoreFront™ são implantados e configurados para gerenciar o acesso a recursos e dados publicados. Para acesso remoto, é recomendável adicionar o Citrix Gateway na frente do StoreFront.

> **Observação:**
>
> Para etapas de configuração detalhadas sobre como integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway, consulte a documentação do StoreFront.

> O diagrama a seguir ilustra um exemplo de uma implantação simplificada do Citrix que inclui o Citrix Gateway. O Citrix Gateway se comunica com o StoreFront para proteger aplicativos e dados entregues pelo Citrix Virtual Apps and Desktops. Os dispositivos do usuário executam o aplicativo Citrix Workspace™ para criar uma conexão segura e acessar seus aplicativos, desktops e arquivos.



Os usuários fazem logon e autenticar usando o Citrix Gateway. O Citrix Gateway é implantado e protegido na DMZ. A autenticação de dois fatores é configurada. Com base nas credenciais do usuário, os usuários recebem os recursos e aplicativos relevantes. Aplicativos e dados estão em servidores apropriados (não mostrados no diagrama). Servidores separados são usados para aplicativos e dados sensíveis à segurança.

Considerações de segurança e melhores práticas

> **Observação:**

> Sua organização pode precisar atender a padrões de segurança específicos para satisfazer requisitos regulatórios. Este documento não aborda este assunto, pois tais padrões de segurança mudam com o tempo. Para informações atualizadas sobre padrões de segurança e produtos Citrix, consulte Citrix Trust Center.

Firewalls

Proteja todas as máquinas em seu ambiente com firewalls de perímetro, inclusive nas fronteiras de enclave, conforme apropriado.

Todas as máquinas em seu ambiente devem ser protegidas por um firewall pessoal. Ao instalar os componentes principais e os VDAs, você pode optar por ter as portas necessárias para a comunicação de componentes e recursos abertas automaticamente se o Serviço de Firewall do Windows for detectado (mesmo que o firewall não esteja ativado). Você também pode optar por configurar manualmente essas portas de firewall. Se você usar um firewall diferente, deverá

configurá-lo manualmente. Para obter mais informações sobre as portas necessárias, consulte Tech Paper: Communication Ports Used by Citrix Technologies.

Se você estiver migrando um ambiente convencional para esta versão, pode ser necessário reposicionar um firewall de perímetro existente ou adicionar novos firewalls de perímetro. Por exemplo, suponha que haja um firewall de perímetro entre um cliente convencional e um servidor de banco de dados no data center. Quando esta versão é usada, esse firewall de perímetro deve ser colocado de forma que o desktop virtual e o dispositivo do usuário estejam de um lado, e os servidores de banco de dados e os Delivery Controllers no data center estejam do outro lado. Portanto, considere criar um enclave dentro do seu data center para conter os servidores de banco de dados e os Controllers. Considere também ter proteção entre o dispositivo do usuário e o desktop virtual.

> **Observação:**
>
> As portas TCP 1494 e 2598 são usadas para ICA e CGP e, portanto, provavelmente estarão abertas nos firewalls para que os usuários fora do data center possam acessá-las. A Citrix recomenda que você não use essas portas para qualquer outra coisa, para evitar a possibilidade de deixar inadvertidamente interfaces administrativas abertas a ataques. As portas 1494 e 2598 estão oficialmente registradas na Internet Assigned Number Authority (http://www.iana.org/).

Comunicações seguras com o Delivery Controller™

Criptografando a comunicação usando HTTPS

O StoreFront e o gateway NetScaler se comunicam com o serviço XML em execução no delivery controller via HTTP ou HTTPS. Dependendo da configuração, os VDAs podem se comunicar com o delivery controller usando WebSocket. Recomenda-se que você ative o HTTPS e desative o HTTP. Isso exige que você tenha ativado Enable HTTPS on Delivery Controllers.

- Para configurar o StoreFront para conectar usando HTTPS, consulte Add resource feeds for Citrix Desktops as a Service e Add Citrix Gateway appliance.
- Para configurar um gateway NetScaler para conectar ao Delivery Controller usando HTTPS, consulte Configuring the Secure Ticket Authority on NetScaler Gateway.

Alternativamente, você pode configurar o Windows para proteger a comunicação entre os servidores usando IPSec.

Chaves de Segurança

Você pode usar Security Keys para garantir que apenas servidores StoreFront e NetScaler autorizados possam se conectar ao DaaS via conectores de nuvem. Isso é especialmente importante se você ativou a confiança XML.

Confiança XML

Por padrão, quando o StoreFront se conecta ao delivery controller para ações como enumeração e inicialização, o StoreFront deve passar as credenciais do Active Directory do usuário para que o DaaS possa autenticar o usuário e verificar a associação do usuário ao grupo. No entanto, ao usar outros métodos de autenticação, como passagem de domínio, cartões inteligentes ou SAML, o StoreFront não possui a senha do Active Directory. Neste caso, você deve habilitar a "Confiança XML". Com a confiança XML ativada, o CVAD permite que o StoreFront execute ações em nome de um usuário, como enumerar e iniciar aplicativos, sem validar a senha do usuário. Antes de habilitar a confiança XML, use Security Keys ou outro mecanismo, como firewalls ou IPsec, para garantir que apenas servidores StoreFront confiáveis possam se conectar aos Delivery Controllers.

Use o Citrix Virtual Apps and Desktops PowerShell SDK para verificar, habilitar ou desabilitar a configuração de confiança XML.

- Para verificar o valor atual da configuração de confiança XML, execute `Get-BrokerSite` e inspecione o valor de `TrustRequestsSentToTheXMLServicePort`.
- Para habilitar ou desabilitar a confiança XML, execute `Set-BrokerSite` com o parâmetro `TrustRequestsSentToTheXmlServicePort`.

Comunicação entre VDA e Delivery Controller

Existem dois mecanismos para VDAs se comunicarem com os controladores.

- Windows Communication Foundation

  A proteção em nível de mensagem do Windows Communication Foundation (WCF) protege a comunicação entre o Delivery Controller e o VDA. Isso elimina a necessidade de proteção extra em nível de transporte usando TLS. A porta padrão usada para comunicação entre VDA e Delivery Controller é 80. No entanto, você pode personalizar a porta. Para obter informações, consulte Personalizar um VDA.

  Para obter informações sobre segurança de mensagens no WCF, consulte a documentação da Microsoft Message Security in WCF.

A configuração do WCF usa Kerberos para autenticação mútua entre o Controller e o VDA. A criptografia usa AES no modo CBC com uma chave de 256 bits. A integridade da mensagem usa SHA-1.

De acordo com a Microsoft, os protocolos de segurança usados pelo WCF estão em conformidade com os padrões da OASIS (Organization for the Advancement of Structured Information Standards), incluindo WS-SecurityPolicy 1.2. Além disso, a Microsoft afirma que o WCF suporta todos os conjuntos de algoritmos listados em Security Policy 1.2.

A comunicação entre o Controller e o VDA usa o conjunto de algoritmos basic256, cujos algoritmos são os mencionados acima.

A configuração do WCF usa o protocolo SOAP sobre HTTP juntamente com a criptografia de segurança em nível de mensagem.

- WebSockets

  Este é o substituto moderno para WCF. Ele oferece o benefício de usar apenas a porta TLS 443 para comunicação do VDA para o Delivery Controller. Atualmente, está disponível apenas para máquinas provisionadas por MCS. Para obter mais informações, consulte Comunicação WebSocket entre VDA e Delivery Controller.

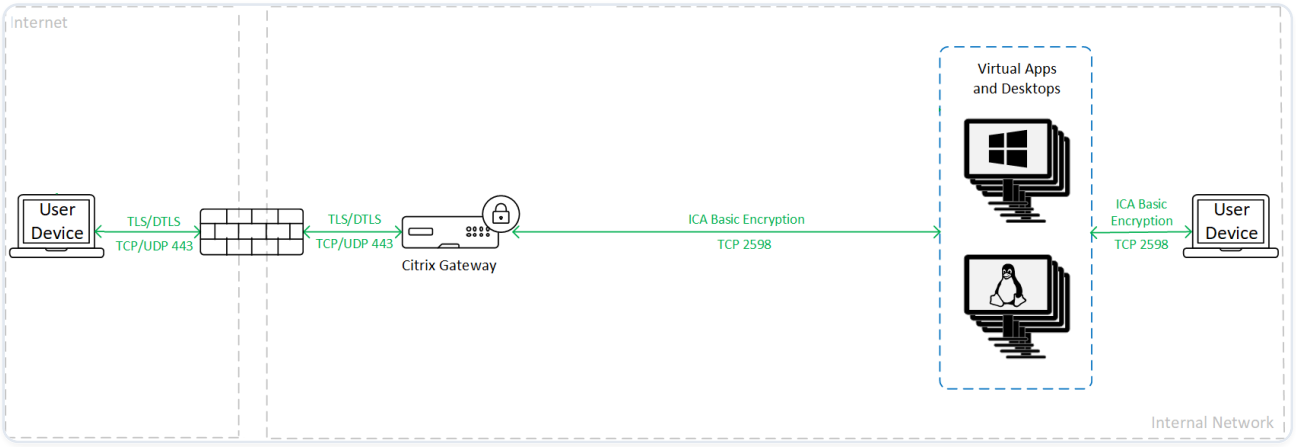
Protegendo as comunicações ICA®

O Citrix CVAD oferece várias opções para proteger o tráfego ICA entre o cliente e o VDA. As opções disponíveis são as seguintes:

- **Criptografia básica:** A configuração padrão.
- **SecureICA:** Permite criptografar dados da sessão usando criptografia RC5 (128 bits).
- **VDA TLS/DTLS:** Permite usar criptografia em nível de rede usando TLS/DTLS.

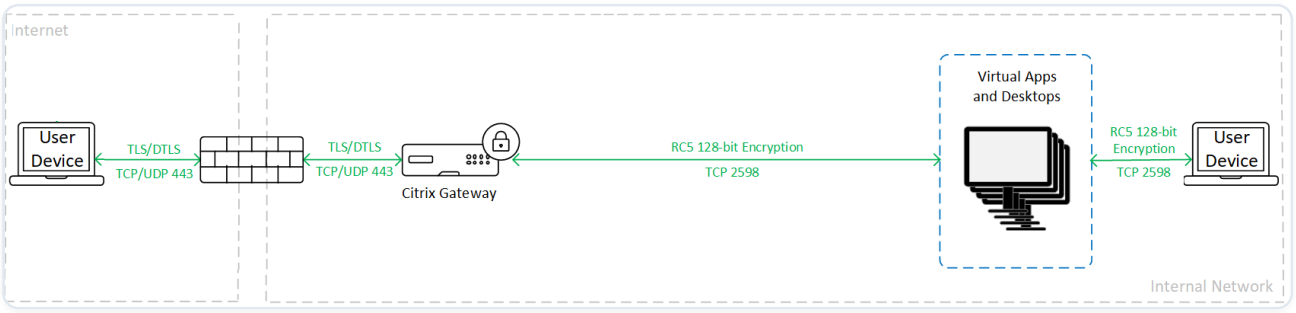
Criptografia básica

Ao usar a criptografia básica, o tráfego é criptografado conforme mostrado no gráfico a seguir.



SecureICA

Ao usar o SecureICA, o tráfego é criptografado conforme mostrado no gráfico a seguir.



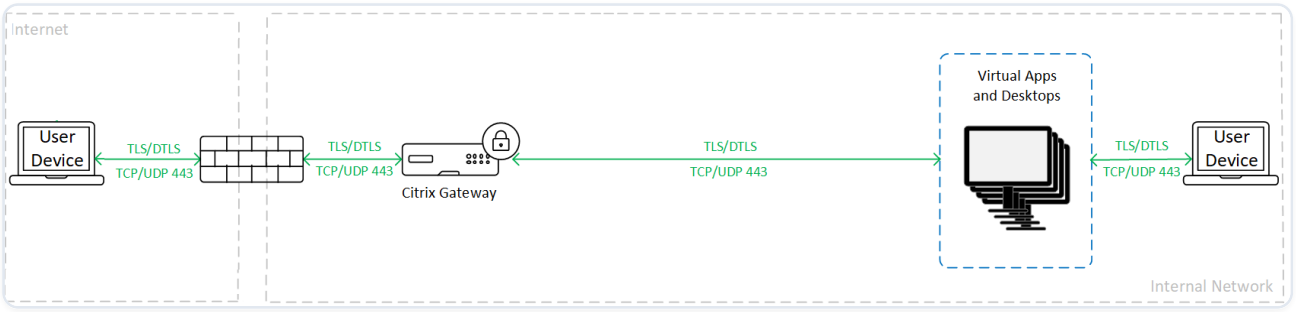
Para obter mais informações, consulte Configurações de política de segurança

> **Nota 1:**
>
> O SecureICA não é compatível ao usar o aplicativo Workspace para HTML5.

> **Nota 2:**
>
> O Citrix SecureICA faz parte do protocolo ICA/HDX, mas não é um protocolo de segurança de rede compatível com padrões como o Transport Layer Security (TLS).

VDA TLS/DTLS

Ao usar a criptografia VDA TLS/DTLS, o tráfego é criptografado conforme mostrado no gráfico a seguir.



Para configurar o VDA TLS/DTLS, consulte Configurações de TLS em VDAs.

Canais virtuais

Use a lista de permissões de canais virtuais para controlar quais canais virtuais não-Citrix são permitidos em seu ambiente.

Comunicações seguras com o servidor de impressão

Você pode habilitar o TLS para conexões baseadas em TCP entre o Virtual Delivery Agent (VDA) e o Universal Print Server. Para obter mais informações, consulte Transport Layer Security (TLS) no Universal Print Server.

Comunicação segura com o banco de dados do site

Para obter informações sobre como habilitar o TLS para o banco de dados do Site, consulte CTX137556.

Segurança da máquina VDA

Recomendações gerais

Certifique-se de que seus VDAs estejam atualizados com as últimas atualizações de segurança do sistema operacional e antivírus.

Segurança de aplicativos

Para evitar que usuários não administradores realizem ações maliciosas, a Citrix recomenda que você configure regras do Windows AppLocker para instaladores, aplicativos, executáveis e scripts no host VDA.

Nomes de arquivo 8.3

Você pode desabilitar nomes de arquivo 8.3 em VDAs. Consulte a documentação do Microsoft fsutil.

Considerações sobre armazenamento de dados

Seu ambiente de desktop pode consistir em vários tipos de desktops, como desktops agrupados e dedicados. Os usuários nunca devem armazenar dados em desktops que são compartilhados entre usuários, como desktops agrupados. Se os usuários armazenarem dados em desktops dedicados, esses dados devem ser removidos se o desktop for posteriormente disponibilizado para outros usuários.

Gerenciamento de contas de usuário

Aplique as melhores práticas do Windows para gerenciamento de contas. Não crie uma conta em um modelo ou imagem antes que ela seja duplicada pelos Serviços de Criação de Máquina ou Serviços de Provisionamento. Não agende tarefas usando contas de domínio privilegiadas armazenadas. Não crie manualmente contas de máquina compartilhadas do Active Directory. Essas práticas ajudarão a evitar que um ataque de máquina obtenha senhas de contas locais persistentes e as use para fazer logon em imagens compartilhadas do MCS/PVS pertencentes a outros.

Conceda aos usuários apenas os recursos de que eles precisam. Os privilégios do Microsoft Windows continuam sendo aplicados aos desktops da maneira usual: configure privilégios por meio da Atribuição de Direitos de Usuário e associações de grupo por meio da Política de Grupo. Uma vantagem desta versão é que é possível conceder a um usuário direitos administrativos a um desktop sem também conceder controle físico sobre o computador no qual o desktop está armazenado.

Observe o seguinte ao planejar os privilégios de desktop:

- Por padrão, quando usuários não privilegiados se conectam a um desktop, eles veem o fuso horário do sistema que executa o desktop em vez do fuso horário de seu próprio dispositivo de usuário. Para obter informações sobre como permitir que os usuários vejam sua hora local ao usar desktops, consulte o artigo Gerenciar Grupos de Entrega.
- Um usuário que é administrador em um desktop tem controle total sobre esse desktop. Se um desktop for um desktop agrupado em vez de um desktop dedicado, o usuário deve ser confiável em relação a todos os outros usuários desse desktop, incluindo futuros usuários. Todos os usuários do desktop precisam estar cientes do risco permanente potencial para a segurança de seus dados que essa situação representa. Essa consideração não se aplica a desktops dedicados, que têm apenas um único usuário; esse usuário não deve ser um administrador em nenhum outro desktop.

- Um usuário que é administrador em um desktop pode geralmente instalar software nesse desktop, incluindo software potencialmente malicioso. O usuário também pode potencialmente monitorar ou controlar o tráfego em qualquer rede conectada ao desktop.

Gerenciar direitos de logon

Os direitos de logon são necessários tanto para contas de usuário quanto para contas de computador. Assim como os privilégios do Microsoft Windows, os direitos de logon continuam a ser aplicados aos desktops da maneira usual: configure os direitos de logon por meio da Atribuição de Direitos de Usuário e as associações de grupo por meio da Política de Grupo.

Os direitos de logon do Windows são: fazer logon localmente, fazer logon por meio dos Serviços de Área de Trabalho Remota, fazer logon pela rede (acessar este computador da rede), fazer logon como um trabalho em lote e fazer logon como um serviço.

Para contas de computador, conceda aos computadores apenas os direitos de logon de que eles precisam. O direito de logon "Acessar este computador da rede" é necessário para as contas de computador dos Delivery Controllers.

Para contas de usuário, conceda aos usuários apenas os direitos de logon de que eles precisam.

De acordo com a Microsoft, por padrão, o grupo Usuários da Área de Trabalho Remota recebe o direito de logon "Permitir logon por meio dos Serviços de Área de Trabalho Remota" (exceto em controladores de domínio).

A política de segurança da sua organização pode declarar explicitamente que este grupo deve ser removido desse direito de logon. Considere a seguinte abordagem:

- O Virtual Delivery Agent (VDA) para SO Multi-sessão usa os Serviços de Área de Trabalho Remota da Microsoft. Você pode configurar o grupo Usuários da Área de Trabalho Remota como um grupo restrito e controlar a associação do grupo por meio de políticas de grupo do Active Directory. Consulte a documentação da Microsoft para obter mais informações.
- Para outros componentes do Citrix Virtual Apps and Desktops™, incluindo o VDA para SO de sessão única, o grupo Usuários da Área de Trabalho Remota não é necessário. Portanto, para esses componentes, o grupo Usuários da Área de Trabalho Remota não requer o direito de logon "Permitir logon por meio dos Serviços de Área de Trabalho Remota"; você pode removê-lo. Além disso:
    - Se você administra esses computadores por meio dos Serviços de Área de Trabalho Remota, certifique-se de que todos esses administradores já sejam membros do grupo Administradores.

    - Se você não administra esses computadores por meio dos Serviços de Área de Trabalho Remota, considere desabilitar os próprios Serviços de Área de Trabalho Remota nesses computadores.

Embora seja possível adicionar usuários e grupos ao direito de logon "Negar logon por meio dos Serviços de Área de Trabalho Remota", o uso de direitos de logon de negação geralmente não é recomendado. Consulte a documentação da Microsoft para obter mais informações.

Segurança do Delivery Controller

Serviços do Windows no Delivery Controller

A instalação do Delivery Controller cria os seguintes serviços do Windows:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Gerencia contas de computador do Microsoft Active Directory para VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Coleta informações de uso da configuração do site para uso pela Citrix, se essa coleta tiver sido aprovada pelo administrador do site. Em seguida, ele envia essas informações à Citrix para ajudar a melhorar o produto.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Suporta o gerenciamento e o provisionamento de AppDisks, integração do AppDNA e gerenciamento do App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Seleciona os desktops virtuais ou aplicativos que estão disponíveis para os usuários.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Registra todas as alterações de configuração e outras alterações de estado feitas pelos administradores no site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Repositório em todo o site para configuração compartilhada.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Gerencia as permissões concedidas aos administradores.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Gerencia autotestes dos outros serviços do Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService): Armazena informações sobre as infraestruturas de hipervisor usadas em uma implantação do Citrix Virtual Apps ou Citrix Virtual Desktops e também oferece funcionalidade usada pelo console para enumerar recursos em um pool de hipervisores.

- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): Orquestra a criação de VMs de desktop.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Coleta métricas para Citrix Virtual Apps ou Citrix Virtual Desktops, armazena informações históricas e fornece uma interface de consulta para ferramentas de solução de problemas e relatórios.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): Suporta o gerenciamento do StoreFront. (Não faz parte do próprio componente StoreFront.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Suporta operações de gerenciamento privilegiado do StoreFront. (Não faz parte do próprio componente StoreFront.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): Propaga dados de configuração do banco de dados principal do site para o Local Host Cache.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): Seleciona os desktops virtuais ou aplicativos que estão disponíveis para os usuários, quando o banco de dados principal do site está indisponível.

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Estes também são criados quando instalados com outros componentes Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Suporta a coleta de informações de diagnóstico para uso pelo Suporte Citrix.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Coleta informações de diagnóstico para análise pela Citrix, de modo que os resultados da análise e as recomendações possam ser visualizados pelos administradores para ajudar a diagnosticar problemas com o site.

A instalação do Delivery Controller também cria o seguinte serviço do Windows. Este não está sendo usado atualmente. Se tiver sido ativado, desative-o.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Estes não estão sendo usados atualmente, mas devem ser ativados. Não os desative.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Exceto pelo Citrix Storefront™ Privileged Administration Service, a esses serviços é concedido o direito de logon Fazer logon como um serviço e os privilégios Ajustar cotas de memória para um processo, Gerar auditorias de segurança e Substituir um token de nível de processo. Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Delivery Controller e são automaticamente desativados.

Exceto pelo serviço Citrix Storefront Privileged Administration e pelo Citrix Telemetry Service, os serviços do Windows do Delivery Controller listados acima são configurados para fazer logon como a identidade NETWORK SERVICE. Não altere essas configurações de serviço.

O Citrix Config Synchronizer Service precisa que a conta NETWORK SERVICE pertença ao grupo Administrador Local no Delivery Controller. Isso permite que o Local Host Cache funcione corretamente.

O serviço Citrix Storefront Privileged Administration está configurado para fazer logon como Sistema Local (NT AUTHORITY\SYSTEM). Isso é necessário para operações do StoreFront do Delivery Controller que normalmente não estão disponíveis para serviços (incluindo a criação de sites do Microsoft IIS). Não altere suas configurações de serviço.

O Citrix Telemetry Service está configurado para fazer logon com sua própria identidade específica de serviço.

Você pode desativar o Citrix Telemetry Service. Além deste serviço e dos serviços que já estão desativados, não desative nenhum outro desses serviços do Windows do Delivery Controller.

Gerenciar direitos de logon

As contas de computador dos VDAs devem ter o direito de logon "Acessar este computador a partir da rede". Consulte Descoberta de Controller baseada em OU do Active Directory.

Acesso do cliente

O acesso do cliente é normalmente fornecido pela implantação do Citrix StoreFront. Para obter mais informações sobre como proteger o StoreFront, consulte a documentação do StoreFront.

Para permitir que usuários remotos se conectem com segurança ao StoreFront e aos VDAs, implante um gateway NetScaler®.

A Citrix recomenda que os clientes se conectem ao StoreFront usando o aplicativo Citrix Workspace. Para obter mais informações, consulte as seções de segurança da documentação do

aplicativo Citrix Workspace para cada sistema operacional. Alternativamente, os usuários podem usar um navegador da web para acessar o StoreFront.

Considere fornecer aos usuários thin clients onde os usuários têm capacidade limitada de executar aplicativos que não sejam o aplicativo Citrix Workspace™. Onde os dispositivos são gerenciados por sua organização, você deve implementar políticas para garantir a implantação de atualizações de segurança do sistema operacional e software antivírus. No entanto, em muitos casos, os usuários precisam ser capazes de se conectar de dispositivos não gerenciados fora do controle de sua organização. Considere usar os seguintes recursos:

- Endpoint Analysis para verificar endpoints em busca de informações de segurança, como sistema operacional e antivírus, e negar acesso a clientes que não atendam aos seus requisitos de segurança.
- App Protection bloqueia keyloggers e captura de tela.

Ambientes de versão mista

Ambientes de versão mista, por exemplo, onde os VDAs têm uma versão diferente do Delivery Controller, são inevitáveis durante algumas atualizações. Siga as melhores práticas e minimize o tempo em que componentes Citrix de diferentes versões coexistem. Em ambientes de versão mista, a política de segurança, por exemplo, pode não ser aplicada uniformemente.

> **Observação:**

> Isso é típico de outros produtos de software; o uso de uma versão anterior do Active Directory apenas aplica parcialmente a Política de Grupo com versões posteriores do Windows.

> O cenário a seguir descreve um problema de segurança que pode ocorrer em um ambiente Citrix específico de versão mista. Quando o Citrix Receiver 1.7 é usado para se conectar a um desktop virtual executando o VDA no XenApp e XenDesktop 7.6 Feature Pack 2, a configuração de política **Permitir transferência de arquivos entre desktop e cliente** está habilitada no Site, mas não pode ser desabilitada por um Delivery Controller executando o XenApp e XenDesktop 7.1. Ele não reconhece a configuração de política, que foi lançada na versão posterior do produto. Essa configuração de política permite que os usuários carreguem e baixem arquivos para seu desktop virtual, o que é o problema de segurança. Para contornar isso, atualize o Delivery Controller (ou uma instância autônoma do Studio) para a versão 7.6 Feature Pack 2 e, em seguida, use a Política de Grupo para desabilitar a

configuração de política. Alternativamente, use a política local em todos os desktops virtuais afetados.

Considerações de segurança do Acesso Remoto ao PC

O Acesso Remoto ao PC implementa os seguintes recursos de segurança:

- O uso de cartão inteligente é suportado.
- Quando uma sessão remota se conecta, o monitor do PC do escritório aparece em branco.
- O Acesso Remoto ao PC redireciona todas as entradas de teclado e mouse para a sessão remota, exceto CTRL+ALT+DEL e cartões inteligentes habilitados para USB e dispositivos biométricos.
- O SmoothRoaming é suportado apenas para um único usuário.
- Quando um usuário tem uma sessão remota conectada a um PC de escritório, somente esse usuário pode retomar o acesso local ao PC de escritório. Para retomar o acesso local, o usuário pressiona Ctrl-Alt-Del no PC local e, em seguida, faz login com as mesmas credenciais usadas pela sessão remota. O usuário também pode retomar o acesso local inserindo um cartão inteligente ou utilizando biometria, se o seu sistema tiver a integração apropriada de Provedor de Credenciais de terceiros. Este comportamento padrão pode ser substituído ativando a Troca Rápida de Usuário via Objetos de Política de Grupo (GPOs) ou editando o registro.

Observação:

A Citrix recomenda que você não atribua privilégios de administrador de VDA a usuários de sessão geral.

Atribuições automáticas

Por padrão, o Acesso Remoto ao PC suporta a atribuição automática de vários usuários a um VDA. No XenDesktop 5.6 Feature Pack 1, os administradores podiam substituir esse comportamento usando o script PowerShell RemotePCAccess.ps1. Esta versão usa uma entrada de registro para permitir ou proibir múltiplas atribuições automáticas de PC remoto; essa configuração se aplica a todo o Site.

Cuidado:

> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> Para restringir atribuições automáticas a um único usuário:

Em cada Controller no Site, defina a seguinte entrada de registro:

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

Se houver atribuições de usuário existentes, remova-as usando comandos SDK para que o VDA seja subsequentemente elegível para uma única atribuição automática.

- Remova todos os usuários atribuídos do VDA: `$machine.AssociatedUserNames | % { Remove-BrokerUser-Name $_ -Machine $machine`
- Remova o VDA do Grupo de Entrega: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Reinicie o PC físico do escritório.

Cartões inteligentes

Cartões inteligentes e tecnologias equivalentes são suportados dentro das diretrizes descritas neste artigo. Para usar cartões inteligentes com o Citrix Virtual Apps ou o Citrix Virtual Desktops™:

- Compreenda a política de segurança da sua organização em relação ao uso de cartões inteligentes. Essas políticas podem, por exemplo, indicar como os cartões inteligentes são emitidos e como os usuários devem protegê-los. Alguns aspectos dessas políticas podem precisar ser reavaliados em um ambiente Citrix Virtual Apps™ ou Citrix Virtual Desktops.
- Determine quais tipos de dispositivos de usuário, sistemas operacionais e aplicativos publicados serão usados com cartões inteligentes.

- Familiarize-se com a tecnologia de cartão inteligente e com o hardware e software do fornecedor de cartão inteligente selecionado.
- Saiba como implantar certificados digitais em um ambiente distribuído.

Observação:

O registro de cartão inteligente não é suportado com cartão inteligente rápido. O registro de cartão inteligente pode funcionar quando o cartão inteligente rápido está desabilitado, mas depende do tipo de cartão inteligente e do middleware. Entre em contato com o fornecedor do seu cartão inteligente e middleware para obter informações sobre a integração deles com o Citrix Virtual Apps and Desktops e o suporte para registro de cartão inteligente em sessões virtuais.

Tipos de cartões inteligentes

Cartões inteligentes empresariais e de consumidor têm as mesmas dimensões, conectores elétricos e se encaixam nos mesmos leitores de cartão inteligente.

Cartões inteligentes para uso empresarial contêm certificados digitais. Esses cartões inteligentes suportam o Logon do Windows e também podem ser usados com aplicativos para assinatura digital e criptografia de documentos e e-mails. O Citrix Virtual Apps and Desktops™ suporta esses usos.

Cartões inteligentes para uso do consumidor não contêm certificados digitais; eles contêm um segredo compartilhado. Esses cartões inteligentes podem suportar pagamentos (como um cartão de crédito com chip e assinatura ou chip e PIN). Eles não suportam o Logon do Windows ou aplicativos típicos do Windows. Aplicativos Windows especializados e uma infraestrutura de software adequada (incluindo, por exemplo, uma conexão a uma rede de cartões de pagamento) são necessários para uso com esses cartões inteligentes. Entre em contato com seu representante Citrix para obter informações sobre o suporte a esses aplicativos especializados no Citrix Virtual Apps ou Citrix Virtual Desktops.

Para cartões inteligentes empresariais, existem equivalentes compatíveis que podem ser usados de forma semelhante.

- Um token USB equivalente a cartão inteligente se conecta diretamente a uma porta USB. Esses tokens USB geralmente têm o tamanho de um pen drive USB, mas podem ser tão

pequenos quanto um cartão SIM usado em um telefone celular. Eles aparecem como a combinação de um cartão inteligente mais um leitor de cartão inteligente USB.

- Um cartão inteligente virtual usando um Módulo de Plataforma Confiável (TPM) do Windows aparece como um cartão inteligente. Esses cartões inteligentes virtuais são suportados para Windows 8 e Windows 10, usando o aplicativo Citrix Workspace (versão mínima Citrix Receiver 4.3).

  - Versões do Citrix Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) anteriores ao XenApp e XenDesktop 7.6 FP3 não suportam cartões inteligentes virtuais.
  - Para mais informações sobre cartões inteligentes virtuais, consulte Visão geral do cartão inteligente virtual.

  Nota: O termo "cartão inteligente virtual" também é usado para descrever um certificado digital armazenado no computador do usuário. Esses certificados digitais não são estritamente equivalentes a cartões inteligentes.

O suporte a cartões inteligentes do Citrix Virtual Apps and Desktops é baseado nas especificações padrão Microsoft Personal Computer/Smart Card (PC/SC). Um requisito mínimo é que os cartões inteligentes e os dispositivos de cartão inteligente devem ser suportados pelo sistema operacional Windows subjacente e devem ser aprovados pelos Microsoft Windows Hardware Quality Labs (WHQL) para serem usados em computadores que executam sistemas operacionais Windows qualificados. Consulte a documentação da Microsoft para obter informações adicionais sobre a conformidade de hardware PC/SC. Outros tipos de dispositivos de usuário podem estar em conformidade com o padrão PS/SC. Para obter mais informações, consulte o programa Citrix Ready.

Geralmente, é necessário um driver de dispositivo separado para o cartão inteligente de cada fornecedor ou equivalente. No entanto, se os cartões inteligentes estiverem em conformidade com um padrão como o NIST Personal Identity Verification (PIV), pode ser possível usar um único driver de dispositivo para uma variedade de cartões inteligentes. O driver de dispositivo deve ser instalado tanto no dispositivo do usuário quanto no Virtual Delivery Agent (VDA). O driver de dispositivo é frequentemente fornecido como parte de um pacote de middleware de cartão inteligente disponível em um parceiro Citrix; o pacote de middleware de cartão inteligente oferece recursos avançados. O driver de dispositivo também pode ser descrito como um Cryptographic Service Provider (CSP), Key Storage Provider (KSP) ou minidriver.

As seguintes combinações de cartão inteligente e middleware para sistemas Windows foram testadas pela Citrix como exemplos representativos de seu tipo. No entanto, outros cartões

inteligentes e middleware também podem ser usados. Para obter mais informações sobre cartões inteligentes e middleware compatíveis com Citrix, consulte `<http://www.citrix.com/ready>`.

MIDDLEWARE	CARTÕES CORRESPONDENTES
Mini Driver Gemalto para cartão .NET	Gemalto .NET v2+

Para obter informações sobre o uso de cartões inteligentes com outros tipos de dispositivos, consulte a documentação do aplicativo Citrix Workspace™ para esse dispositivo.

Acesso Remoto ao PC

Os cartões inteligentes são suportados apenas para acesso remoto a PCs físicos de escritório que executam Windows 10, Windows 8 ou Windows 7.

Os seguintes cartões inteligentes foram testados com o Acesso Remoto a PC:

MIDDLEWARE	CARTÕES CORRESPONDENTES
Minidriver Gemalto .NET	Gemalto .NET v2+

Cartão inteligente rápido

O cartão inteligente rápido é uma melhoria em relação ao redirecionamento de cartão inteligente baseado em HDX PC/SC existente. Ele melhora o desempenho quando os cartões inteligentes são usados em situações de WAN com alta latência. Quando a latência é alta, a melhoria de desempenho pode ser significativa (por exemplo, 15 segundos para um logon de cartão inteligente rápido do Windows em comparação com mais de 1 minuto com o redirecionamento de cartão inteligente baseado em PC/SC).

O cartão inteligente rápido é ativado por padrão em máquinas host com VDAs Windows atualmente suportados. Para desativar o Cartão Inteligente Rápido no lado do host — por exemplo, para fins de diagnóstico — defina a configuração de registro 'Disable Cryptographic Redirection' para qualquer valor diferente de zero:

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

No lado do cliente, para habilitar o cartão inteligente rápido, inclua o parâmetro ICA SmartCardCryptographicRedirection no arquivo *default.ica* do site StoreFront associado:

```
[WFClient]

SmartCardCryptographicRedirection=On
```

Além disso, no lado do cliente, o cartão inteligente rápido pode ser forçado a ser ativado ou forçado a ser desativado (por exemplo, para fins de diagnóstico) com as seguintes configurações de registro:

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (como um DWORD diferente de zero)

Ou

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (como um DWORD diferente de zero)

O hive de registro de 32 bits deve ser especificado (usando `WOW6432Node`) se a máquina cliente for de 64 bits.

Limitações:

- Apenas o aplicativo Citrix Workspace para Windows suporta cartão inteligente rápido. Se você configurar cartões inteligentes rápidos no arquivo default.ica, os aplicativos Citrix Workspace que não são para Windows ainda usarão o redirecionamento PC/SC existente.
- Os únicos cenários de salto duplo que o cartão inteligente rápido suporta são ICA® > ICA com cartão inteligente rápido ativado em ambos os saltos. Como o cartão inteligente rápido não suporta cenários de salto duplo ICA > RDP, esses cenários não funcionam.
- O cartão inteligente rápido não suporta Criptografia de Próxima Geração. Assim, o cartão inteligente rápido não suporta cartões inteligentes de Criptografia de Curva Elíptica (ECC).
- O cartão inteligente rápido suporta apenas operações de contêiner de chave somente leitura.
- O cartão inteligente rápido não suporta a alteração do PIN do cartão inteligente.

A partir da versão 2203 do VDA e da versão 2202 do aplicativo Citrix Workspace para Windows (ou posterior), o cartão inteligente rápido é compatível com a Criptografia de Próxima Geração (CNG). Além disso, os cartões inteligentes de Criptografia de Curva Elíptica (ECC) são suportados com as seguintes curvas: P-256, P-384, P-521 bits, para ECDSA e ECDH.

A partir da versão 2203 do VDA, o cartão inteligente rápido adiciona a capacidade de armazenar em cache o PIN do cartão inteligente entre os aplicativos da mesma sessão de logon do usuário. Por exemplo, se o **Cache de PIN da Sessão** estiver ativado e o usuário final tiver fornecido anteriormente seu PIN de cartão inteligente ao Outlook, quando o Word for usado para assinar um documento, o Word usará o PIN de cartão inteligente já armazenado em cache (enviado ao Outlook). O **Cache de PIN da Sessão** melhora a experiência do usuário, reduzindo o número de vezes que o usuário precisa inserir seu PIN de cartão inteligente. Além disso, se o cartão inteligente for usado para fazer logon no VDA, o PIN de logon do cartão inteligente do Windows pode ser opcionalmente salvo no **Cache de PIN da Sessão**. Isso pode melhorar ainda mais a experiência do usuário.

O **Cache de PIN da Sessão** está desativado por padrão. Ele pode ser ativado e controlado com as seguintes configurações de registro no VDA:

Em HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` como um DWORD (diferente de zero para ativar)
- `EnableLogonPinSessionCache` como um DWORD (diferente de zero para ativar)
- `PinSessionCacheEntryStaleTimeout` como um DWORD (número de segundos antes que uma entrada se torne obsoleta, o padrão é 1 hora)

Tipos de leitores de cartão inteligente

Um leitor de cartão inteligente pode ser integrado ao dispositivo do usuário ou anexado separadamente ao dispositivo do usuário (geralmente via USB ou Bluetooth). Leitores de cartão de contato que estão em conformidade com a especificação USB Chip/Smart Card Interface Devices (CCID) são suportados. Eles contêm um slot ou um leitor onde o usuário insere o cartão inteligente. O padrão Deutsche Kreditwirtschaft (DK) define quatro classes de leitores de cartão de contato.

- Os leitores de cartão inteligente Classe 1 são os mais comuns e geralmente contêm um slot. Os leitores de cartão inteligente Classe 1 são suportados, geralmente com um driver de dispositivo CCID padrão fornecido com o sistema operacional.
- Os leitores de cartão inteligente Classe 2 também contêm um teclado seguro que não pode ser acessado pelo dispositivo do usuário. Os leitores de cartão inteligente Classe 2 podem ser integrados a um teclado com um teclado seguro integrado. Para leitores de cartão inteligente Classe 2, entre em contato com seu representante Citrix; um driver de dispositivo específico do leitor pode ser necessário para habilitar a capacidade do teclado seguro.

- Os leitores de cartão inteligente Classe 3 também contêm um display seguro. Os leitores de cartão inteligente Classe 3 não são suportados.
- Os leitores de cartão inteligente Classe 4 também contêm um módulo de transação seguro. Os leitores de cartão inteligente Classe 4 não são suportados.

> **Observação:**
>
> A classe do leitor de cartão inteligente não está relacionada à classe de dispositivo USB.
>
> Os leitores de cartão inteligente devem ser instalados com um driver de dispositivo correspondente no dispositivo do usuário.

Para obter informações sobre leitores de cartão inteligente suportados, consulte a documentação do aplicativo Citrix Workspace que você está usando. Na documentação do aplicativo Citrix Workspace, as versões suportadas são listadas em um artigo sobre cartão inteligente ou no artigo de requisitos do sistema.

Experiência do usuário

O suporte a smart card é integrado ao Citrix Virtual Apps and Desktops, usando um canal virtual de smart card ICA/HDX específico que é habilitado por padrão.

Importante: Não use o redirecionamento USB genérico para leitores de smart card. Isso é desabilitado por padrão para leitores de smart card e não é suportado se habilitado.

Vários smart cards e vários leitores podem ser usados no mesmo dispositivo do usuário, mas se a autenticação pass-through estiver em uso, apenas um smart card deve ser inserido quando o usuário inicia um desktop ou aplicativo virtual. Quando um smart card é usado dentro de um aplicativo (por exemplo, para funções de assinatura digital ou criptografia), pode haver outros avisos para inserir um smart card ou digitar um PIN. Isso pode ocorrer se mais de um smart card tiver sido inserido ao mesmo tempo.

- Se os usuários forem solicitados a inserir um smart card quando o smart card já estiver no leitor, eles devem selecionar Cancelar.
- Se os usuários forem solicitados a inserir o PIN, eles devem digitá-lo novamente.

Você pode redefinir PINs usando um sistema de gerenciamento de cartão ou um utilitário do fornecedor.

Importante:

Dentro de uma sessão do Citrix Virtual Apps ou Citrix Virtual Desktops, o uso de um smart card com o aplicativo Microsoft Remote Desktop Connection não é suportado. Isso é às vezes descrito como um uso de "salto duplo".

Antes de implantar smart cards

- Obtenha um driver de dispositivo para o leitor de smart card e instale-o no dispositivo do usuário. Muitos leitores de smart card podem usar o driver de dispositivo CCID fornecido pela Microsoft.
- Obtenha um driver de dispositivo e software de provedor de serviços criptográficos (CSP) do seu fornecedor de smart card e instale-os em dispositivos de usuário e desktops virtuais. O driver e o software CSP devem ser compatíveis com o Citrix Virtual Apps and Desktops; verifique a documentação do fornecedor para compatibilidade. Para desktops virtuais que usam smart cards que suportam e usam o modelo de minidriver, os minidrivers de smart card são baixados automaticamente, mas você também pode obtê-los em http://catalog.update.microsoft.com ou do seu fornecedor. Além disso, se o middleware PKCS#11 for necessário, obtenha-o do fornecedor do cartão.
- Importante: A Citrix recomenda que você instale e teste os drivers e o software CSP em um computador físico antes de instalar o software Citrix.
- Adicione a URL do Citrix Receiver™ for Web à lista de Sites Confiáveis para usuários que usam smart cards no Internet Explorer com Windows 10. No Windows 10, o Internet Explorer não é executado no modo protegido por padrão para sites confiáveis.
- Certifique-se de que sua infraestrutura de chave pública (PKI) esteja configurada adequadamente. Isso inclui garantir que o mapeamento de certificado para conta esteja configurado corretamente para o ambiente do Active Directory e que a validação do certificado do usuário possa ser realizada com sucesso.
- Certifique-se de que sua implantação atenda aos requisitos de sistema dos outros componentes Citrix usados com smart cards, incluindo o aplicativo Citrix Workspace e o StoreFront.
- Garanta o acesso aos seguintes servidores em seu Site:
    - O controlador de domínio do Active Directory para a conta de usuário associada a um certificado de logon no cartão inteligente
    - Delivery Controller™

- Citrix StoreFront
- Citrix Gateway/Citrix Access Gateway 10.x
- VDA
- (Opcional para Acesso Remoto a PC): Microsoft Exchange Server

Habilitar o uso de cartão inteligente

Etapa 1. Emita cartões inteligentes para os usuários de acordo com sua política de emissão de cartões.

Etapa 2. (Opcional) Configure os cartões inteligentes para habilitar os usuários para o Acesso Remoto a PC.

Etapa 3. Instale e configure o Delivery Controller e o StoreFront (se ainda não estiverem instalados) para o acesso remoto de cartão inteligente.

Etapa 4. Habilite o StoreFront para o uso de cartão inteligente. Para obter detalhes, consulte Configure smart card authentication na documentação do StoreFront.

Etapa 5. Habilite o Citrix Gateway/Access Gateway para o uso de cartão inteligente. Para obter detalhes, consulte Configuring Authentication and Authorization e Configuring Smart Card Access with the Web Interface na documentação do NetScaler.

Etapa 6. Habilite os VDAs para o uso de cartão inteligente.

- Garanta que o VDA tenha os aplicativos e atualizações necessários.
- Instale o middleware.
- Configure o acesso remoto de cartão inteligente, habilitando a comunicação de dados do cartão inteligente entre o aplicativo Citrix Workspace em um dispositivo de usuário e uma sessão de desktop virtual.

Etapa 7. Habilite os dispositivos de usuário (incluindo máquinas ingressadas ou não ingressadas no domínio) para o uso de cartão inteligente. Consulte Configure smart card authentication na documentação do StoreFront para obter detalhes.

- Importe o certificado raiz da autoridade de certificação e o certificado da autoridade de certificação emissora para o keystore do dispositivo.
- Instale o middleware de cartão inteligente do seu fornecedor.

- Instale e configure o aplicativo Citrix Workspace para Windows, certificando-se de importar icaclient.adm usando o Console de Gerenciamento de Política de Grupo e habilitar a autenticação de cartão inteligente.

Etapa 8. Teste a implantação. Certifique-se de que a implantação esteja configurada corretamente iniciando um desktop virtual com o cartão inteligente de um usuário de teste. Teste todos os mecanismos de acesso possíveis (por exemplo, acessando o desktop através do Internet Explorer e do aplicativo Citrix Workspace).

Rastrear a contagem de inserções do leitor de cartão inteligente

Com o acesso remoto de cartão inteligente, você pode rastrear o número de vezes que um cartão inteligente foi inserido ou removido de um leitor usando a função SCardGetStatusChange. A função atualiza um array de estruturas de dados SCARD_READERSTATE — uma para cada leitor que você monitora. A palavra alta (16 bits) do campo dwEventState de cada SCARD_READERSTATE contém a contagem do leitor. Para obter mais informações, consulte os artigos da Microsoft SCardGetStatusChangeA function e SCARD_READERSTATEA structure.

A configuração **Relatório de Contagem de Inserções do Leitor** está desabilitada por padrão. Para habilitar o rastreamento, adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Name: EnableReaderInsertCountReporting

Tipo: DWORD

Valor: Qualquer valor diferente de zero

Quando a sessão é desconectada, a contagem é redefinida para zero.

Relatório de Contagem de Inserções do Leitor é compatível com middleware de cartão inteligente de terceiros.

Implantações de cartão inteligente

Os seguintes tipos de implantações de cartão inteligente são suportados por esta versão do produto e por ambientes mistos que contêm esta versão. Outras configurações podem funcionar, mas não são suportadas.

TIPO	CONECTIVIDADE DO STOREFRONT™
Computadores locais ingressados no domínio	Conectado diretamente
Acesso remoto de computadores ingressados no domínio	Conectado via Citrix Gateway
Computadores não ingressados no domínio	Conectado diretamente
Acesso remoto de computadores não ingressados no domínio	Conectado via Citrix Gateway
Computadores não ingressados no domínio e thin clients acessando o site do Desktop Appliance	Conectado via sites do Desktop Appliance
Computadores ingressados no domínio e thin clients acessando o StoreFront através da URL dos Serviços XenApp®	Conectado via URLs dos Serviços XenApp

Os tipos de implantação são definidos pelas características do dispositivo do usuário ao qual o leitor de cartão inteligente está conectado:

- Se o dispositivo está ingressado no domínio ou não ingressado no domínio.
- Como o dispositivo está conectado ao StoreFront.
- Qual software é usado para visualizar desktops e aplicativos virtuais.

Além disso, aplicativos habilitados para cartão inteligente, como Microsoft Word e Microsoft Excel, podem ser usados nessas implantações. Esses aplicativos permitem que os usuários assinem ou criptografem documentos digitalmente.

Autenticação bimodal

Sempre que possível em cada uma dessas implantações, o Receiver oferece suporte à autenticação bimodal, oferecendo ao usuário a escolha entre usar um cartão inteligente e inserir seu nome de usuário e senha. Isso é útil se o cartão inteligente não puder ser usado (por exemplo, o usuário o deixou em casa ou o certificado de logon expirou).

Como os usuários de dispositivos não ingressados no domínio fazem logon diretamente no Receiver para Windows, você pode permitir que os usuários recorram à autenticação explícita. Se você configurar a autenticação bimodal, os usuários serão inicialmente solicitados a fazer logon

usando seus cartões inteligentes e PINs, mas terão a opção de selecionar a autenticação explícita se tiverem algum problema com seus cartões inteligentes.

Se você implantar o Citrix Gateway, os usuários farão logon em seus dispositivos e serão solicitados pelo Receiver para Windows a autenticar no Citrix Gateway. Isso se aplica a dispositivos ingressados no domínio e não ingressados no domínio. Os usuários podem fazer logon no Citrix Gateway usando seus cartões inteligentes e PINs, ou com credenciais explícitas. Isso permite que você forneça aos usuários autenticação bimodal para logons no Citrix Gateway. Configure a autenticação pass-through do Citrix Gateway para o StoreFront e delegue a validação de credenciais ao Citrix Gateway para usuários de cartão inteligente, para que os usuários sejam autenticados silenciosamente no StoreFront.

Considerações sobre várias florestas do Active Directory

Em um ambiente Citrix, os cartões inteligentes são suportados dentro de uma única floresta. Logons de cartão inteligente entre florestas exigem uma confiança de floresta bidirecional direta para todas as contas de usuário. Implantações multifloresta mais complexas envolvendo cartões inteligentes (ou seja, onde as confianças são apenas unidirecionais ou de tipos diferentes) não são suportadas.

Você pode usar cartões inteligentes em um ambiente Citrix que inclui desktops remotos. Esse recurso pode ser instalado localmente (no dispositivo do usuário ao qual o cartão inteligente está conectado) ou remotamente (no desktop remoto ao qual o dispositivo do usuário se conecta).

Política de remoção de cartão inteligente

A política de remoção de cartão inteligente definida no produto determina o que acontece se você remover o cartão inteligente do leitor durante uma sessão. A política de remoção de cartão inteligente é configurada e gerenciada pelo sistema operacional Windows.

CONFIGURAÇÃO DA POLÍTICA	COMPORTAMENTO DA ÁREA DE TRABALHO
Nenhuma ação	Nenhuma ação.
Bloquear estação de trabalho	A sessão da área de trabalho é desconectada e a área de trabalho virtual é bloqueada.
Forçar logoff	O usuário é forçado a fazer logoff. Se a conexão de rede for perdida e essa configuração estiver ativada, a sessão poderá ser desconectada e o usuário poderá perder dados.

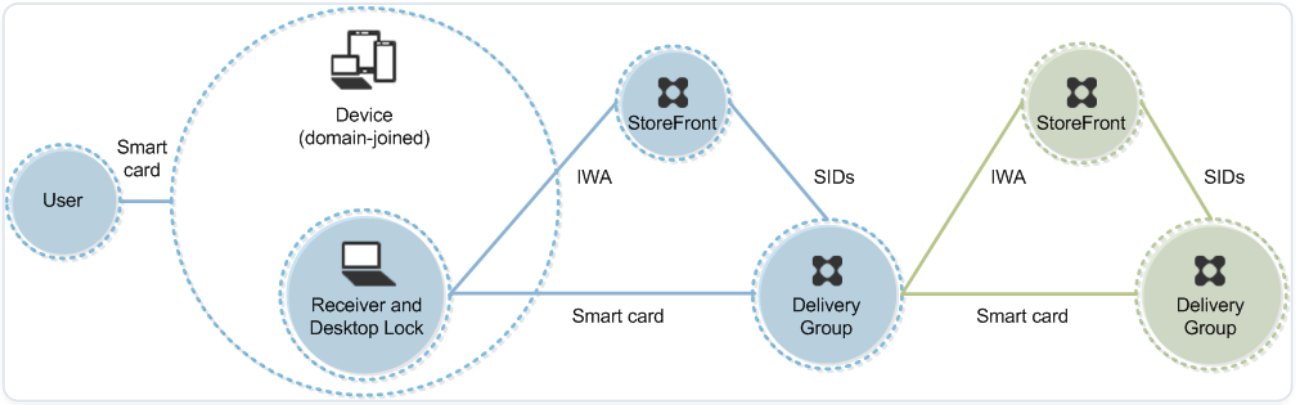
CONFIGURAÇÃO DA POLÍTICA	COMPORTAMENTO DA ÁREA DE TRABALHO
Desconectar se for uma sessão remota do Terminal Services	A sessão é desconectada e a área de trabalho virtual é bloqueada.

Verificação de revogação de certificado

Se a verificação de revogação de certificado estiver ativada e um usuário inserir um cartão inteligente com um certificado inválido em um leitor de cartão, o usuário não poderá autenticar ou acessar a área de trabalho ou o aplicativo relacionado ao certificado. Por exemplo, se o certificado inválido for usado para descriptografia de e-mail, o e-mail permanecerá criptografado. Se outros certificados no cartão, como os usados para autenticação, ainda forem válidos, essas funções permanecerão ativas.

Exemplo de implantação: computadores ingressados no domínio

Esta implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.

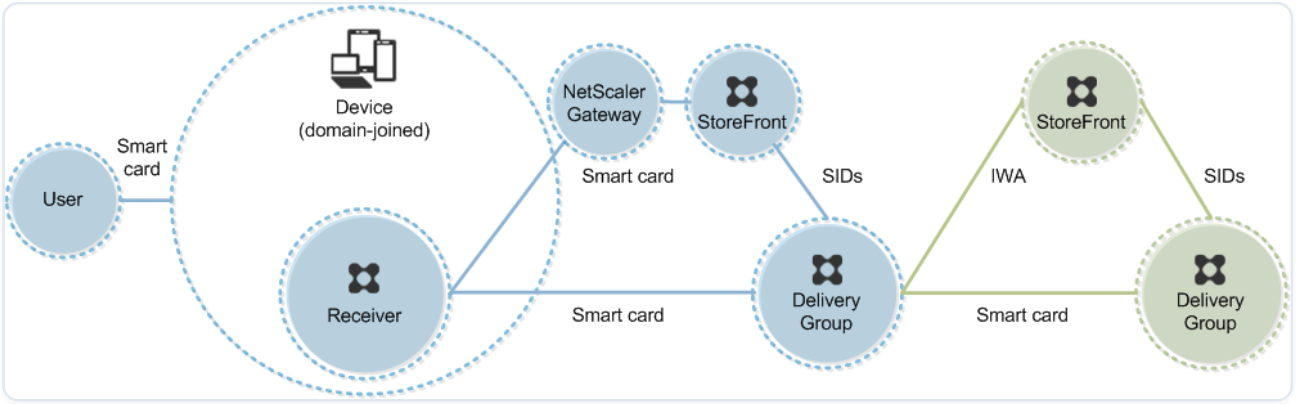


Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN. O Receiver autentica o usuário em um servidor StoreFront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia uma área de trabalho virtual ou aplicativo, o usuário não é solicitado a inserir um PIN novamente porque o recurso de logon único está configurado no Receiver.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Exemplo de implantação: acesso remoto de computadores ingressados no domínio

Esta implantação envolve dispositivos de usuário ingressados no domínio que executam o Desktop Viewer e se conectam ao StoreFront através do Citrix Gateway/Access Gateway.



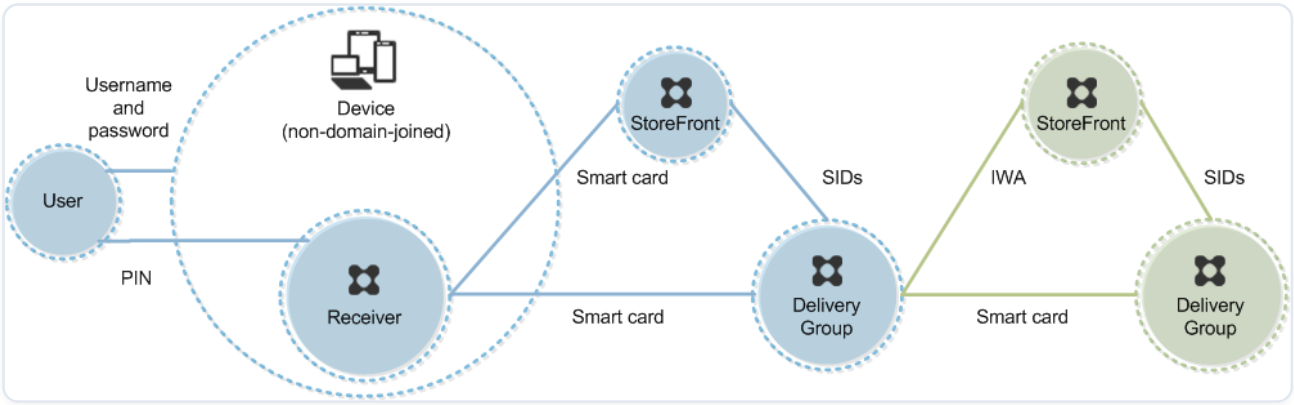
Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN, e então faz logon novamente no Citrix Gateway/Access Gateway. Este segundo logon pode ser com o cartão inteligente e PIN ou com um nome de usuário e senha, pois o Receiver permite autenticação bimodal nesta implantação.

O usuário é automaticamente conectado ao StoreFront, que passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps™ ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual ou aplicativo, ele não é solicitado novamente por um PIN porque o recurso de logon único está configurado no Receiver.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Exemplo de implantação: computadores não ingressados no domínio

Esta implantação envolve dispositivos de usuário não ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.



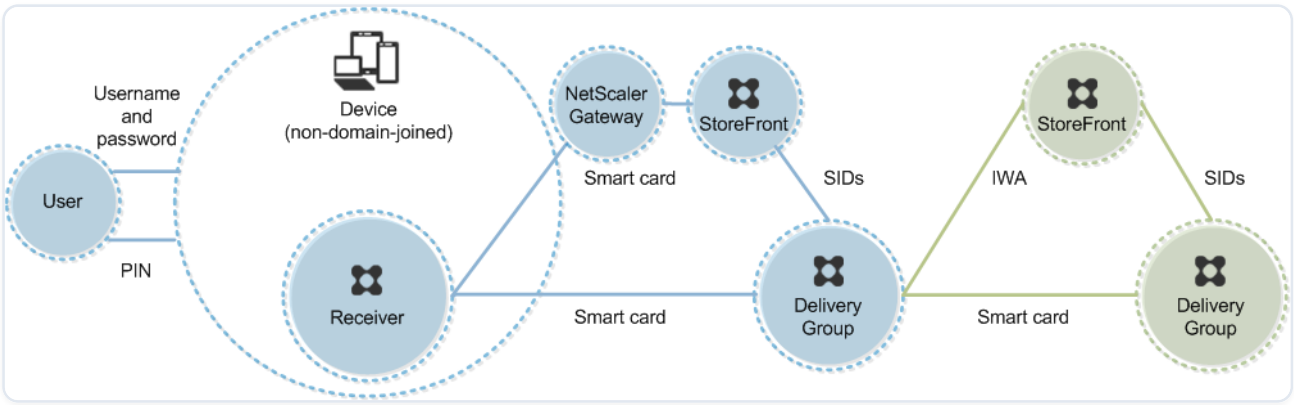
Um usuário faz logon em um dispositivo. Normalmente, o usuário insere um nome de usuário e senha, mas, como o dispositivo não está ingressado em um domínio, as credenciais para este logon são opcionais. Como a autenticação bimodal é possível nesta implantação, o Receiver solicita ao usuário um cartão inteligente e PIN ou um nome de usuário e senha. O Receiver então autentica-se no StoreFront.

O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual ou aplicativo, ele é solicitado novamente por um PIN porque o recurso de logon único não está disponível nesta implantação.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual autentica-se no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Exemplo de implantação: acesso remoto de computadores não ingressados no domínio

Esta implantação envolve dispositivos de usuário não ingressados no domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.



Um usuário faz logon em um dispositivo. Normalmente, o usuário insere um nome de usuário e senha, mas, como o dispositivo não está associado a um domínio, as credenciais para este logon são opcionais. Como a autenticação bimodal é possível nesta implantação, o Receiver solicita ao usuário um cartão inteligente e PIN ou um nome de usuário e senha. O Receiver então se autentica no StoreFront.

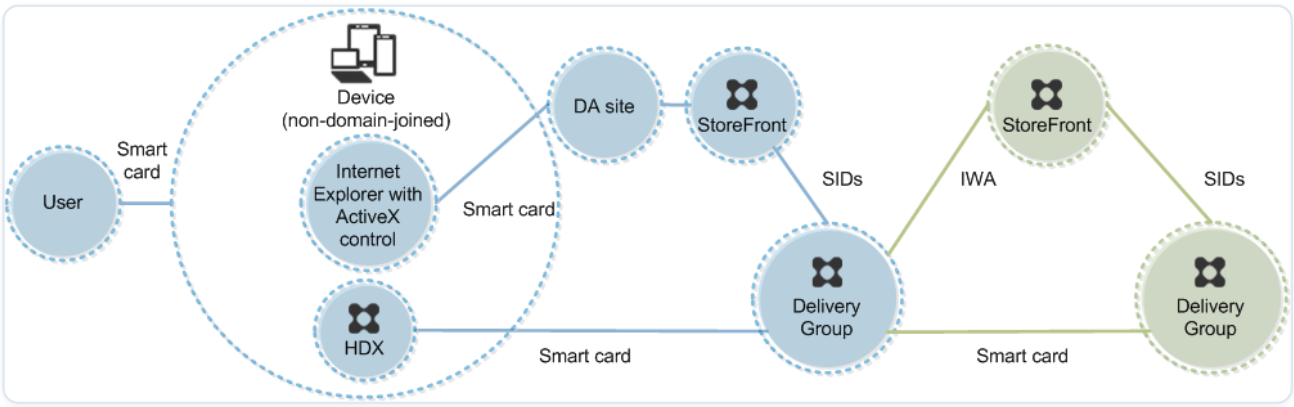
O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop ou aplicativo virtual, ele é solicitado a inserir um PIN novamente porque o recurso de logon único não está disponível nesta implantação.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Exemplo de implantação: computadores não associados a domínio e thin clients acessando o site do Desktop Appliance

Esta implantação envolve dispositivos de usuário não associados a domínio que podem executar o Desktop Lock e se conectar ao StoreFront por meio de sites do Desktop Appliance.

O Desktop Lock é um componente separado que é lançado com o Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. É uma alternativa ao Desktop Viewer e foi projetado principalmente para computadores Windows reaproveitados e thin clients Windows. O Desktop Lock substitui o shell do Windows e o Gerenciador de Tarefas nesses dispositivos de usuário, impedindo que os usuários acessem os dispositivos subjacentes. Com o Desktop Lock, os usuários podem acessar desktops de Máquina de Servidor Windows e desktops de Máquina de Desktop Windows. A instalação do Desktop Lock é opcional.



Um usuário faz logon em um dispositivo com um cartão inteligente. Se o Desktop Lock estiver em execução no dispositivo, o dispositivo será configurado para iniciar um site do Desktop Appliance

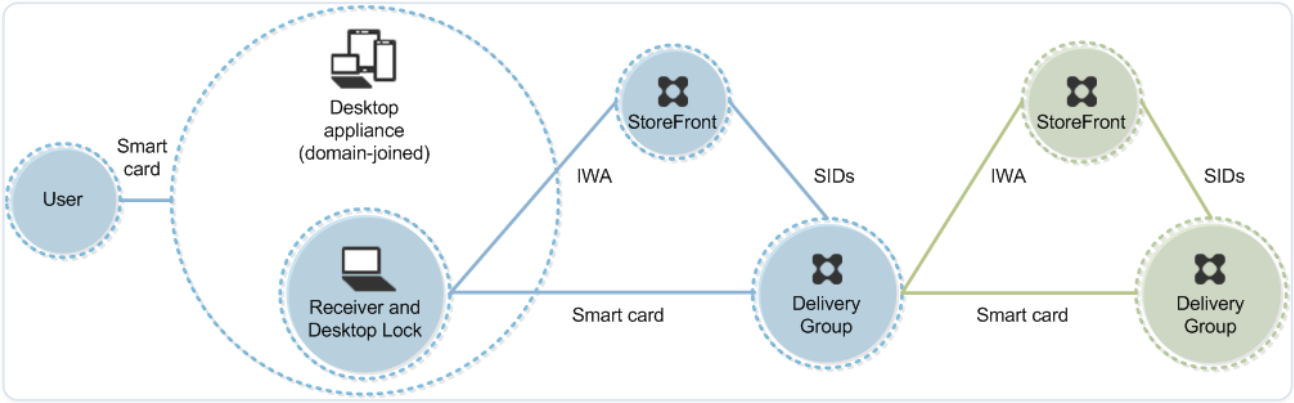
por meio do Internet Explorer em execução no Modo Quiosque. Um controle ActiveX no site solicita ao usuário um PIN e o envia ao StoreFront. O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. O primeiro desktop disponível na lista alfabética em um Grupo de Desktop atribuído é iniciado.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Exemplo de implantação: computadores associados a domínio e thin clients acessando o StoreFront por meio da URL dos Serviços XenApp

Esta implantação envolve dispositivos de usuário associados a domínio que executam o Desktop Lock e se conectam ao StoreFront por meio de URLs dos Serviços XenApp.

O Desktop Lock é um componente separado que é lançado com o Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. É uma alternativa ao Desktop Viewer e foi projetado principalmente para computadores Windows reaproveitados e thin clients Windows. O Desktop Lock substitui o shell do Windows e o Gerenciador de Tarefas nesses dispositivos de usuário, impedindo que os usuários acessem os dispositivos subjacentes. Com o Desktop Lock, os usuários podem acessar desktops de Máquina de Servidor Windows e desktops de Máquina de Desktop Windows. A instalação do Desktop Lock é opcional.



Um usuário faz logon em um dispositivo usando um cartão inteligente e PIN. Se o Desktop Lock estiver em execução no dispositivo, ele autentica o usuário em um servidor StoreFront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia um desktop virtual, ele não é solicitado a inserir um PIN novamente porque o recurso de logon único está configurado no Receiver.

Esta implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver do desktop virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para esta segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada apenas no segundo salto.

Autenticação pass-through e logon único com cartões inteligentes

Autenticação pass-through

A autenticação pass-through com cartões inteligentes para desktops virtuais é suportada em dispositivos de usuário que executam Windows 10, Windows 8 e Windows 7 SP1 Enterprise e Professional Editions.

A autenticação pass-through com cartões inteligentes para aplicativos hospedados é suportada em servidores que executam Windows Server 2012 e Windows Server 2008 R2 SP1.

Para usar a autenticação pass-through com aplicativos hospedados por cartões inteligentes, certifique-se de habilitar o uso do Kerberos ao configurar o Pass-through com cartão inteligente como método de autenticação para o site.

Nota: A disponibilidade da autenticação pass-through com cartões inteligentes depende de muitos fatores, incluindo, mas não se limitando a:

- As políticas de segurança da sua organização em relação à autenticação pass-through.
- Tipo e configuração do middleware.
- Tipos de leitores de cartão inteligente.
- Política de cache de PIN do middleware.

A autenticação pass-through com cartões inteligentes é configurada no Citrix StoreFront. Consulte a documentação do StoreFront para obter detalhes.

Logon único

O logon único é um recurso da Citrix que implementa a autenticação pass-through com o lançamento de desktops e aplicativos virtuais. Você pode usar esse recurso em implantações de cartão inteligente ingressadas no domínio, diretas para o StoreFront e ingressadas no domínio, NetScaler para o StoreFront, para reduzir o número de vezes que os usuários inserem seu PIN. Para usar o logon único nesses tipos de implantação, edite os seguintes parâmetros no arquivo default.ica, que está localizado no servidor StoreFront:

- Implantações de cartão inteligente ingressadas no domínio, diretas para o StoreFront — Defina DisableCtrlAltDel como Off
- Implantações de cartão inteligente ingressadas no domínio, NetScaler para o StoreFront — Defina UseLocalUserAndPassword como On

Para mais instruções sobre como definir esses parâmetros, consulte a documentação do StoreFront ou do Citrix Gateway.

A disponibilidade da funcionalidade de logon único depende de muitos fatores, incluindo, mas não se limitando a:

- As políticas de segurança da sua organização em relação ao logon único.
- Tipo e configuração do middleware.
- Tipos de leitores de cartão inteligente.
- Política de cache de PIN do middleware.

> **Observação:**
>
> Quando um usuário faz logon no Virtual Delivery Agent (VDA) em uma máquina com um leitor de cartão inteligente conectado, um bloco do Windows pode aparecer representando o modo de autenticação bem-sucedido anterior, como cartão inteligente ou senha. Como resultado, quando o logon único está ativado, o bloco de logon único pode aparecer. Para fazer logon, o usuário deve selecionar **Trocar Usuários** para selecionar outro bloco, pois o bloco de logon único não funcionará.

Habilitar TLS em Delivery Controllers

Para habilitar o TLS em um delivery controller™, você deve:

- Obtenha, instale e registre um certificado de servidor em todos os Delivery Controllers. Para obter detalhes, consulte Solicitando e instalando um certificado.
- Configure uma porta com o certificado TLS. Para obter detalhes, consulte Solicitando e instalando um certificado.
- Imponha o tráfego HTTPS desabilitando o HTTP. Para obter mais detalhes, consulte Impor tráfego HTTPS apenas.

- Opcionalmente, você pode alterar as portas que o Controller usa para escutar o tráfego HTTP e HTTPS. Para obter mais detalhes, consulte Alterar portas HTTP ou HTTPS.

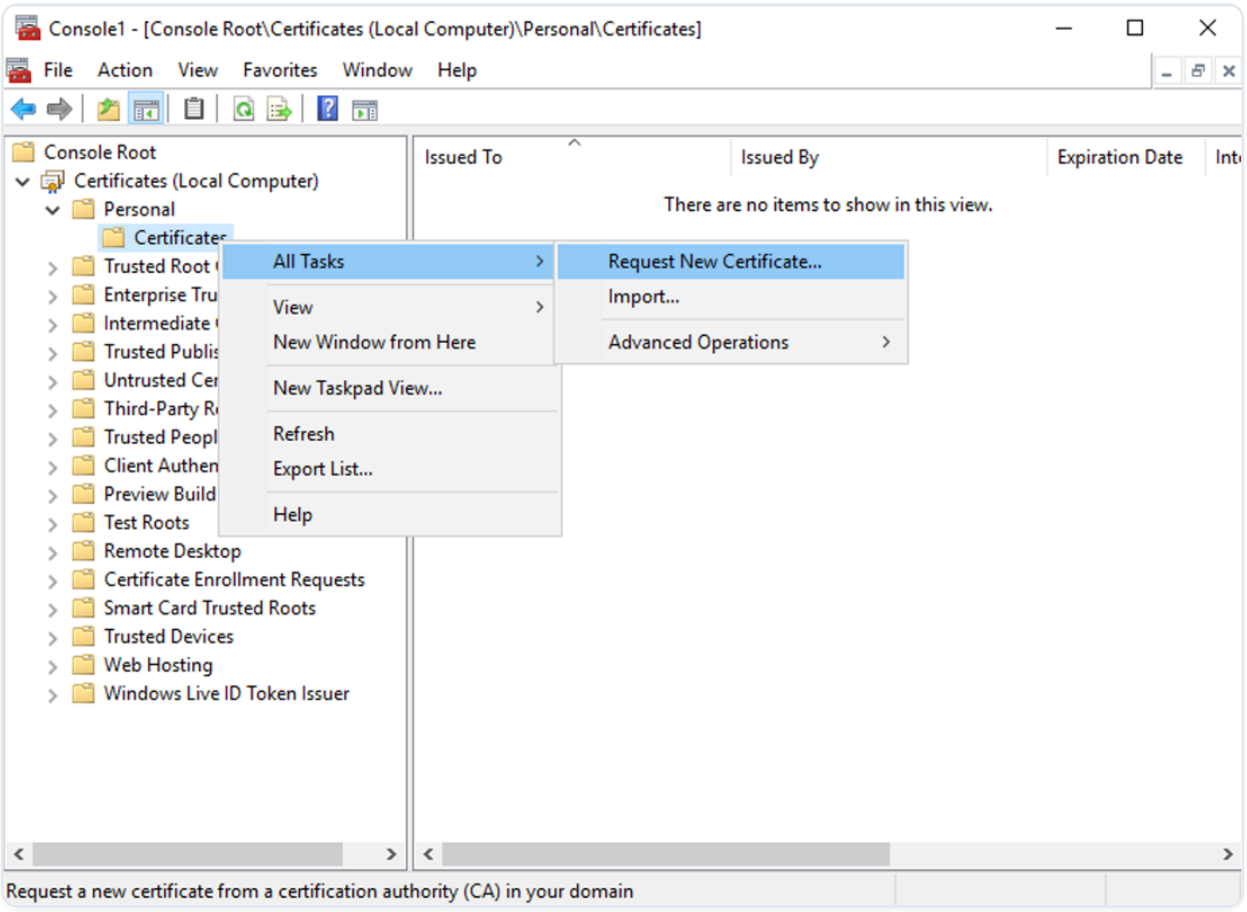
Solicitando e instalando um certificado

Para usar o TLS, você deve instalar um certificado cujo Nome Alternativo inclua o FQDN do DDC. Você deve criar um certificado adequado. Isso pode ser feito usando uma Autoridade de Certificação Microsoft ou outras autoridades de certificação internas ou externas.

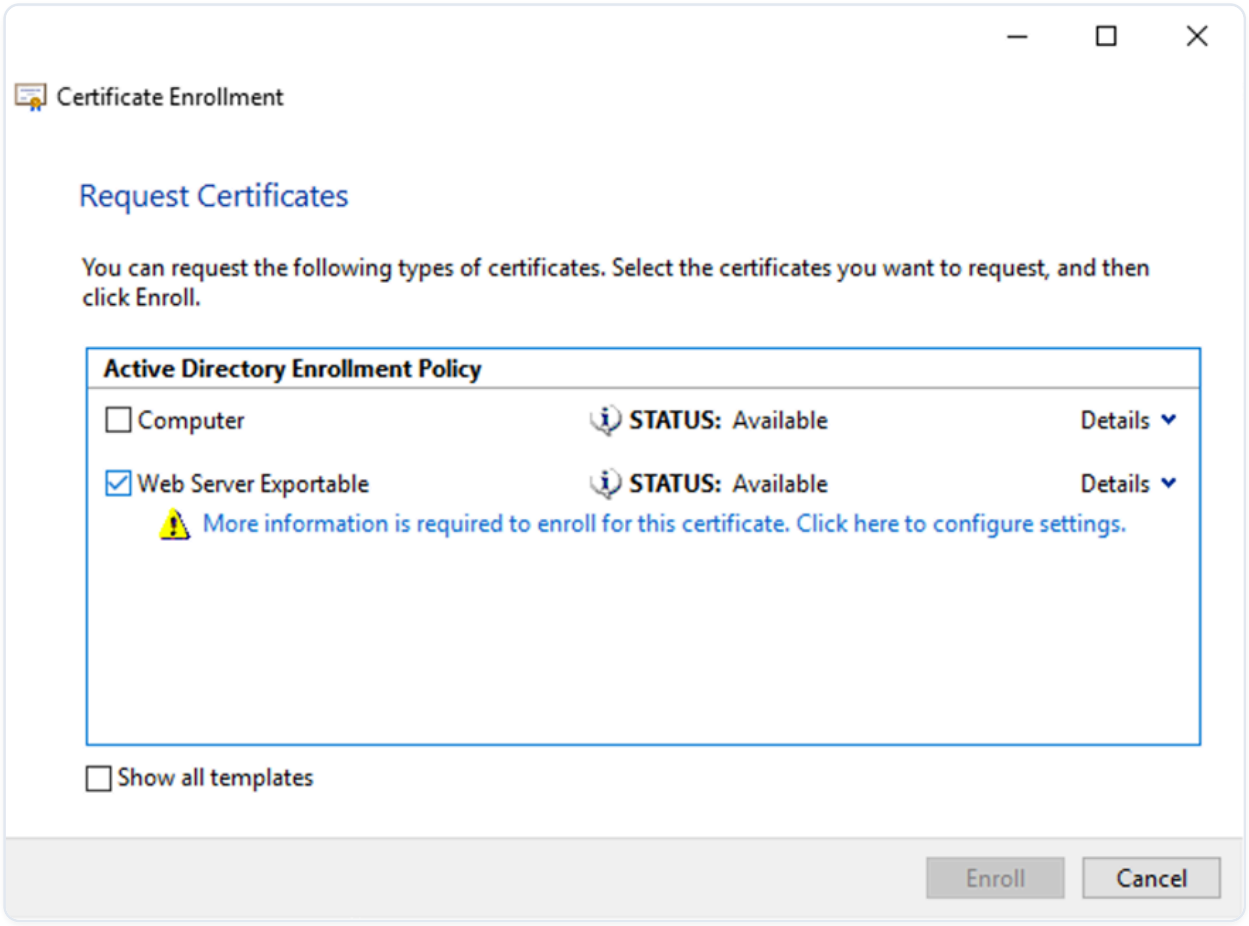
Criar certificado usando a Autoridade de Certificação Microsoft

Se a Autoridade de Certificação Microsoft estiver integrada a um domínio do Active Directory ou à floresta confiável à qual os Delivery Controllers estão unidos, você poderá adquirir um certificado do assistente de Registro de Certificado do snap-in Certificados do MMC. A Autoridade de Certificação Microsoft precisa ter um modelo de certificado publicado adequado para uso por servidores web. Se você estiver usando um Citrix Gateway ou um servidor StoreFront™ em um domínio diferente, será necessário exportar o Certificado da Autoridade de Certificação Raiz e importá-lo para o Citrix Gateway e o StoreFront.

1. No Delivery Controller, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando do menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.



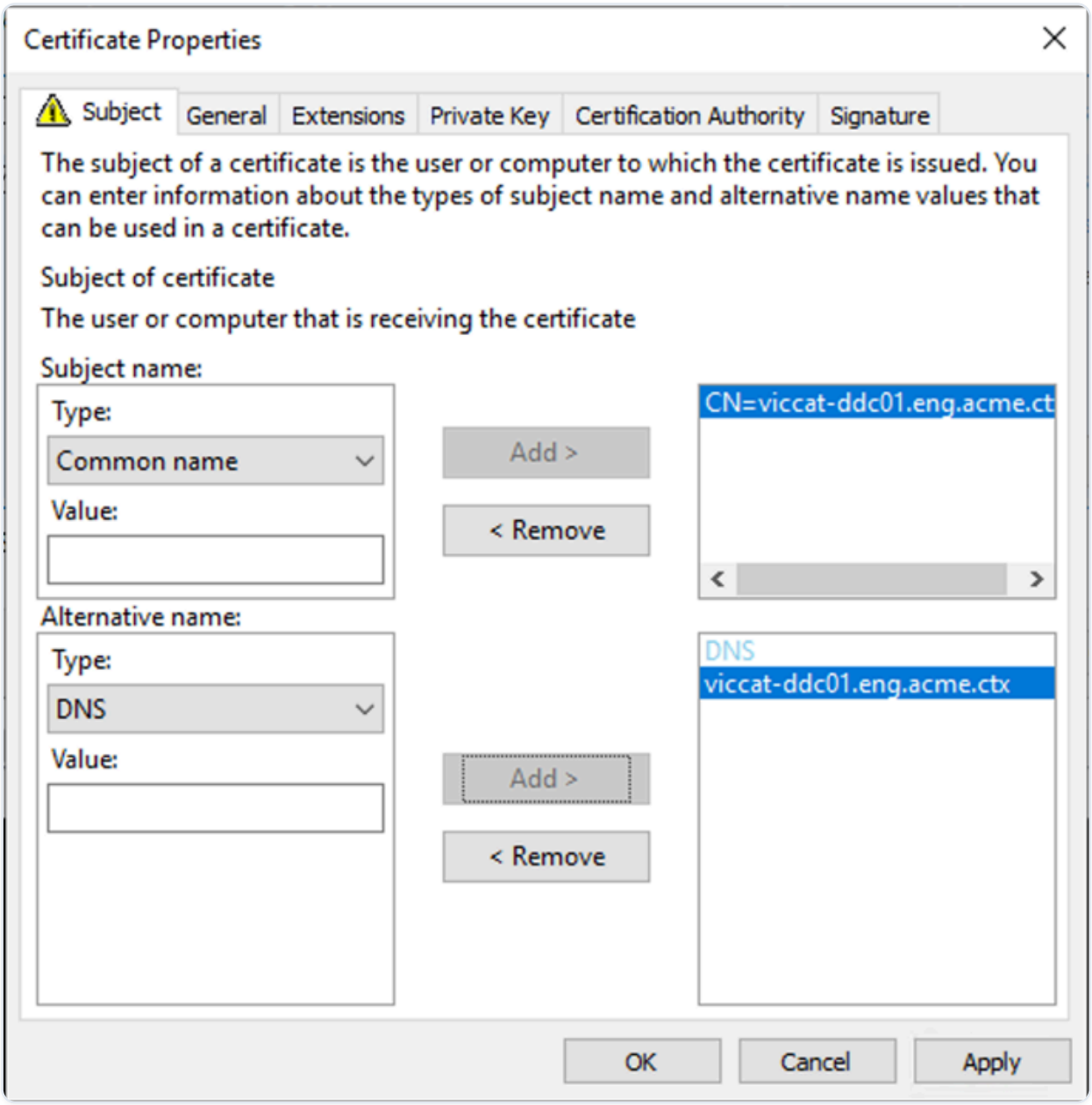
3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.
4. Selecione um modelo adequado, como **Servidor Web Exportável**. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você poderá clicar em **Registrar** sem fornecer mais detalhes.



5. Para fornecer mais detalhes para o modelo de certificado, clique no botão de seta **Detalhes** e configure o seguinte:

   Nome do assunto: selecione Nome Comum e adicione o FQDN do Delivery Controller.

   Nome alternativo: selecione DNS e adicione o FQDN do Delivery Controller.



6. Pressione **OK**.
7. Pressione **Registrar** para criar e instalar o certificado

Instalar arquivo de certificado existente

Se você tiver um certificado existente como um arquivo, poderá instalá-lo:

1. No Delivery Controller, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando de menu de contexto **Todas as Tarefas > Importar**.
3. Procure o arquivo de certificado.

Configurando a porta do ouvinte SSL/TLS

Se o componente IIS do Windows estiver instalado no mesmo servidor, que é instalado como parte do Web Studio e do Director, você pode configurar o TLS usando o IIS. Para obter mais informações, consulte Habilitar TLS no Web Studio e Director. Caso contrário, para configurar o certificado usando o PowerShell:

1. Para verificar se há um certificado existente vinculado, abra um prompt de comando e execute `netsh http show sslcert`:

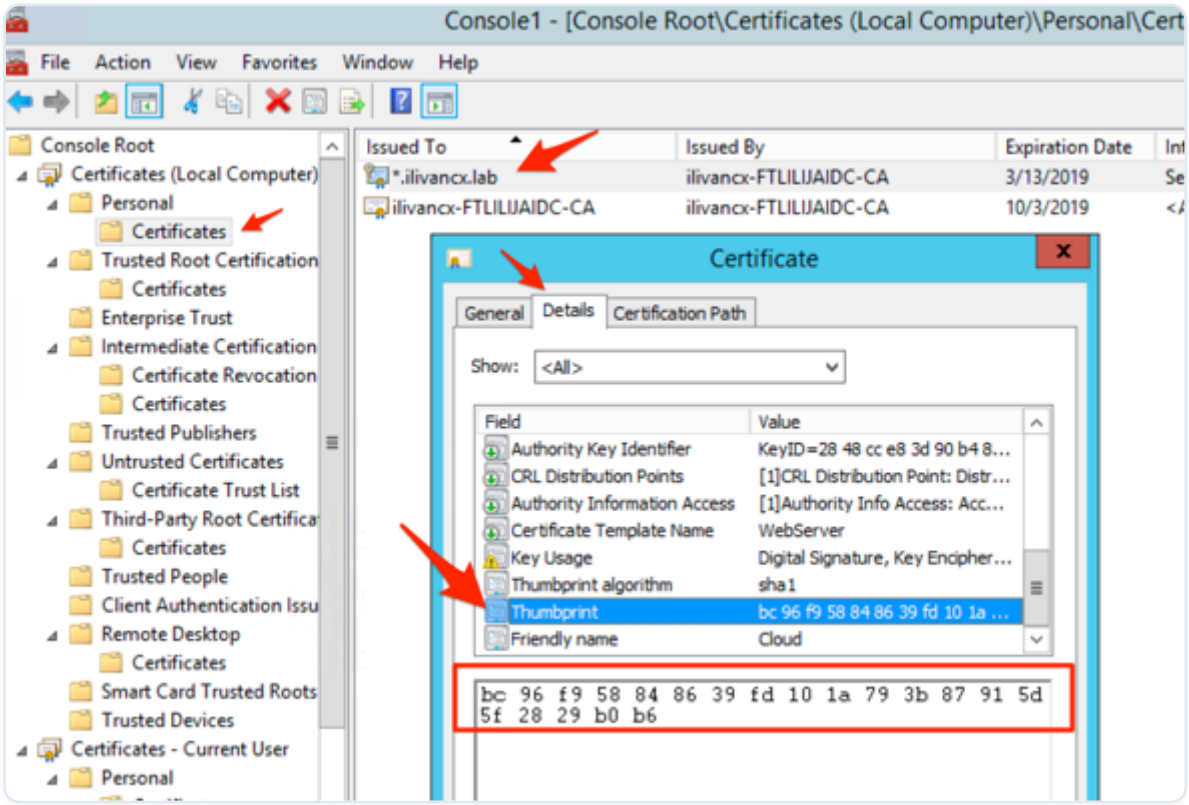
   ```
   netsh http show sslcert
   ```

2. Se houver uma vinculação existente, exclua-a.

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   Substituindo `0.0.0.0:443` por um endereço IP e porta específicos, se houver um especificado na vinculação existente.

3. Encontre a impressão digital do certificado que você instalou anteriormente. Para visualizar a impressão digital, abra **Gerenciar certificados do computador**, navegue até o certificado, abra-o e vá para a guia **Detalhes**.



Alternativamente, você pode usar o PowerShell. Por exemplo, o script a seguir procura um certificado cujo nome comum corresponde ao nome do host do servidor e imprime a miniatura:

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

Se o nome comum do certificado não corresponder aos nomes de host, isso falhará. Se houver vários certificados para o nome do host, isso retornará várias impressões digitais concatenadas e você deverá escolher a impressão digital apropriada.

O exemplo a seguir procura um certificado por nome amigável:

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

Se houver vários certificados com o nome amigável especificado, isso retornará várias impressões digitais concatenadas e você deverá escolher a impressão digital apropriada.

4. Para vincular o certificado à porta, use o comando `netsh http add sslcert`:

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: O endereço IP e a porta. Usar 0.0.0.0:443 aplica isso a todos os endereços IP. Você pode, em vez disso, especificar um endereço IP específico.
- `certhash`: A impressão digital do certificado que você identificou na etapa anterior.
- `appid`: O GUID do Serviço de Broker da Citrix.

> **Observação:**
>
> Ao renovar um certificado ou refazer a vinculação, use o `appid` específico associado ao Serviço de Broker em vez de um GUID arbitrário.
>
> Para encontrar o `appid` correto para o Serviço de Broker da Citrix:

a. Abra uma janela de comando do PowerShell como administrador e execute o seguinte comando:

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. Localize o IdentifyingNumber (GUID) para o Serviço de Broker Citrix na saída (por exemplo, `{D333C884-187F-447C-8C67-463F33989C8F}`). Use este GUID para o parâmetro `appid`.

- `disablelegacytls=enable`: Desativa versões legadas de TLS. Este parâmetro está disponível no Windows 2022 e superior. No Windows 2022, ele desativa o TLS 1.0 e 1.1. No Windows 2025, isso é desnecessário, pois o TLS 1.0 e 1.1 são desativados por padrão.

Por exemplo, execute o seguinte comando para vincular o certificado com a impressão digital `bc96f958848639fd101a793b87915d5f2829b0b6` à porta `443` em todos os endereços IP:

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

Uma vez que o HTTPS esteja habilitado, você deve configurar quaisquer implantações do StoreFront e Netscaler Gateways para usar HTTPS em vez de HTTP para se conectar ao delivery controller.

Configurar conjuntos de cifras

A lista de ordem de conjuntos de cifras deve incluir os conjuntos de cifras `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (ou ambos); e esses conjuntos de cifras devem preceder quaisquer conjuntos de cifras `TLS_DHE_`.

1. Usando o Editor de Política de Grupo da Microsoft, navegue até **Configuração do Computador > Modelos Administrativos > Rede > Configurações de Configuração SSL**.
2. Edite a política "Ordem do Conjunto de Cifras SSL". Por padrão, esta política está definida como "Não Configurado". Defina esta política como Habilitado.
3. Organize os conjuntos na ordem correta; remova quaisquer conjuntos de cifras que você não deseja usar.

Certifique-se de que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` preceda quaisquer conjuntos de cifras `TLS_DHE_`.

No Microsoft Learn, consulte também Configurando a Ordem do Conjunto de Cifras TLS.

Impor apenas tráfego HTTPS

Recomenda-se que você configure o Serviço XML para ignorar o tráfego HTTP.

1. Execute `regedit`
2. Abra HKLM\Software\Citrix\DesktopServer\
3. Crie um novo valor DWORD com o nome `XmlServicesEnableNonSsl` e defina-o como 0.
4. Reinicie o Serviço de Broker.

Existe um valor DWORD de registro correspondente `XmlServicesEnableSsl` que você pode criar para ignorar o tráfego HTTPS. Certifique-se de que não esteja definido como 0.

Alterar portas HTTP ou HTTPS

Por padrão, o Serviço XML no Controller escuta na porta 80 para tráfego HTTP e na porta 443 para tráfego HTTPS. Embora você possa usar portas não padrão, esteja ciente dos riscos de segurança de expor um Controller a redes não confiáveis. A implantação de um servidor StoreFront autônomo é preferível a alterar os padrões.

Para alterar as portas HTTP ou HTTPS padrão usadas pelo Controller, execute o seguinte comando no Studio:

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

onde `<http-port>` é o número da porta para tráfego HTTP e `<https-port>` é o número da porta para tráfego HTTPS.

Observação:

Após alterar uma porta, o Studio pode exibir uma mensagem sobre compatibilidade de licença e atualização. Para resolver o problema, registre novamente as instâncias de serviço usando a seguinte sequência de cmdlets do PowerShell:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Habilitar TLS em VDAs

Habilite as conexões TLS entre o aplicativo Citrix Workspace™ e os Virtual Delivery Agents (VDAs) concluindo as seguintes tarefas:

- Instale certificados nos VDAs. Para obter detalhes, consulte solicitar e instalar um certificado
- Configure o TLS nas máquinas onde os VDAs estão instalados. (Para sua conveniência, referências futuras a máquinas onde os VDAs estão instalados são simplesmente chamadas de "VDAs."). É altamente recomendável que você use o script PowerShell fornecido pela Citrix para configurar TLS/DTLS. Para obter detalhes, consulte Configurar TLS em um VDA usando o script PowerShell. No entanto, se você quiser configurar TLS/DTLS manualmente, consulte Configurar TLS manualmente em um VDA.
- Configure o TLS nos Delivery Groups que contêm os VDAs executando um conjunto de cmdlets PowerShell no Studio. Para obter detalhes, consulte Configurar TLS em Delivery Groups.

Requisitos e considerações:

- Configure o TLS nos Delivery Groups e nos VDAs depois de instalar os componentes, criar um Site, criar catálogos de máquinas e criar Delivery Groups.
- Para configurar o TLS nos Delivery Groups, você deve ter permissão para alterar as regras de acesso do Controller. Um Administrador Completo tem essa permissão.

- Para configurar o TLS nos VDAs, você deve ser um administrador do Windows na máquina onde o VDA está instalado.
- Em VDAs agrupados que são provisionados por Machine Creation Services™ ou Provisioning Services, a imagem da máquina VDA é redefinida na reinicialização, fazendo com que as configurações TLS anteriores sejam perdidas. Execute o script PowerShell cada vez que o VDA for reiniciado para reconfigurar as configurações TLS.

Um Delivery Group não pode ter uma mistura de alguns VDAs com TLS configurado e alguns VDAs sem TLS configurado. Antes de configurar o TLS para um Delivery Group, certifique-se de que você já configurou o TLS para todos os VDAs nesse Delivery Group.

Ao configurar o TLS nos VDAs, as permissões no certificado TLS instalado são alteradas, concedendo ao Serviço ICA® acesso de leitura à chave privada do certificado e informando ao Serviço ICA o seguinte:

- Qual certificado no armazenamento de certificados usar para TLS.
- Qual número de porta TCP usar para conexões TLS.

  O Firewall do Windows (se ativado) deve ser configurado para permitir a conexão de entrada nesta porta TCP. Essa configuração é feita automaticamente para você ao usar o script PowerShell.
- Quais versões do protocolo TLS permitir.

  > **Importante:**
  >
  > A Citrix recomenda usar TLS 1.2 ou superior. SSL e versões mais antigas de TLS estão obsoletas.
  >
  > As versões de protocolo TLS suportadas seguem uma hierarquia (da mais baixa para a mais alta): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3. Especifique a versão mínima permitida; todas as conexões de protocolo usando essa versão ou uma versão superior são permitidas.

  Por exemplo, se você especificar TLS 1.1 como a versão mínima, então as conexões de protocolo TLS 1.1, TLS 1.2 e TLS 1.3 serão permitidas. Se você especificar SSL 3.0 como a versão mínima, então as conexões para todas as versões suportadas serão permitidas. Se você especificar TLS 1.3 como a versão mínima, apenas as conexões TLS 1.3 serão permitidas.

- Quais conjuntos de cifras TLS permitir.

  Um conjunto de cifras seleciona a criptografia usada para uma conexão. Clientes e VDAs podem suportar diferentes conjuntos de cifras. Quando um cliente (aplicativo Citrix Workspace) se conecta e envia uma lista de conjuntos de cifras TLS suportados, o VDA compara um dos conjuntos de cifras do cliente com um dos conjuntos de cifras em sua própria lista de conjuntos de cifras configurados e aceita a conexão. Se não houver um conjunto de cifras correspondente, o VDA rejeita a conexão.

  O VDA suporta três conjuntos de cifras (também conhecidos como modos de conformidade): GOV(erno), COM(ercial) e ALL (todos). Os conjuntos de cifras aceitáveis também dependem do modo FIPS do Windows; consulte `<http://support.microsoft.com/kb/811833>` para obter informações sobre o modo FIPS do Windows. A tabela a seguir lista os conjuntos de cifras em cada conjunto:

CONJUNTO DE CIFRAS	ALL	COM	GOV	ALL	COM	GOV
Modo FIPS	Desativado	Desativado	Desativado	Ativado	Ativado	Ativado
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH	X		X	X		X

CONJUNTO DE CIFRAS	ALL	COM	GOV	ALL	COM	GOV
_AES_256_CBC_SHA384						
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

Observação:

O VDA não oferece suporte a conjuntos de cifras DHE (por exemplo, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 e TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Se selecionado pelo Windows, a conexão falhará.

Se você estiver usando um NetScaler Gateway, consulte a documentação do NetScaler para obter informações sobre o suporte a conjuntos de cifras para comunicação de back-end. Para obter informações sobre o suporte a conjuntos de cifras TLS, consulte Cifras disponíveis nos dispositivos Citrix ADC. Para obter informações sobre o suporte a conjuntos de cifras DTLS, consulte Suporte a cifras DTLS.

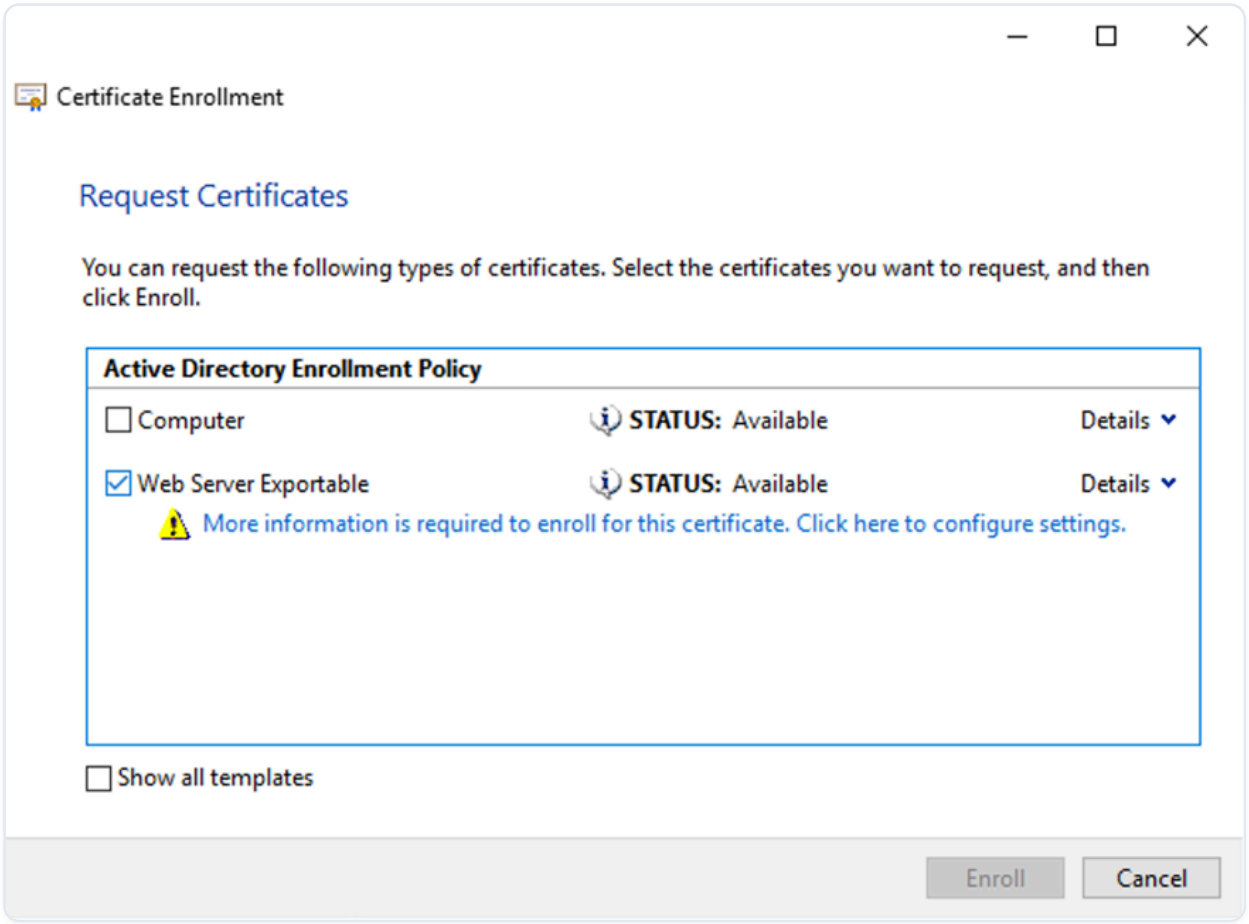
Solicitando e instalando um certificado

Para usar TLS, você deve instalar um certificado cujo Nome Alternativo inclua o FQDN do VDA. O certificado deve ser confiável para quaisquer clientes que se conectem diretamente ao VDA (não via um Citrix Gateway). Para permitir que dispositivos não gerenciados, onde você não pode implantar certificados facilmente, se conectem ao VDA, considere implantar um NetScaler® Gateway.

Criar certificado usando a Autoridade de Certificação Microsoft

Se seus clientes e VDAs estiverem em uma floresta confiável e ela tiver uma Autoridade de Certificação Microsoft, você poderá adquirir um certificado do assistente de Registro de Certificados do snap-in de Certificados do MMC.

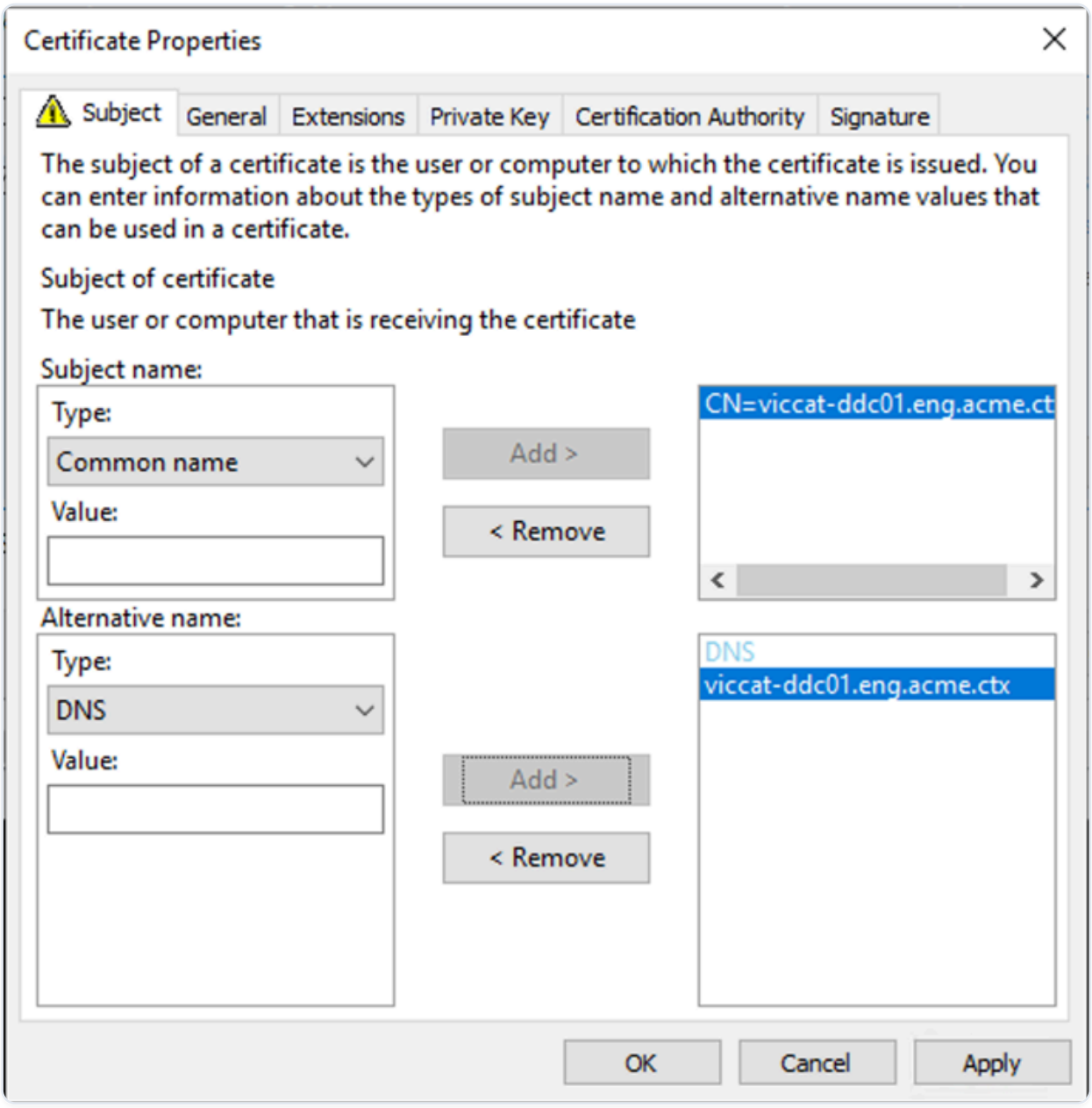
1. No VDA, abra o console MMC e adicione o snap-in Certificados. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificados** e, em seguida, use o comando do menu de contexto **Todas as Tarefas > Solicitar Novo Certificado**.
3. Clique em **Avançar** para começar e em **Avançar** para confirmar que você está adquirindo o certificado do registro do Active Directory.
4. Selecione o modelo para o certificado de Autenticação de Servidor. Tanto o padrão do Windows **Computador** quanto o **Servidor Web Exportável** são aceitáveis. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Assunto, você poderá clicar em **Registrar** sem fornecer mais detalhes.



5. Para fornecer mais detalhes para o modelo de certificado, clique em **Detalhes** e configure o seguinte:

Nome do assunto — selecione o tipo **Nome comum** e adicione o FQDN do VDA

Nome alternativo — selecione o tipo **DNS** e adicione o FQDN do VDA



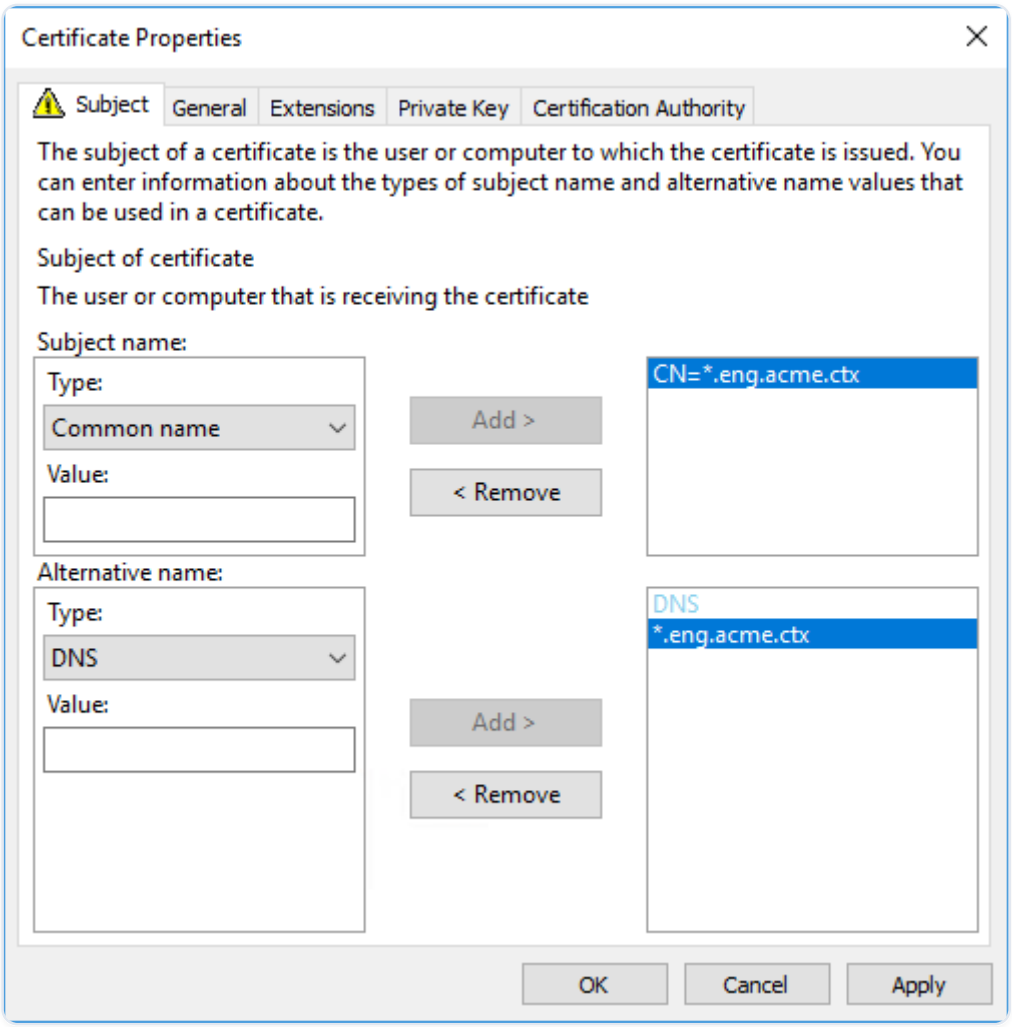
Observação:

Use o Registro Automático de Certificados dos Serviços de Certificados do Active Directory para automatizar a emissão e a implantação de certificados nos VDAs. Isso é descrito em Habilitar o registro automático de certificados).

Você pode usar certificados curinga para permitir que um único certificado proteja vários VDAs:

Nome do assunto — selecione o tipo **Nome comum** e insira o *.primary.domain dos VDAs

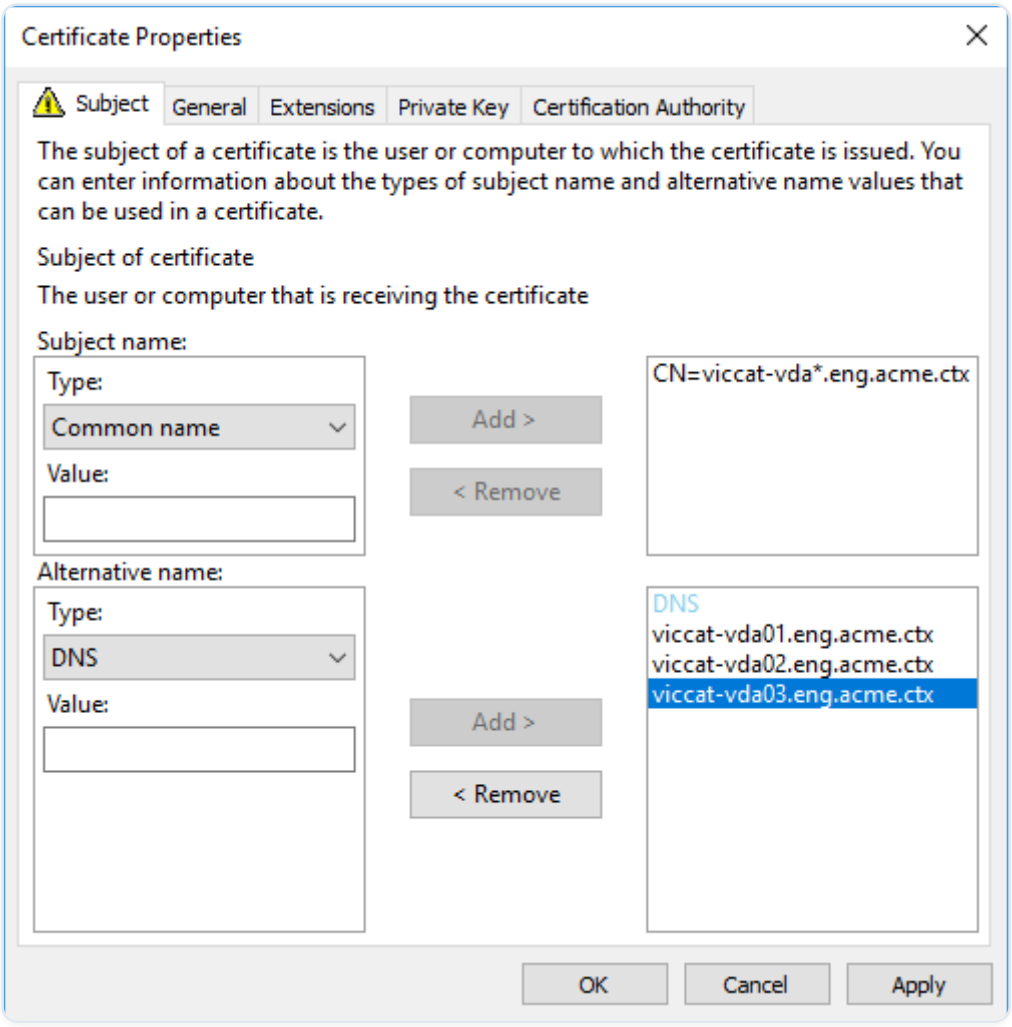
Nome alternativo — selecione o tipo **DNS** e adicione o *.primary.domain dos VDAs



Você pode usar certificados SAN para permitir que um único certificado proteja vários VDAs específicos:

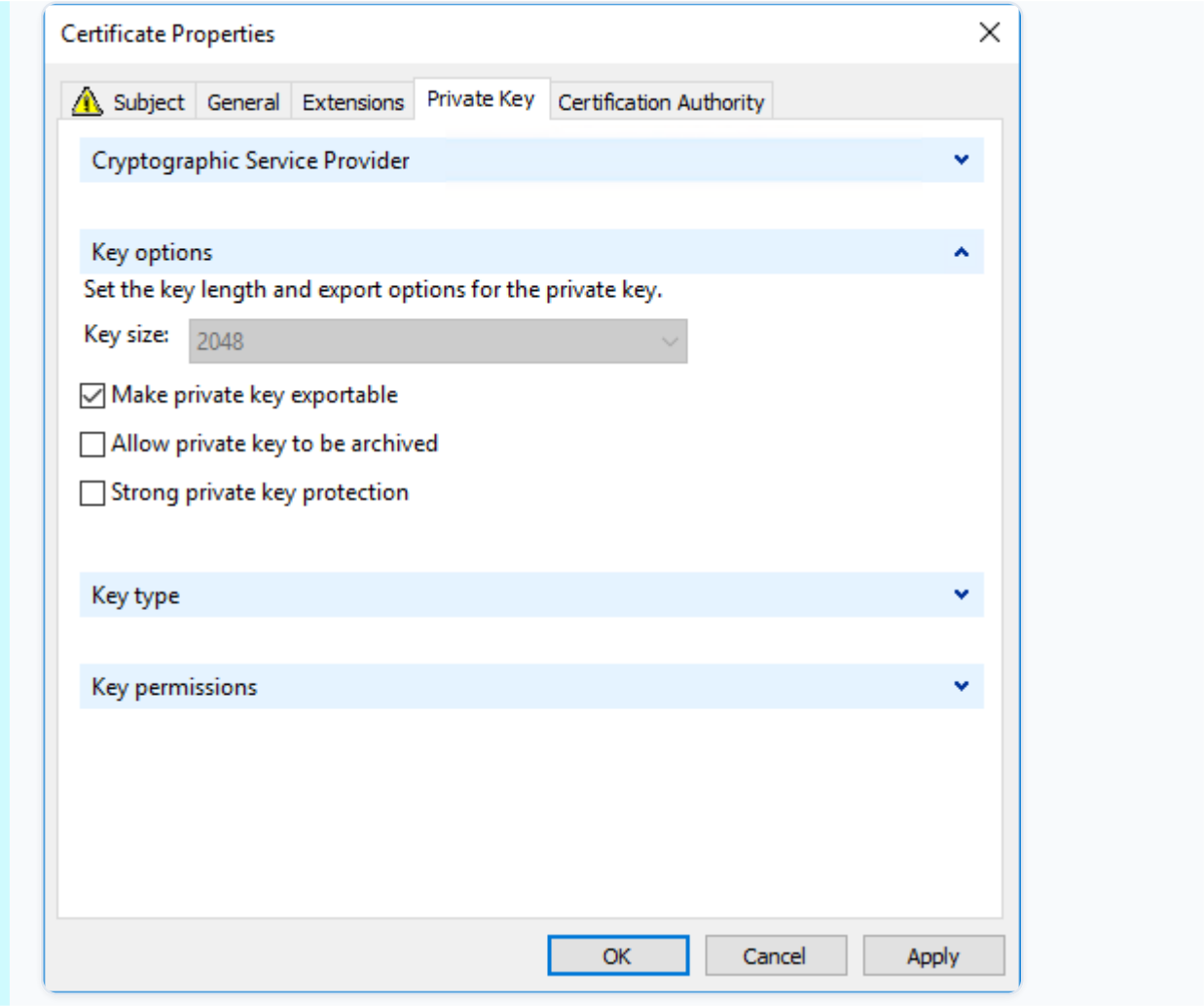
Nome do assunto — selecione o tipo **Nome comum** e insira uma string para ajudar a identificar o uso do certificado

Nome alternativo — selecione o tipo **DNS** e adicione uma entrada para o FQDN de cada VDA. Mantenha o número de Nomes Alternativos no mínimo para garantir uma negociação TLS ideal.



Observação:

Tanto os certificados curinga quanto os SAN exigem que **Tornar a chave privada exportável** na guia Chave Privada esteja selecionada:



Configurar TLS em um VDA usando o script PowerShell

Instale o Certificado TLS na área Computador Local > Pessoal > Certificados do armazenamento de certificados. Se mais de um certificado residir nesse local, forneça a impressão digital do certificado ao script PowerShell.

Observação:

A partir do XenApp e XenDesktop 7.15 LTSR, o script PowerShell encontra o certificado correto com base no FQDN do VDA. Você não precisa fornecer a impressão digital quando apenas um único certificado está presente para o FQDN do VDA.

O script Enable-VdaSSL.ps1 habilita ou desabilita o ouvinte TLS em um VDA. Este script está disponível na pasta *Support* > *Tools* > *SslSupport* na mídia de instalação.

Ao habilitar o TLS, os conjuntos de cifras DHE são desabilitados. Os conjuntos de cifras ECDHE não são afetados.

Ao habilitar o TLS, o script desabilita todas as regras existentes do Firewall do Windows para a porta TCP especificada. Em seguida, ele adiciona uma nova regra que permite que o Serviço ICA aceite conexões de entrada apenas nas portas TCP e UDP TLS. Ele também desabilita as regras do Firewall do Windows para:

- Citrix ICA (padrão: 1494)
- Citrix CGP (padrão: 2598)
- Citrix WebSocket (padrão: 8008)

O efeito é que os usuários só podem se conectar usando TLS ou DTLS. Eles não podem usar ICA/HDX, ICA/HDX com Confiabilidade de Sessão, ou HDX sobre WebSocket, sem TLS ou DTLS.

> **Observação:**
>
> DTLS não é suportado com Áudio ICA/HDX sobre Transporte UDP em Tempo Real, ou com ICA/HDX Framehawk.

> Consulte Portas de rede.

O script contém as seguintes descrições de sintaxe, além de exemplos extras; você pode usar uma ferramenta como o Notepad++ para revisar essas informações.

> **Importante:**
>
> Especifique o parâmetro Enable ou Disable, e o parâmetro CertificateThumbPrint. Os outros parâmetros são opcionais.

Sintaxe

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

PARÂMETRO	DESCRIÇÃO
Enable	Instala e habilita o ouvinte TLS no VDA. Este parâmetro ou o parâmetro Disable é obrigatório.
Disable	Desabilita o ouvinte TLS no VDA. Este parâmetro ou o parâmetro Enable é obrigatório. Se você especificar este parâmetro, nenhum outro parâmetro será válido.
Impressão digital do certificado "<thumbprint>"	Impressão digital do certificado TLS no armazenamento de certificados, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar. Se este parâmetro for omitido, um certificado incorreto será selecionado.
Porta SSL <port>	Porta TLS. Padrão: 443
SSLMinVersion "<versão>"	Versão mínima do protocolo TLS, entre aspas. Valores válidos: `SSL_3.0`, `TLS_1.0` (padrão), `TLS_1.1`, `TLS_1.2` e `TLS_1.3`. `TLS_1.3` requer Windows 11 ou Windows Server 2022 ou superior.
SSLCipherSuite "<conjunto>"	Conjunto de cifras TLS, entre aspas. Valores válidos: "GOV", "COM" e "ALL" (padrão).

Exemplos

O script a seguir instala e habilita o valor da versão do protocolo TLS. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

O script a seguir instala e habilita o ouvinte TLS e especifica a porta TLS 400, o conjunto de cifras GOV e um valor mínimo de protocolo TLS 1.2. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

O script a seguir desabilita o ouvinte TLS no VDA.

```
Enable-VdaSSL -Disable
```

Configurar o TLS manualmente em um VDA

Ao configurar o TLS em um VDA manualmente, você concede acesso de leitura genérico à chave privada do certificado TLS para o serviço apropriado em cada VDA: NT SERVICE\PorticaService para um VDA para SO de sessão única do Windows, ou NT SERVICE\TermService para um VDA para SO de múltiplas sessões do Windows. Na máquina onde o VDA está instalado:

ETAPA 1. Inicie o console de gerenciamento da Microsoft (MMC): Iniciar > Executar > mmc.exe.

ETAPA 2. Adicione o snap-in Certificados ao MMC:

1. Selecione Arquivo > Adicionar/Remover Snap-in.
2. Selecione Certificados e clique em Adicionar.
3. Quando solicitado com "Este snap-in sempre gerenciará certificados para:", escolha "Conta de computador" e clique em Avançar.
4. Quando solicitado com "Selecione o computador que você deseja que este snap-in gerencie", escolha "Computador local" e clique em Concluir.

PASSO 3. Em Certificados (Computador Local) > Pessoal > Certificados, clique com o botão direito do mouse no certificado e selecione Todas as Tarefas > Gerenciar Chaves Privadas.

PASSO 4. O Editor da Lista de Controle de Acesso exibe "Permissões para chaves privadas (FriendlyName)" onde (FriendlyName) é o nome do seu certificado TLS. Adicione um dos seguintes serviços e conceda a ele acesso de Leitura:

- Para um VDA para SO de sessão única do Windows, "PORTICASERVICE"
- Para um VDA para SO de múltiplas sessões do Windows, "TERMSERVICE"

PASSO 5. Clique duas vezes no certificado TLS instalado. Na caixa de diálogo do certificado, selecione a guia Detalhes e role até o final. Clique em Impressão digital.

PASSO 6. Execute o regedit e vá para HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Edite a chave SSL Thumbprint e copie o valor da impressão digital do certificado TLS para este valor binário. Você pode ignorar com segurança itens desconhecidos na caixa de diálogo Editar Valor Binário (como '0000' e caracteres especiais).
2. Edite a chave SSLEnabled e altere o valor DWORD para 1. (Para desabilitar o SSL posteriormente, altere o valor DWORD para 0.)
3. Se você quiser alterar as configurações padrão (opcional), use o seguinte no mesmo caminho do registro:

   SSLPort DWORD – Número da porta SSL. Padrão: 443.

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3. Padrão: 2 (TLS 1.0).

   SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Padrão: 3 (TODOS).

PASSO 7. Certifique-se de que as portas TCP e UDP TLS estejam abertas no Firewall do Windows, caso não sejam a porta padrão 443. (Ao criar a regra de entrada no Firewall do Windows, certifique-se de que suas propriedades tenham as entradas "Permitir a conexão" e "Ativado" selecionadas.)

PASSO 8. Certifique-se de que nenhum outro aplicativo ou serviço (como o IIS) esteja usando a porta TCP TLS.

PASSO 9. Para VDAs de múltiplas sessões, reinicie a máquina para que as alterações entrem em vigor. (Você não precisa reiniciar máquinas VDA de sessão única.)

PASSO 10. Modifique a preferência da suíte de cifras do Windows para que as suítes de cifras compatíveis com o VDA tenham a mais alta prioridade, a fim de evitar problemas de conexão.

> **Importante:**
>
> As alterações da Política de Grupo descritas abaixo só entram em vigor após a reinicialização do sistema.

Se você estiver usando hosts de sessão não persistentes provisionados com MCS ou PVS, deverá aplicar essas configurações na imagem mestre.

Opção 1:

Usando o Editor de Política de Grupo, vá para Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order. Certifique-se de que as seguintes suítes de cifras estejam no topo da lista:

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

Observação:

TLS_AES_256_GCM_SHA384 e TLS_AES_128_GCM_SHA256 se aplicam apenas ao Windows 11 e Windows Server 2022 ou mais recentes. Se você estiver usando sistemas operacionais mais antigos, não inclua essas suítes de cifras em sua lista.

Observe que as suítes de cifras listadas também especificam a curva elíptica, P384 ou P256, para garantir que “curve25519” não seja selecionada. O Modo FIPS não impede o uso de “curve25519”.

> Não é necessário remover nenhuma suíte de cifras da lista. Observe que essas configurações se aplicam a todo o sistema, portanto, se você decidir remover alguma suíte de cifras, deve garantir que elas não sejam exigidas por nenhum aplicativo ou serviço em execução em seus hosts de sessão.

> Opção 2:

Usando o Editor de Política de Grupo, vá para Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > SSL Cipher Suite Order. Certifique-se de que as seguintes suítes de cifras estejam no topo da lista:

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

> **Nota:** TLS_AES_256_GCM_SHA384 e TLS_AES_128_GCM_SHA256 se aplicam apenas ao Windows 11 e Windows Server 2022, ou mais recentes. Se você estiver usando sistemas operacionais mais antigos, não inclua essas suítes de cifras em sua lista.

> Não é necessário remover nenhuma suíte de cifras da lista. Observe que essas configurações se aplicam a todo o sistema, portanto, se você decidir remover alguma suíte de cifras, deve garantir que elas não sejam exigidas por nenhum aplicativo ou serviço em execução em seus hosts de sessão.

> Usando o Editor de Política de Grupo, vá para Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings > ECC Curve Order. Habilite a configuração e inclua as seguintes curvas na lista:

```
NistP384

NistP256
```

Observação:

Isso garante que “curve25519” não seja selecionada. O Modo FIPS não impede o uso de “curve25519”.

O VDA seleciona uma suíte de cifras somente se ela aparecer em ambas as listas: a lista da Política de Grupo e a lista para o modo de conformidade selecionado (COM, GOV ou ALL). A suíte de cifras também deve aparecer na lista enviada pelo cliente (aplicativo Citrix Workspace).

Configurar TLS em Grupos de Entrega

Conclua este procedimento para cada Grupo de Entrega que contém VDAs que você configurou para conexões TLS.

1. No Studio, abra o console do PowerShell.
2. Execute **asnp Citrix.*** para carregar os cmdlets do produto Citrix.
3. Execute **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Execute **Set-BrokerSite -DnsResolutionEnabled $true**.

Habilitando SSL para VDAs Agrupados usando Registro Automático

Ao usar VDAs agrupados, se você adicionar um certificado à imagem mestre, todos os VDAs compartilharão a mesma imagem. Você pode usar um certificado curinga, mas uma desvantagem é que, se qualquer um dos VDAs for comprometido, este certificado todo-poderoso significaria que as conexões HDX™ pertencentes a todos os VDAs estariam em risco.

Em vez disso, uma alternativa segura é aproveitar os Serviços de Certificados do Microsoft Active Directory para provisionar certificados automaticamente usando a política de grupo. Você pode usar um script de inicialização no VDA para provisionar dinamicamente um novo certificado e habilitar SSL para o VDA.

Observe que essa abordagem funcionará apenas para VDAs de Desktop de sessão única. Para VDAs de várias sessões, o listener ICA é iniciado muito cedo durante o processo de inicialização, antes que os certificados possam ser provisionados automaticamente.

Como os Serviços de Certificados do Active Directory usam uma Autoridade de Certificação (CA) Corporativa interna, ela não será automaticamente confiável por todas as instalações do Windows. Se os clientes forem gerenciados pela corporação e fizerem parte de uma floresta de domínio, os certificados de CA confiáveis poderão ser distribuídos automaticamente usando a política de grupo. Para BYOD e outros dispositivos não associados ao domínio, você precisa distribuir os certificados de CA confiáveis aos seus usuários por algum outro mecanismo (como oferecer um link de download) ou usar um gateway NetScaler.

Habilitar o Registro Automático de Certificados

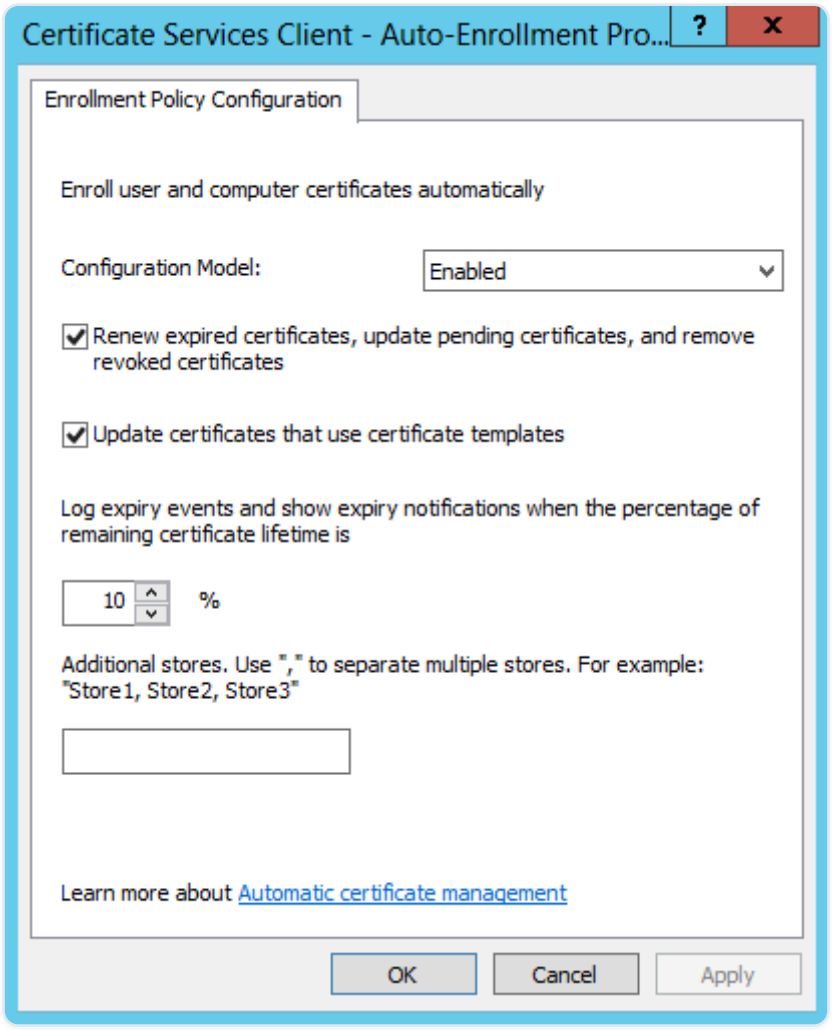
Primeiro, certifique-se de ter a função de Serviços de Certificados do Active Directory instalada em um servidor em sua floresta de domínio VDA, fornecendo uma CA Corporativa, caso contrário, o registro automático não será possível.

Observe que isso pode gerar uma carga consideravelmente maior do que o normal em sua CA Corporativa, já que os VDAs enviarão uma solicitação de certificado a cada inicialização. Certifique-se de alocar CPU e memória suficientes no servidor CA para lidar com a carga e, como sempre, teste a escalabilidade da implantação em um ambiente de laboratório antes de passar para a produção.

No Editor de Gerenciamento de Política de Grupo, crie uma nova política que se aplique à Unidade Organizacional que conterá seus VDAs agrupados com SSL habilitado, da seguinte forma:

1. Expandir Configuração do Computador -> Políticas -> Configurações do Windows -> Configurações de Segurança -> Políticas de Chave Pública
2. Editar as propriedades do objeto ‘Cliente de Serviços de Certificado – Política de Registro Automático’
3. Configurar conforme mostrado na captura de tela abaixo.
4. Clique com o botão direito do mouse no contêiner Solicitação de Certificado Automático e selecione Novo -> Solicitação de Certificado Automático...
5. No Assistente de Configuração de Solicitação de Certificado Automático, clique em Avançar
6. Certifique-se de que o modelo de certificado de Computador esteja selecionado, clique em Avançar

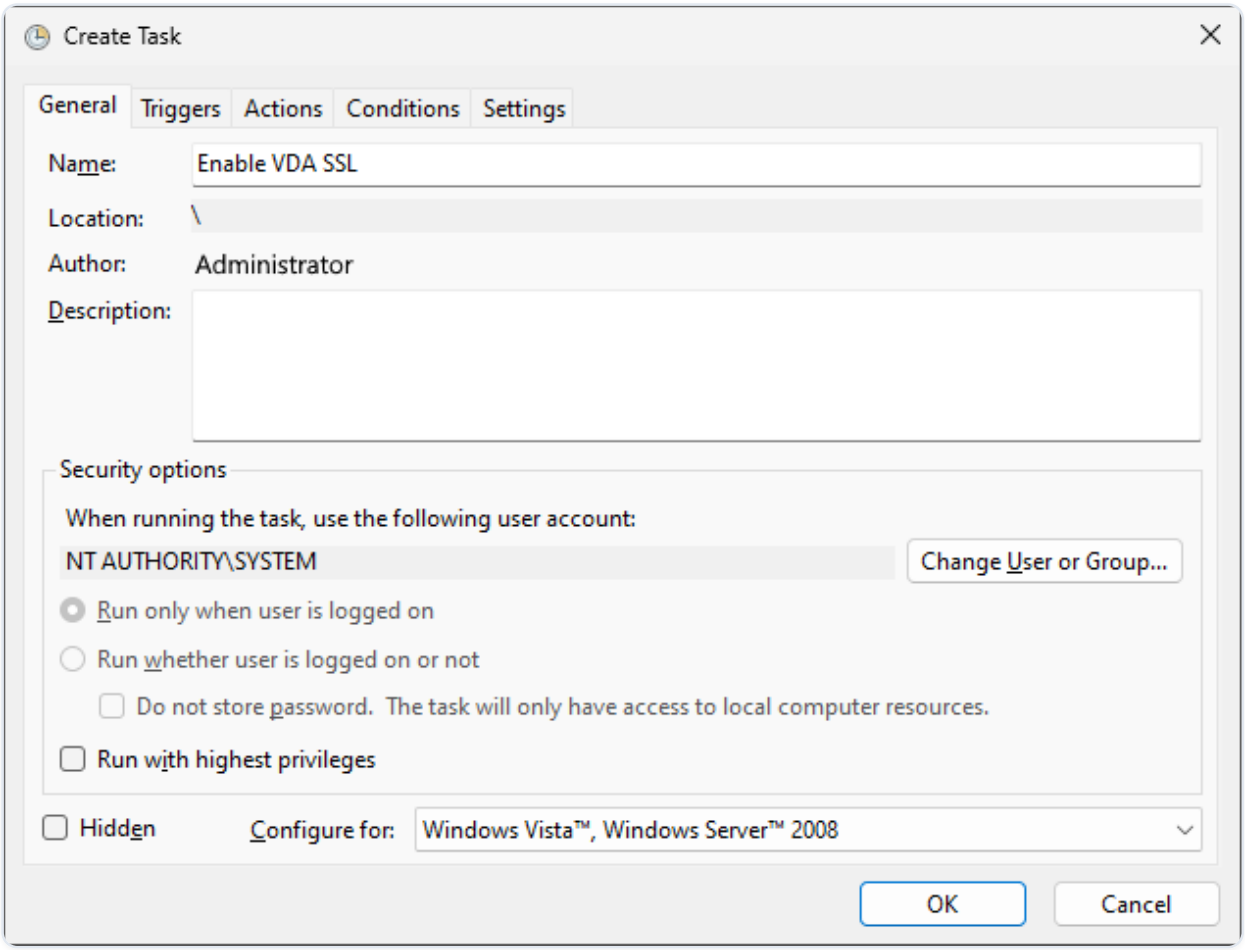
7. Clique em Concluir



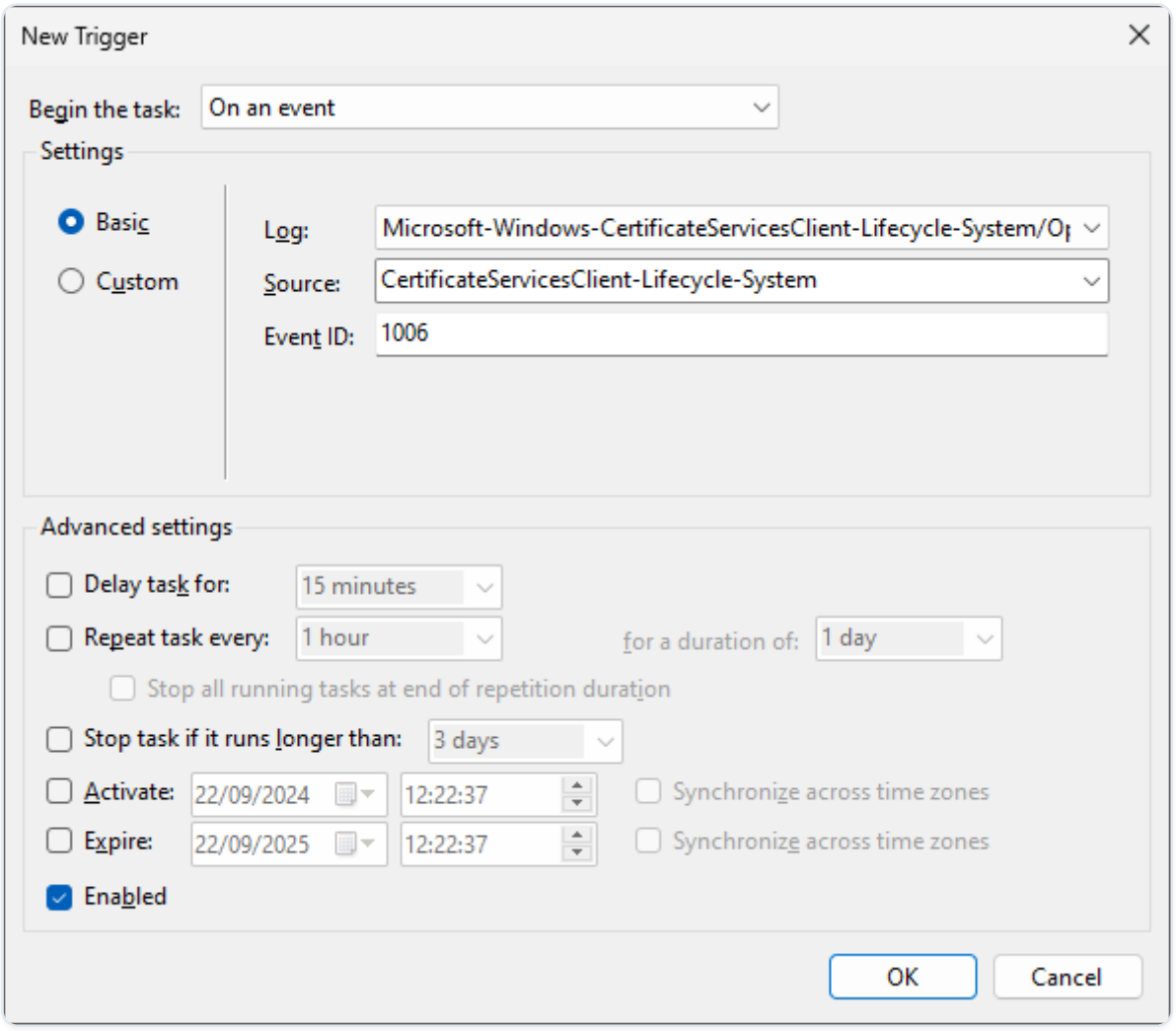
Preparando a Imagem Mestra do Windows

Copie o script Enable-VdaSsl.ps1 da mídia de instalação do produto na pasta `Support\Tools\SslSupport` para a imagem mestra do VDA. Observe que a imagem mestra não deve conter nenhum certificado a ser usado para conexões HDX SSL. Os certificados serão provisionados quando o catálogo de máquinas MCS ou PVS for criado. Agora crie uma nova tarefa agendada da seguinte forma (não execute a tarefa agendada agora):

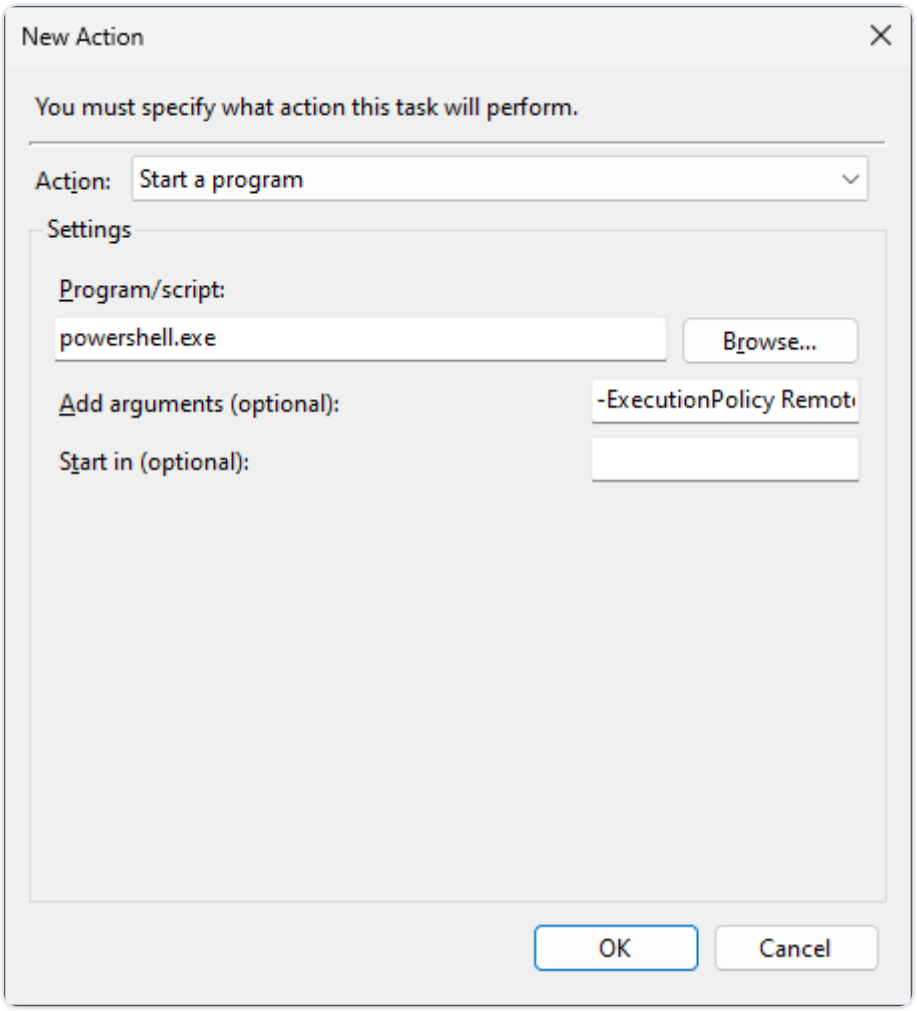
1. Abra o Agendador de Tarefas.
2. No painel **Ações**, pressione **Criar Tarefa...**
3. Na guia geral:
    - Insira um **Nome** como `Enable VDA SSL`
    - Clique em **Alterar Usuário ou Grupo...** e na caixa de diálogo Selecionar Usuário ou Grupo insira `SYSTEM` e clique em **OK**



4. Selecione a guia Acionadores
5. Clique em **Novo…**. Na caixa de diálogo **Novo Acionador**:
    a. Defina **Iniciar a tarefa** como **Em um evento**
    b. Defina **Log** como **Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**
    c. Defina **Origem** como **Microsoft-Windows-CertificateServicesClient-Lifecycle-System**
    d. Defina **ID do Evento** como `1006`
    e. Clique em **OK** para salvar o acionador



6. Selecione a guia **Ações**
7. Clique em **Novo…**
8. Na caixa de diálogo **Nova Ação**:
    a. Defina **Ação** como **Iniciar um programa**
    b. No campo Programa/script, insira `powershell.exe`
    c. No campo Adicionar argumentos, insira `-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`, incluindo o caminho para o script do PowerShell.
    d. Pressione **OK** para salvar a ação



9. Pressione **OK** para salvar a tarefa

Solução de problemas

Se ocorrer um erro de conexão, verifique o log de eventos do sistema no VDA.

Ao usar o Citrix Workspace app para Windows, se você receber um erro de conexão que indica um erro de TLS, desative o Desktop Viewer e tente conectar novamente. Embora a conexão ainda falhe, uma explicação do problema de TLS subjacente pode ser fornecida. Por exemplo, você especificou um modelo incorreto ao solicitar um certificado da autoridade de certificação.)

A maioria das configurações que usam o HDX Adaptive Transport funciona com sucesso com DTLS, incluindo aquelas que usam as versões mais recentes do Citrix Workspace app, Citrix Gateway e VDA. Algumas configurações que usam DTLS entre o Citrix Workspace app e o Citrix Gateway, e que usam DTLS entre o Citrix Gateway e o VDA, exigem ação adicional.

Ação adicional é necessária se:

- a versão do Citrix Receiver suporta HDX Adaptive Transport e DTLS: Receiver para Windows (4.7, 4.8, 4.9), Receiver para Mac (12.5, 12.6, 12.7), Receiver para iOS (7.2, 7.3.x) ou Receiver para Linux (13.7)

e qualquer um dos seguintes também se aplica:

- a versão do Citrix Gateway suporta DTLS para o VDA, mas a versão do VDA não suporta DTLS (versão 7.15 ou anterior),
- a versão do VDA suporta DTLS (versão 7.16 ou posterior), mas a versão do Citrix Gateway não suporta DTLS para o VDA.

Para evitar que as conexões do Citrix Receiver™ falhem, faça uma das seguintes ações:

- atualize o Citrix Receiver para a versão 4.10 ou posterior do Receiver para Windows, 12.8 ou posterior do Receiver para Mac, ou 7.5 ou posterior do Receiver para iOS; ou,
- atualize o Citrix Gateway para uma versão que suporte DTLS para o VDA; ou,
- atualize o VDA para a versão 7.16 ou posterior; ou,
- desabilitar DTLS no VDA; ou,
- desabilitar o Transporte Adaptável HDX.

> **Observação:**
>
> Uma atualização adequada para o Receiver para Linux ainda não está disponível. O Receiver para Android (versão 3.12.3) não oferece suporte ao Transporte Adaptável HDX e DTLS via Citrix Gateway e, portanto, não é afetado.

> Para desabilitar o DTLS no VDA, modifique a configuração do firewall do VDA para desabilitar a porta UDP 443. Consulte Portas de rede.

Redirecionamento de vídeo TLS e HTML5 e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX em execução no VDA. Para conseguir isso, o Serviço de Redirecionamento de Vídeo HTML5 gera

dois certificados personalizados no armazenamento de certificados no VDA. Parar o serviço remove os certificados.

A política de redirecionamento de vídeo HTML5 está desabilitada por padrão.

O redirecionamento de conteúdo do navegador está habilitado por padrão.

Para obter mais informações sobre o redirecionamento de vídeo HTML5, consulte Configurações de política de multimídia.

Habilitar TLS no Universal Print Server

O protocolo TLS (Transport Layer Security) é compatível com conexões baseadas em TCP entre o Virtual Delivery Agent (VDA) e o Universal Print Server.

> **Aviso:**
>
> Para tarefas que incluem trabalhar no registro do Windows — editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Tipos de conexões de impressão entre o VDA e o Universal Print Server

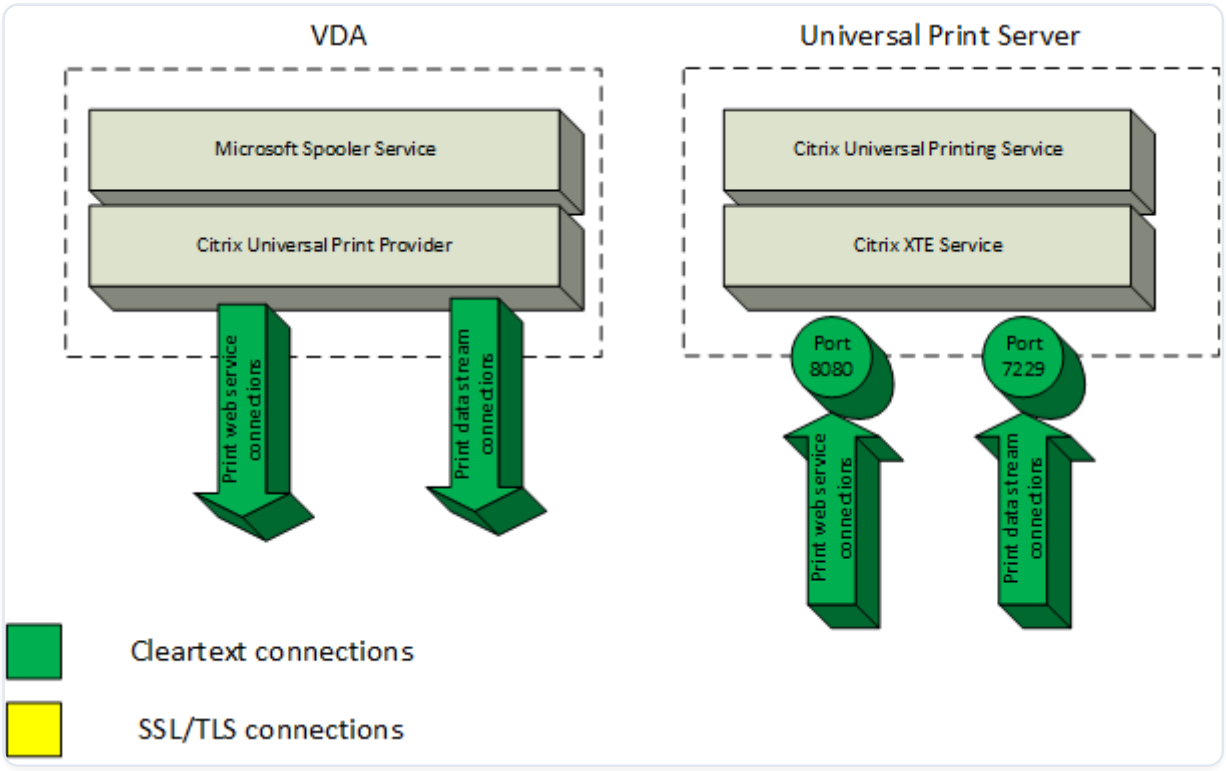
Conexões de texto simples

As seguintes conexões relacionadas à impressão se originam do VDA e se conectam a portas no Universal Print Server. Essas conexões são feitas somente quando a configuração de política **SSL enabled** está definida como **Disabled** (o padrão).

- Conexões de serviço web de impressão de texto simples (porta TCP 8080)
- Conexões de fluxo de dados de impressão de texto simples (CGP) (porta TCP 7229)

O artigo de suporte da Microsoft (https://support.microsoft.com/pt-br/help/832017/service-overview-and-network-port-requirements-for-windows) descreve as portas usadas pelo Serviço de Spooler de Impressão do Microsoft Windows. As configurações de SSL/TLS neste documento não se aplicam às conexões NetBIOS e RPC feitas pelo serviço de Spooler de Impressão do Windows. O VDA usa o Provedor de Impressão de Rede do Windows (win32spl.dll) como fallback

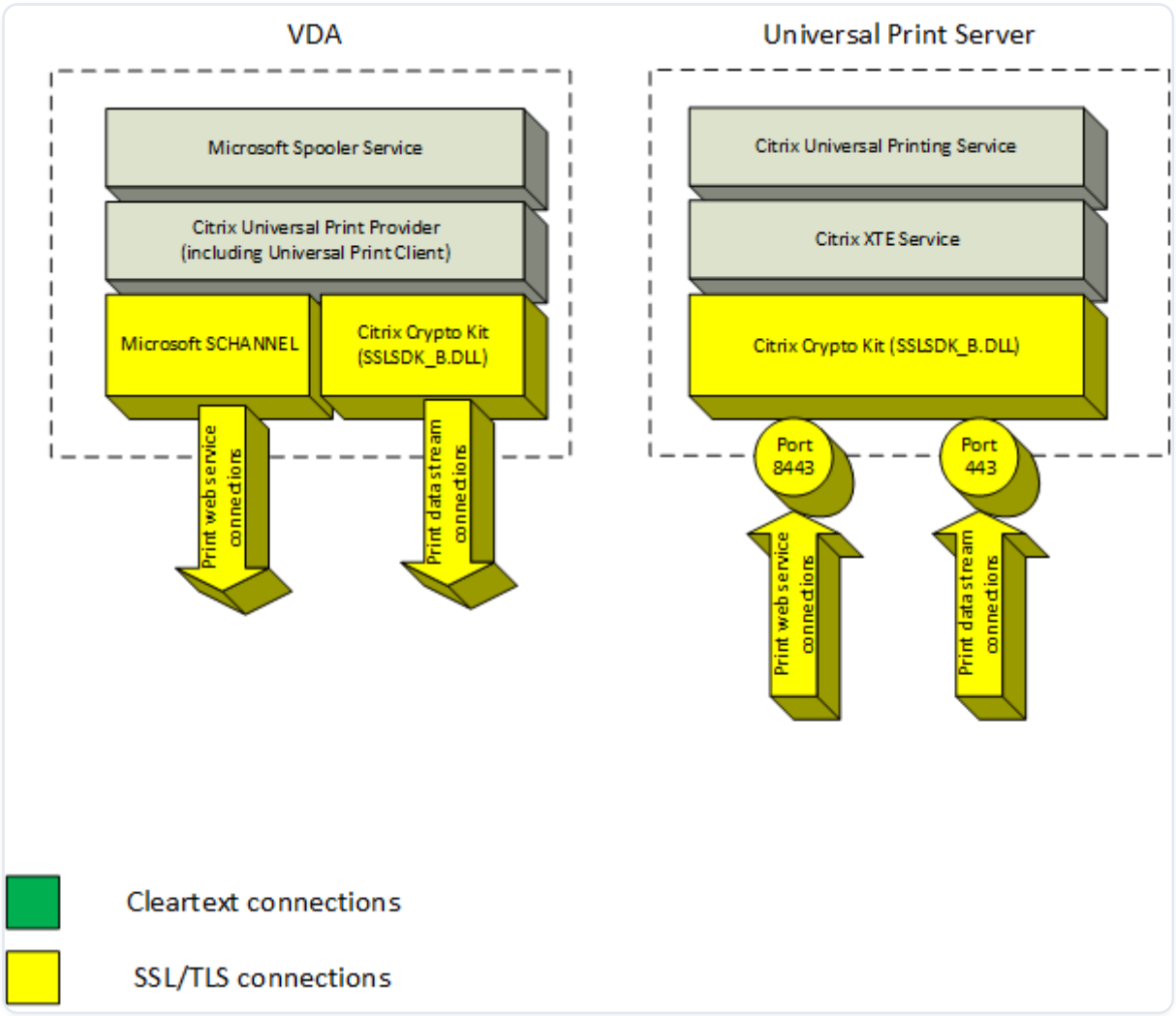
se a configuração de política **Universal Print Server enable** estiver definida como **Enabled with fallback to Windows' native remote printing**.



Conexões criptografadas

Essas conexões SSL/TLS relacionadas à impressão se originam do VDA e se conectam a portas no Universal Print Server. Essas conexões são feitas somente quando a configuração de política **SSL enabled** está definida como **Enabled**.

- Conexões de serviço web de impressão criptografadas (porta TCP 8443)
- Conexões de fluxo de dados de impressão criptografadas (CGP) (porta TCP 443)



Configuração do cliente SSL/TLS

O VDA funciona como o cliente SSL/TLS.

Use a Política de Grupo da Microsoft e o registro para configurar o Microsoft SCHANNEL SSP para conexões de serviço web de impressão criptografadas (porta TCP 8443). O artigo de suporte da Microsoft Configurações de Registro TLS descreve as configurações de registro para o Microsoft SCHANNEL SSP.

Usando o Editor de Política de Grupo no VDA, vá para **Configuração do Computador > Modelos Administrativos > Rede > Configurações de Configuração SSL > Ordem do Conjunto de Cifras SSL**. Selecione a seguinte ordem quando o TLS 1.3 estiver definido:

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

Selecione a seguinte ordem quando o TLS 1.2 estiver definido:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

Observação:

Quando esta configuração de Política de Grupo é configurada, o VDA seleciona um conjunto de cifras para conexões de serviço web de impressão criptografadas (porta padrão: 8443) somente se as conexões aparecerem em ambas as listas de conjuntos de cifras SSL:

- Lista de ordem do conjunto de cifras SSL da Política de Grupo
- Lista correspondente à configuração de política de Conjunto de Cifras SSL selecionada (COM, GOV ou ALL)

Esta configuração de Política de Grupo também afeta outros aplicativos e serviços TLS no VDA. Se seus aplicativos exigirem conjuntos de cifras específicos, talvez seja necessário adicioná-los a esta lista de Ordem do Conjunto de Cifras da Política de Grupo.

Importante:

As alterações da Política de Grupo para a configuração TLS só entram em vigor após a reinicialização do sistema operacional.

Use uma política Citrix para configurar as configurações de SSL/TLS para conexões de fluxo de dados de impressão criptografados (CGP) (porta TCP 443).

Configuração do servidor SSL/TLS

O Universal Print Server funciona como o servidor SSL/TLS.

Use o script PowerShell `Enable-UpsSsl.ps1` para configurar as configurações de SSL/TLS.

Instalar o certificado de servidor TLS no Universal Print Server

Para HTTPS, o Universal Print Server oferece suporte a recursos TLS usando certificados de servidor. Certificados de cliente não são usados. Use os Serviços de Certificados do Microsoft Active Directory ou outra autoridade de certificação para solicitar um certificado para o Universal Print Server.

Tenha em mente as seguintes considerações ao registrar/solicitar um certificado usando os Serviços de Certificados do Microsoft Active Directory:

1. Coloque o certificado no armazenamento de certificados **Pessoal** do Computador Local.
2. Defina o atributo **Nome Comum** do Nome Distinto do Assunto (Subject DN) do certificado para o nome de domínio totalmente qualificado (FQDN) do Universal Print Server. Especifique isso no modelo de certificado.
3. Defina o Provedor de Serviços Criptográficos (CSP) usado para gerar a solicitação de certificado e a chave privada como **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Especifique isso no modelo de certificado.
4. Defina o Tamanho da Chave para pelo menos 2048 bits. Especifique isso no modelo de certificado.

Configurando SSL no Universal Print Server

O Serviço XTE no Universal Print Server escuta as conexões de entrada. Ele funciona como um servidor SSL quando o SSL está habilitado. As conexões de entrada são de dois tipos: conexões de serviço web de impressão, que contêm comandos de impressão, e conexões de fluxo de dados de impressão, que contêm trabalhos de impressão. O SSL pode ser habilitado nessas conexões. O SSL protege a confidencialidade e a integridade dessas conexões. Por padrão, o SSL está desabilitado.

O script PowerShell usado para configurar o SSL está na mídia de instalação e tem este nome de arquivo: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Configurando números de porta de escuta no Universal Print Server

Estas são as portas padrão para o Serviço XTE:

- Porta TCP do serviço web de impressão em texto simples (HTTP): 8080
- Porta TCP do fluxo de dados de impressão em texto simples (CGP): 7229
- Serviço web de impressão criptografado (HTTPS) porta TCP: 8443
- Fluxo de dados de impressão criptografado (CGP) porta TCP: 443

Para alterar as portas usadas pelo Serviço XTE no Universal Print Server, execute os seguintes comandos no PowerShell como administrador (consulte a seção posterior para obter notas sobre o uso do script PowerShell Enable-UpsSsl.ps1):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` ou `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

Configurações de TLS no Universal Print Server

Se você tiver vários Universal Print Servers em uma configuração com balanceamento de carga, certifique-se de que as configurações de **TLS** estejam configuradas de forma consistente em todos os Universal Print Servers.

Ao configurar o TLS no Universal Print Server, as permissões no certificado TLS instalado são alteradas, concedendo ao Serviço de Impressão Universal acesso de leitura à chave privada do certificado e informando ao Serviço de Impressão Universal o seguinte:

- Qual certificado no armazenamento de certificados usar para TLS.
- Quais números de porta TCP usar para conexões TLS.

O Firewall do Windows (se ativado) deve ser configurado para permitir conexões de entrada nessas portas TCP. Essa configuração é feita automaticamente quando você usa o script PowerShell Enable-UpsSsl.ps1.

- Quais versões do protocolo TLS permitir.

O Universal Print Server suporta as versões 1.3 e 1.2 do protocolo TLS. Especifique a versão mínima permitida.

A versão padrão do protocolo TLS é 1.2.

> **Observação:**

> TLS 1.1 e 1.0 não são mais suportados a partir da versão 2311 do Citrix Virtual Apps and Desktops.

- Quais conjuntos de cifras TLS permitir.

Um conjunto de cifras seleciona os algoritmos criptográficos usados para uma conexão. VDAs e Universal Print Server podem suportar diferentes conjuntos de cifras. Quando um VDA se conecta e envia uma lista de conjuntos de cifras TLS suportados, o Universal Print Server compara um dos conjuntos de cifras do cliente com um dos conjuntos de cifras em sua própria lista de conjuntos de cifras configurados e aceita a conexão. Se não houver um conjunto de cifras correspondente, o Universal Print Server rejeita a conexão.

O Universal Print Server suporta os seguintes conjuntos de suites de cifras nomeados GOV(ernment), COM(mercial) e ALL para os modos de Crypto Kit nativos OPEN, FIPS e SP800-52. As suites de cifras aceitáveis também dependem da configuração da política **Modo FIPS SSL** e do Modo FIPS do Windows. Consulte este artigo de suporte da Microsoft para obter informações sobre o modo FIPS do Windows.

CONJUNTO DE CIFRAS (EM ORDEM DECRESCENTE DE PRIORIDADE)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECD	X		X	X		X	X		X

CONJUNTO DE CIFRAS (EM ORDEM DECRESCENTE DE PRIORIDADE)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
HE_RSA_AES256_CBC_SHA384									
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

Configurar TLS em um Universal Print Server usando o script PowerShell

Instale o Certificado TLS na área **Computador Local > Pessoal > Certificados** do armazenamento de certificados. Se mais de um certificado residir nesse local, forneça o thumbprint do certificado ao script do PowerShell `Enable-UpsSsl.ps1`.

> **Observação:**

O script do PowerShell encontra o certificado correto com base no FQDN do Universal Print Server. Você não precisa fornecer o thumbprint do certificado quando apenas um único certificado está presente para o FQDN do Universal Print Server.

O script `Enable-UpsSsl.ps1` habilita ou desabilita as conexões TLS originadas do VDA para o Universal Print Server. Este script está disponível na pasta **Support > Tools > SslSupport** na mídia de instalação.

Ao habilitar o TLS, o script desabilita todas as regras existentes do Firewall do Windows para as portas TCP do Universal Print Server. Em seguida, ele adiciona novas regras que permitem que o Serviço XTE aceite conexões de entrada apenas nas portas TCP e UDP TLS. Ele também desabilita as regras do Firewall do Windows para:

- Conexões de serviço web de impressão em texto simples (padrão: 8080)
- Conexões de fluxo de dados de impressão em texto simples (CGP) (padrão: 7229)

O efeito é que o VDA pode fazer essas conexões somente ao usar TLS.

Observação:

A habilitação do TLS não afeta as conexões RPC/SMB do Spooler de Impressão do Windows originadas do VDA e destinadas ao Universal Print Server.

Importante:

Especifique **Enable** ou **Disable** como o primeiro parâmetro. O parâmetro CertificateThumbprint é opcional se apenas um certificado no armazenamento de certificados Pessoal do Computador Local tiver o FQDN do Universal Print Server. Os outros parâmetros são opcionais.

Sintaxe

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-
HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;]
[-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-
FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]
```

```
Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum>] [-CGPPort
&lt;portnum>]
```

PARÂMETRO	DESCRIÇÃO
Habilitar	Habilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Disable é obrigatório.
Desabilitar	Desabilita SSL/TLS no Servidor XTE. Este parâmetro ou o parâmetro Enable é obrigatório.
CertificateThumbprint `"<thumbprint>"`	Impressão digital do certificado TLS no armazenamento de certificados Pessoal do Computador Local, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar.
HTTPPort `<port>`	Porta do serviço web de impressão em texto simples (HTTP/SOAP). Padrão: 8080
CGPPort `<port>`	Porta do fluxo de dados de impressão em texto simples (CGP). Padrão: 7229
HTTPSPort `<port>`	Porta do serviço web de impressão criptografado (HTTPS/SOAP). Padrão: 8443
CGPSSLPort `<port>`	Porta do fluxo de dados de impressão criptografado (CGP). Padrão: 443
SSLMinVersion `"<version>"`	Versão mínima do protocolo TLS, entre aspas. Valores válidos: "TLS_1.2" e "TLS_1.3". Padrão: TLS_1.2.
SSLCipherSuite `"<name>"`	Nome do pacote de conjuntos de cifras TLS, entre aspas. Valores válidos: "GOV", "COM" e "ALL" (padrão).
FIPSMode `<Boolean>`	Ativa ou desativa o modo FIPS 140 no Servidor XTE. Valores válidos: $true para

PARÂMETRO	DESCRIÇÃO
	ativar o modo FIPS 140, $false para desativar o modo FIPS 140.

Exemplos

O script a seguir habilita o TLS. A impressão digital (representada como "12345678987654321" neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

O script a seguir desabilita o TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Configurando o modo FIPS

A habilitação do modo FIPS (US Federal Information Processing Standards) garante que apenas criptografia compatível com FIPS 140 seja usada para conexões criptografadas do Universal Print Server.

Configure o modo FIPS no servidor antes de configurar o modo FIPS no cliente.

Consulte o site de documentação da Microsoft para habilitar/desabilitar o modo FIPS do Windows.

Habilitando o modo FIPS no cliente

No Delivery Controller™, execute o Web Studio e defina a configuração da política Citrix **Modo FIPS SSL** como **Habilitado**. Habilite a política Citrix.

Faça isso em cada VDA:

1. Habilite o modo FIPS do Windows.
2. Reinicie o VDA.

Habilitando o modo FIPS no servidor

Faça isso em cada Universal Print Server:

1. Habilite o modo FIPS do Windows.
2. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $true`.

4. Reinicie o Universal Print Server.

Desativando o modo FIPS no cliente

No Web Studio, defina a configuração da política Citrix **Modo FIPS SSL** como **Desativado**. Habilite a política Citrix. Você também pode excluir a configuração da política Citrix **Modo FIPS SSL**.

Faça isso em cada VDA:

1. Desative o modo FIPS do Windows.
2. Reinicie o VDA.

Desativando o modo FIPS no servidor

Faça isso em cada Universal Print Server:

1. Desative o modo FIPS do Windows.
2. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $false`.
4. Reinicie o Universal Print Server.

> **Observação:**
>
> O modo FIPS não é compatível quando a versão do protocolo SSL está definida como TLS 1.3.

Configurando a versão do protocolo SSL/TLS

A versão padrão do protocolo SSL/TLS é TLS 1.2. TLS 1.2 e TLS 1.3 são as versões de protocolo SSL/TLS recomendadas para uso em produção. Para solução de problemas, pode ser necessário alterar temporariamente a versão do protocolo SSL/TLS em um ambiente que não seja de produção.

SSL 2.0 e SSL 3.0 não são suportados no Universal Print Server.

Definindo a versão do protocolo SSL/TLS no servidor

Faça isso em cada Universal Print Server:

1. Execute este comando PowerShell como Administrador: `stop-service CitrixXTEServer, UpSvc`
2. Execute o script `Enable-UpsSsl.ps1` com os parâmetros de versão `-Enable -SSLMinVersion`. Lembre-se de reverter para TLS 1.2 ou TLS 1.3 quando terminar os testes.
3. Reinicie o Universal Print Server.

Definindo a versão do protocolo SSL/TLS no cliente

Faça isso em cada VDA:

1. No Delivery Controller, defina a configuração da política **Versão do Protocolo SSL** para a versão de protocolo desejada e habilite a política.
2. O artigo de suporte da Microsoft Configurações de Registro TLS descreve as configurações de registro para Microsoft SCHANNEL SSP. Habilite o lado do cliente **TLS 1.2 ou TLS 1.3** usando as configurações de registro.

   > **Importante:**
   >
   > Lembre-se de restaurar as configurações de registro para seus valores originais quando terminar os testes.

3. Reinicie o VDA.

Solução de problemas

Se ocorrer um erro de conexão, verifique o arquivo C:\Program Files (x86)\Citrix\XTE\logs\error.log no Universal Print Server.

A mensagem de erro **SSL handshake from client failed** aparece neste arquivo de log se o handshake SSL/TLS falhar. Tais falhas podem ocorrer se a versão do protocolo SSL/TLS no VDA e no Universal Print Server não corresponderem.

Use o FQDN do Universal Print Server nas seguintes configurações de política que contêm nomes de host do Universal Print Server:

- Impressoras de sessão
- Atribuições de impressora
- Universal Print Servers para balanceamento de carga

Certifique-se de que o relógio do sistema (data, hora e fuso horário) esteja correto nos Universal Print Servers e nos VDAs.

Lista de permissões de canal virtual

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas os canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

Configuração

A lista de permissões de canal virtual é habilitada por padrão. Você pode configurar esse recurso usando as seguintes configurações na política Citrix:

- **Lista de permissões de canal virtual**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.
- **Limitação de log da lista de permissões de canal virtual**: define o período de limitação para o registro de eventos da lista de permissões de canal virtual.
- **Registro em log da lista de permissões de canal virtual**: define o nível de registro em log para a lista de permissões de canal virtual.

Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando a configuração de política da lista de permissões de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para vários processos

Se houver vários processos, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`

- Todos os caminhos devem ser locais.

> **Nota:**

> - Caminhos de rede não são permitidos.
> - O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
> - O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

> **Nota:**

> Variáveis de ambiente de usuário não são suportadas.

> O suporte a variáveis de ambiente está disponível a partir do Citrix Virtual Apps and Desktops versão 2209.

Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política de lista de permissões de canais virtuais para o canal virtual e o processo identificados.
5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- Pacote de Otimização HDX RealTime para Skype for Business

Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`

- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

Pacote de Otimização HDX RealTime para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Comunicação WebSocket entre VDA e Delivery Controller™

Este artigo descreve como configurar uma conexão WebSocket para comunicação entre VDAs e Delivery Controllers como uma alternativa ao uso da comunicação WCF. Ele oferece o benefício de que apenas a porta TLS 443 é usada para comunicação do VDA para o Delivery Controller.

Atualmente, isso está disponível apenas para máquinas provisionadas por MCS. Máquinas provisionadas manualmente estão em pré-visualização técnica, consulte /pt-br/citrix-virtual-apps-desktops/2407/install-configure/machine-catalogs-manage#enroll-non-mcs-provisioned-vdas-using-tokens-preview).

Como funciona

A seção a seguir descreve o fluxo de trabalho para a conexão WebSocket entre um Delivery Controller e um VDA:

1. Os administradores do Citrix Virtual Apps and Desktops™ iniciam o processo provisionando VDAs usando o Machine Creation Service (MCS).
2. Durante o processo de provisionamento do MCS, o MCS gera pares de chaves pública-privada para cada VDA e registra as chaves públicas com o serviço de confiança FMA no Delivery Controller. O MCS salva o par de chaves pública-privada como um arquivo no disco de identidade nos VDAs.

3. Quando a máquina VDA inicializa, o agente MCS instalado na máquina VDA lê o par de chaves do disco de identidade e grava essas informações no local do registro do VDA.
4. O agente broker instalado no VDA lê os pares de chaves do registro e gera uma solicitação WebSocket habilitada para SSL para o Delivery Controller com a chave de serviço assinada pela chave privada.
5. O Delivery Controller verifica o cabeçalho de autorização da chave de serviço assinada com a chave pública do serviço de confiança FMA.
6. Concluída a verificação, o sistema estabelece a conexão WebSocket entre o VDA e o Delivery Controller.

Suporte a WebSocket

Antes de começar

1. Configure seu site. Para obter mais informações, consulte Criar um site.
2. Instale certificados TLS nos Delivery Controllers. Para obter mais informações, consulte Instalar certificados de servidor TLS nos Controllers.
3. Instale a CA raiz e a CA intermediária no VDA para confiar no Delivery Controller.

Procedimento

Siga as instruções para configurar uma conexão WebSocket:

1. Habilite a conexão WebSocket no Delivery Controller. Execute o seguinte comando em cada Delivery Controller presente em seu site:

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   > **Observação:**
   >
   > Certifique-se de reiniciar os Delivery Controllers após habilitar o WebSocket.

2. Crie um catálogo de máquinas para VDAs unidos ao AD com provisionamento MCS. Para obter mais informações, consulte Criar catálogo de máquinas.
3. Crie um grupo de entrega e adicione seu VDA a ele. Para obter mais informações, consulte Criar grupos de entrega.

4. Habilite a conexão WebSocket no VDA. Execute o seguinte comando PowerShell no VDA:

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

   - Para verificar se o WebSocket está habilitado, verifique o seguinte valor da chave de registro. O valor de `Enabled` deve ser 1.

     Chave:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
     nt\WebSocket
     ```

     Nome: Enabled

     Tipo: REG_DWORD

     Valor: 1

Conectividade HDX™

O Citrix HDX representa um amplo conjunto de tecnologias que oferecem uma experiência de alta definição a usuários de aplicativos e desktops centralizados, em qualquer dispositivo e em qualquer rede.

O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptável
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência de TI e do usuário, diminuem o consumo de largura de banda e aumentam a densidade de usuários por servidor de hospedagem.

Dentro da oferta HDX, você pode se conectar por meio de um protocolo de transporte exclusivo e proprietário, utilizar as unidades máximas de transmissão ao estabelecer sessões e otimizar a conectividade com o Citrix SD-WAN.

Transporte adaptável

O Transporte Adaptável é um mecanismo no Citrix Virtual Apps and Desktops™ que permite estabelecer conexões para sessões HDX usando um protocolo de transporte preferencial, ao mesmo tempo que oferece um fallback para TCP se a conectividade com o protocolo preferencial não estiver disponível.

Os seguintes protocolos de transporte são suportados:

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

Configuração

O Transporte Adaptável é ativado por padrão. Você pode configurar o Transporte Adaptável para operar nos seguintes modos:

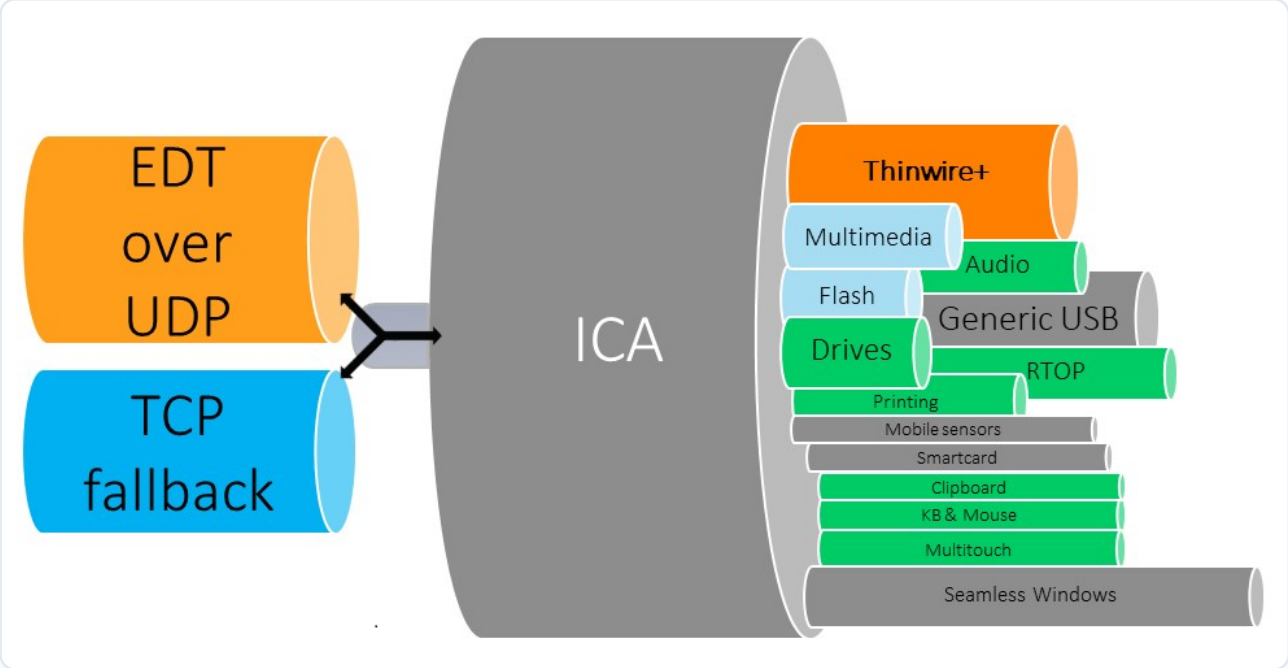
- **Preferencial**: (Padrão) O cliente tenta se conectar com o protocolo preferencial e retorna ao TCP se a conectividade com o protocolo preferencial não estiver disponível.
- **Modo de diagnóstico**: O cliente tenta se conectar apenas usando o protocolo preferencial. O fallback para TCP é desativado.
- **Desativado**: O cliente tenta se conectar apenas usando TCP.

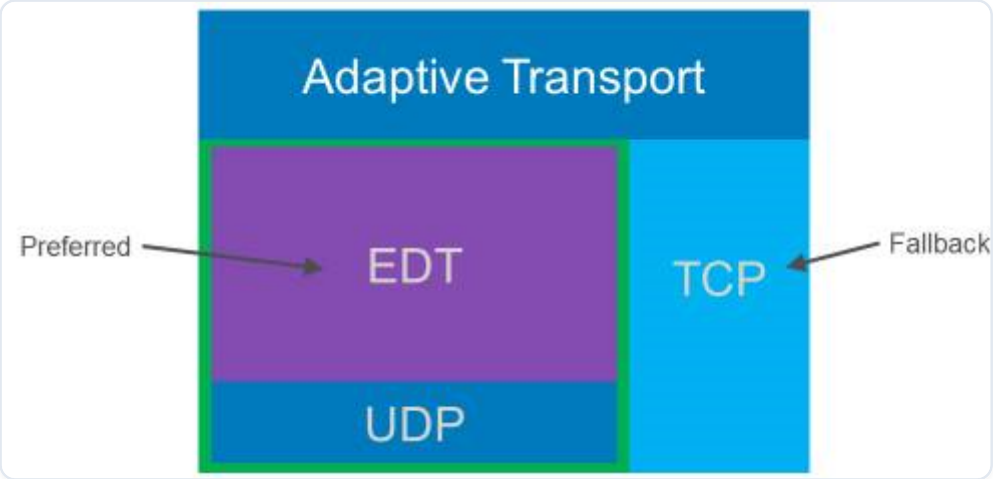
Como funciona

Quando o **Transporte Adaptável** está definido como `Preferred`, o cliente tenta se conectar à sessão com o protocolo preferencial e o TCP em paralelo. Isso permite otimizar o tempo de conexão se não for possível conectar com o protocolo preferencial e o cliente precisar retornar ao uso de TCP. Se a conexão for estabelecida usando TCP, o cliente tenta se conectar com o protocolo preferencial em segundo plano a cada cinco minutos.

Quando o **Transporte Adaptável** está definido como `Diagnostic mode`, o cliente se conecta à sessão apenas com o protocolo preferencial. Se o cliente não conseguir estabelecer uma conexão usando o protocolo preferencial, ele não retorna ao uso de TCP, e a conexão falha.

Quando o **Transporte Adaptável** está definido como `Off`, o **Transporte Adaptável** é desativado, e o cliente se conecta à sessão usando apenas TCP.





Requisitos do sistema

A seguir estão os requisitos para usar o Transporte Adaptável e o EDT:

- Plano de controle
  - Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops)
  - Citrix Virtual Apps and Desktops: versão atualmente suportada
- Virtual Delivery Agent
  - Windows: versão atualmente suportada (2402 ou posterior é recomendada)
  - Linux: versão atualmente suportada (2402 ou posterior é recomendada)
- Aplicativo Citrix Workspace™
  - Windows: versão atualmente suportada (2402 ou posterior é recomendada)
  - Linux: versão atualmente suportada (2402 ou posterior é recomendada)
  - Mac: versão atualmente suportada (2402 ou posterior é recomendada)
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível no Google Play
- Citrix NetScaler® Gateway
  - 14.1.12.30 ou posterior (recomendado)
  - 13.1.17.42 ou posterior (13.1-52.19 ou posterior recomendado)

> **Observação:**

Para obter detalhes sobre o VDA Linux, consulte a documentação do Linux Virtual Delivery Agent.

Requisitos de rede

As seções a seguir são os requisitos de rede para usar o EDT com o Transporte Adaptável:

Hosts de sessão

Se os seus hosts de sessão tiverem um firewall como o Firewall do Windows Defender, você deve permitir o seguinte tráfego de entrada para conexões internas.

DESCRIÇÃO	ORIGEM	PROTOCOLO	PORTA
Conexão interna - Confiabilidade da Sessão ativada	Cliente	UDP	2598
Conexão interna - Confiabilidade da Sessão desativada			1494
Conexão interna - HDX™ Direto ou VDA SSL			443

Observação:

O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

Rede interna

A tabela a seguir descreve as regras de firewall necessárias para usar o EDT em sua rede:

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta - Confiabilidade	UDP	Rede do cliente	Rede VDA	2598

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
da Sessão ativada				
Conexão interna direta - Confiabilidade da Sessão desativada				1494
Conexão interna direta - HDX Direto ou VDA SSL				443
NetScaler Gateway		NetScaler SNIP		2598
NetScaler Gateway - VDA SSL				443

Observação:

Se você estiver usando o Citrix Gateway Service, você deve habilitar o **Rendezvous** para usar o EDT como seu protocolo de transporte. Consulte a documentação do Rendezvous para requisitos de sistema e rede.

Rede do cliente

A tabela a seguir descreve os requisitos de conectividade para dispositivos cliente:

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna - Confiabilidade	UDP	IP do cliente	Rede VDA	2598

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
da sessão habilitada				
Conexão interna - Confiabilidade da sessão desabilitada				1494
Conexão interna - HDX Direct ou SSL VDA				443
Conexão externa - NetScaler Gateway			Endereço IP público do NetScaler Gateway	443
Conexão externa - Citrix Gateway Service			Citrix Gateway Service	443

Observação:

Se você estiver usando o Citrix Gateway Service, os clientes devem conseguir acessar `<https://*.*.nssvc.net>`. Se você não conseguir permitir todos os subdomínios usando `<https://*.*.nssvc.net>`, você pode usar `<https://*.c.nssvc.net>` e `<https://*.g.nssvc.net>` em vez disso. Para obter mais informações, consulte o artigo do Knowledge Center CTX270584.

Transporte de Dados Iluminado

O Transporte de Dados Iluminado (EDT) é um protocolo de transporte proprietário da Citrix construído sobre o User Datagram Protocol (UDP). Ele oferece uma experiência de usuário superior em conexões de longa distância desafiadoras, mantendo a escalabilidade do servidor. O

EDT melhora o rendimento de dados para todos os canais virtuais ICA® em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.

Quando o **Transporte Adaptável** está ativado, o EDT é o protocolo preferencial.

Coisas a saber

- A **Confiabilidade da Sessão** deve ser ativada para usar a **Descoberta de MTU** e o EDT com o NetScaler® Gateway e o Citrix Gateway Service.
- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha na abertura de sessões em alguns casos. Para evitar isso, você deve ajustar o MTU do EDT para um valor adequado às suas redes. Você pode usar a Descoberta de MTU do EDT ou uma solução alternativa manual descrita em Como configurar o MSS ao usar o EDT em redes com MTU não padrão.
- Para obter detalhes sobre como habilitar o uso do EDT com o NetScaler Gateway, consulte Configurar o NetScaler Gateway para oferecer suporte ao Transporte de Dados Iluminado.

Descoberta de MTU do EDT

A Descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso evita a fragmentação de pacotes EDT que pode resultar em degradação do desempenho ou falha no estabelecimento de uma sessão.

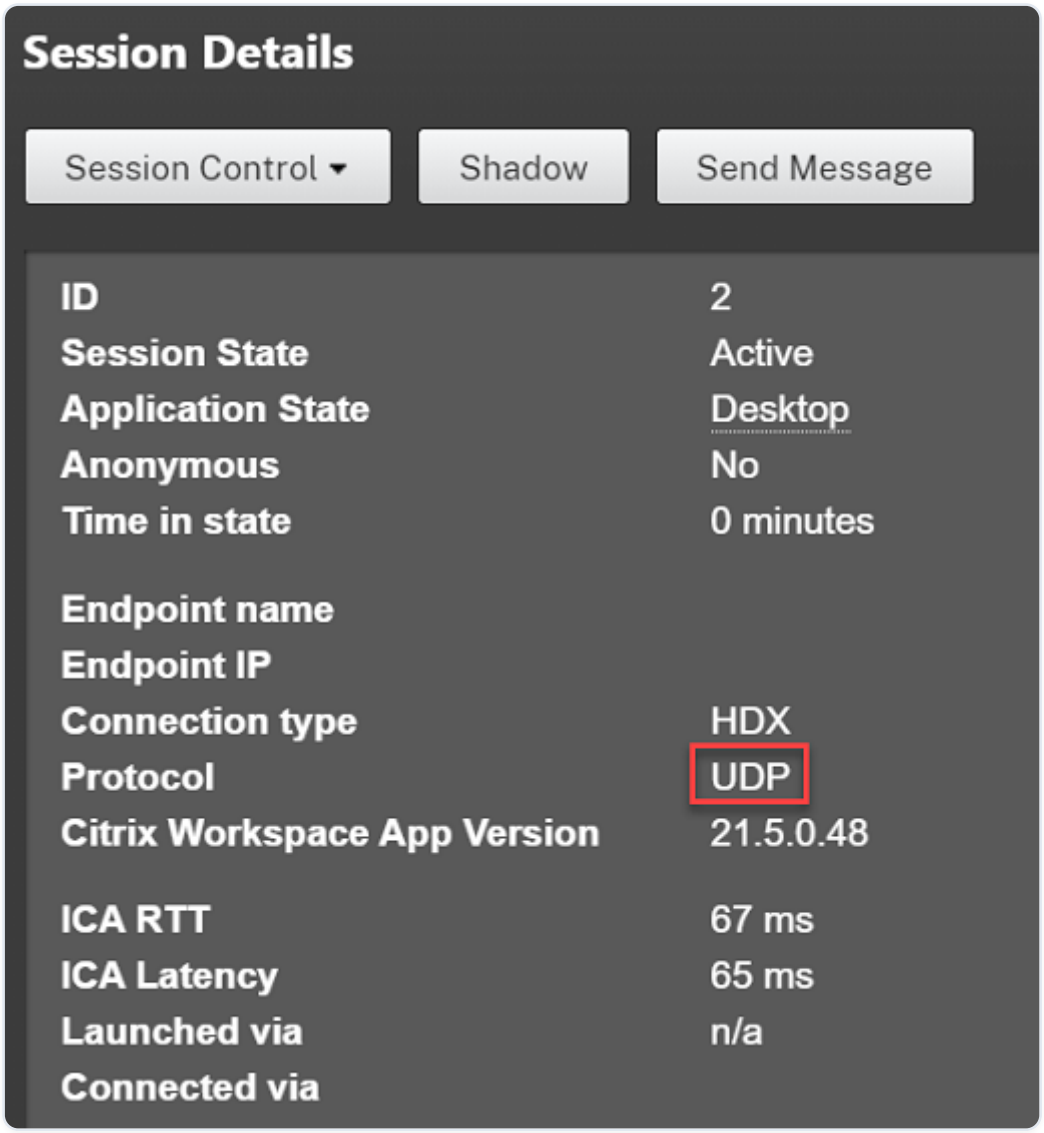
A Descoberta de MTU é ativada por padrão. Se você precisar desativá-la, consulte Recursos HDX gerenciados através do registro para obter detalhes.

> **Observação:**
>
> - A **Confiabilidade da Sessão** deve ser ativada para que a Descoberta de MTU funcione.
> - A Descoberta de MTU com ICA Multi-Stream está disponível com as versões 2209 e posteriores do VDA.

Solução de problemas

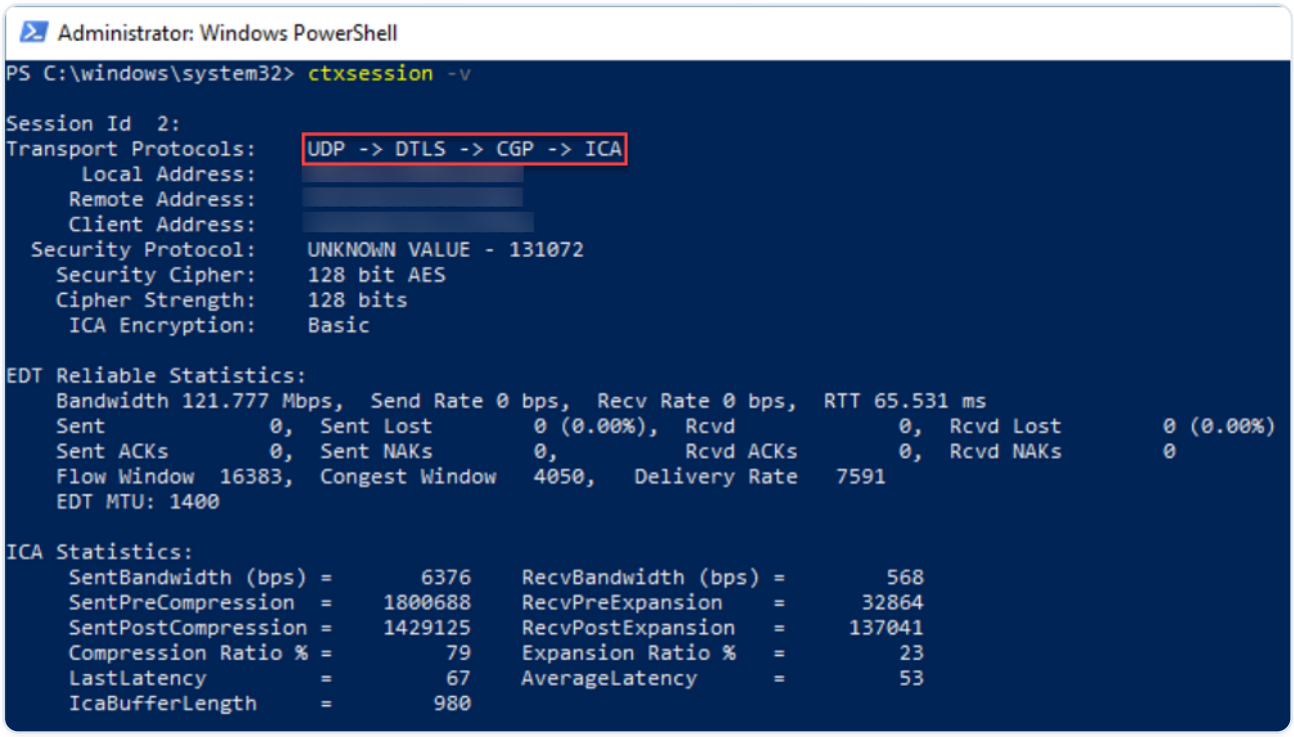
Para confirmar que o EDT está sendo usado como protocolo de transporte para a sessão, você pode usar o Director ou o utilitário de linha de comando `CtxSession.exe` no VDA.

No Director, procure a sessão e selecione **Detalhes**. Se o **Tipo de conexão** for `HDX` e o **Protocolo** for `UDP`, o EDT estará sendo usado como protocolo de transporte para a sessão.



Para usar o utilitário CtxSession.exe, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe`. Para ver estatísticas detalhadas, execute `ctxsession.exe -v`. Se o EDT estiver em uso, o protocolo de transporte mostrará um dos seguintes:

- **UDP > ICA®** (Confiabilidade da sessão desabilitada)
- **UDP > CGP > ICA** (Confiabilidade da sessão habilitada)
- **UDP > DTLS > CGP > ICA** (ICA é criptografado de ponta a ponta com DTLS)



Quando as sessões falham ao conectar com EDT

Para solucionar problemas de **Transporte Adaptável** e **EDT**, sugerimos o seguinte:

1. Revise os Requisitos do sistema, Requisitos de rede, Problemas conhecidos e Coisas a saber, e certifique-se de que todos os itens foram abordados.
2. Verifique se há políticas Citrix® no Studio ou GPO substituindo a configuração desejada de **Transporte Adaptável HDX**.
3. Verifique se há configurações no cliente substituindo a configuração desejada de Transporte Adaptável HDX. Isso pode ser uma preferência de GPO, uma configuração usando o modelo administrativo opcional do aplicativo Workspace ou uma configuração manual da configuração **HDXoverUDP** no registro ou no arquivo de configuração do cliente.
4. Em máquinas VDA de várias sessões, certifique-se de que os ouvintes UDP estejam ativos. Abra um prompt de comando na máquina VDA e execute `netstat -a -p udp`. Para obter mais informações, consulte Como confirmar o protocolo de transporte de dados iluminado HDX.
5. Verifique se as regras de firewall apropriadas foram configuradas tanto nos firewalls de rede quanto nos firewalls em execução nas máquinas VDA.
6. Inicie uma sessão direta internamente, ignorando o NetScaler® Gateway ou o Citrix Gateway Service, e verifique o protocolo em uso. Se a sessão usar EDT, o VDA estará pronto para usar EDT para conexões externas através do NetScaler Gateway ou do Citrix Gateway Service.

7. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo NetScaler Gateway ou Citrix Gateway Service:
    - Certifique-se de que a **Confiabilidade da Sessão** esteja ativada.
    - Se estiver usando o NetScaler Gateway, certifique-se de que sua configuração esteja de acordo com a configuração necessária descrita em Configurar o NetScaler Gateway para oferecer suporte ao Enlightened Data Transport e ao HDX Insight.
8. Se estiver usando o Citrix Gateway Service, certifique-se de que o Rendezvous esteja ativado e funcionando.
9. Verifique se as conexões dos seus usuários exigem um MTU não padrão. Conexões com um MTU efetivo inferior a 1500 bytes causam fragmentação de pacotes EDT, o que, por sua vez, pode afetar o desempenho ou até mesmo causar falhas no lançamento da sessão. Esse problema é comum ao usar VPNs, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Certifique-se de ter a Descoberta de MTU ativada ou de estar configurando um MTU personalizado conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

Problemas conhecidos

- Caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe para conexões que não passam pelo NetScaler Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para a versão 2103 ou posterior do VDA.
- Ao usar o NetScaler Gateway, caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe. Isso ocorre devido a um problema no Gateway que faz com que o bit Don’t Fragment (DF) no cabeçalho dos pacotes EDT não seja propagado. Uma correção para esse problema está disponível, a partir da versão de firmware 13.1 build 17.42. Para obter detalhes sobre como ativar a correção, consulte a documentação do NetScaler Gateway.
- A Descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não respeitam o bit DF quando o processamento de pacotes está ativado, impedindo que a Descoberta de MTU detecte a fragmentação. Nesta situação, as seguintes opções estão disponíveis:
    - Desative o processamento de pacotes no modem do usuário.
    - Desative a **Descoberta de MTU** e use um MTU codificado, conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

- Desative o **Transporte Adaptável** para forçar as sessões a usar TCP. Se apenas um subconjunto de usuários for afetado, considere desativá-lo no lado do cliente para que outros usuários possam continuar a usar o EDT.

HDX™ Direct (Pré-visualização)

Ao acessar recursos fornecidos pela Citrix, o HDX Direct permite que dispositivos cliente internos e externos estabeleçam uma conexão direta segura com o host da sessão, se a comunicação direta for possível.

> **Importante:**

> O HDX Direct está atualmente em pré-visualização. Este recurso é fornecido sem suporte e ainda não é recomendado para uso em ambientes de produção. Para enviar feedback ou relatar problemas, use este formulário.

Requisitos do sistema

A seguir estão os requisitos de sistema para usar o HDX Direct:

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2402 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2402 ou posterior
- Aplicativo Workspace
  - Windows: versão 2402 ou posterior
- Camada de acesso
  - Citrix Workspace™ com Citrix Gateway Service
  - Citrix Workspace com NetScaler® Gateway
- Outro
  - O Adaptive Transport deve ser habilitado para conexões diretas externas

Requisitos de rede

A seguir estão os requisitos de rede para usar o HDX Direct.

Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deverá permitir o seguinte tráfego de entrada para conexões internas.

DESCRIÇÃO	ORIGEM	PROTOCOLO	PORTA
Conexão interna direta	Cliente	TCP	443
Conexão interna direta	Cliente	UDP	443

> Nota:
>
> O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

Rede do cliente

A tabela a seguir descreve a rede do cliente para usuários internos e externos.

Usuários internos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta	TCP	Rede do cliente	1024–65535	Rede VDA	443
Conexão interna direta	UDP	Rede do cliente	1024–65535	Rede VDA	443

Usuários externos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
STUN (somente usuários externos)	UDP	Rede do cliente	1024–65535	Internet (consulte a nota abaixo)	3478, 19302
Conexão de usuário externo	UDP	Rede do cliente	1024–65535	Endereço IP público do data center	1024–65535

Rede do data center

A tabela a seguir descreve a rede do data center para usuários internos e externos.

Usuários internos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta	TCP	Rede do cliente	1024–65535	Rede VDA	443
Conexão interna direta	UDP	Rede do cliente	1024–65535	Rede VDA	443

Usuários externos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
STUN (somente usuários externos)	UDP	Rede VDA	1024–65535	Internet (ver nota abaixo)	3478, 19302
Conexão de usuário externo	UDP	DMZ / Rede interna	1024–65535	Rede VDA	55000–55250

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão de usuário externo	UDP	Rede VDA	55000–55250	IP público do cliente	1024–65535

Observação:

Tanto o VDA quanto o aplicativo Workspace tentam enviar solicitações STUN para os seguintes servidores na mesma ordem:

- stunserver.stunprotocol.org:3478
- employees.org:3478
- stun.l.google.com:19302

Se você alterar o intervalo de portas padrão para conexões de usuários externos usando a configuração de política **Intervalo de portas HDX Direct**, as regras de firewall correspondentes devem corresponder ao seu intervalo de portas personalizado.

Configuração

O HDX Direct está desabilitado por padrão. Você pode configurar este recurso usando a configuração **HDX Direct** na política do Citrix.

- **HDX Direct**: Para habilitar ou desabilitar um recurso.
- **Modo HDX Direct**: Determina se o **HDX Direct** está disponível apenas para clientes internos ou para clientes internos e externos.
- **Intervalo de portas HDX Direct**: Define o intervalo de portas que o VDA usa para conexões de clientes externos.

Considerações

A seguir estão as considerações para usar o HDX Direct:

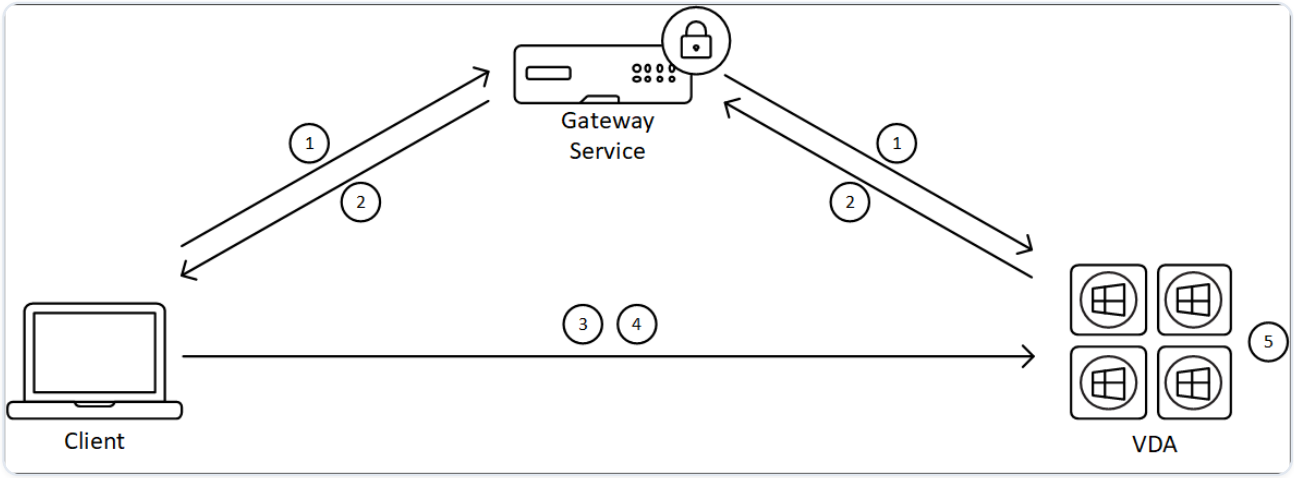
- O HDX Direct para usuários externos está disponível apenas com EDT (UDP) como protocolo de transporte. Portanto, o **Transporte Adaptável** deve estar habilitado.
- Se você estiver usando o **HDX Insight**, observe que o uso do **HDX Direct** impede a coleta de dados do HDX Insight, pois a sessão não seria mais proxy através do NetScaler Gateway.
- Ao usar máquinas não persistentes para seus aplicativos e desktops virtuais, a Citrix recomenda habilitar o **HDX Direct** nos hosts de sessão em vez de na imagem mestre/modelo para que cada máquina gere seus próprios certificados.
- O uso de seus próprios certificados com o HDX Direct não é atualmente suportado.

Como funciona

O HDX Direct permite que os clientes estabeleçam uma conexão direta com o host de sessão quando a comunicação direta está disponível. Quando as conexões diretas são feitas usando o HDX Direct, certificados autoassinados são usados para proteger a conexão direta com criptografia em nível de rede (TLS/DTLS).

Usuários internos

O diagrama a seguir descreve a visão geral do processo de conexão HDX Direct de usuários internos.



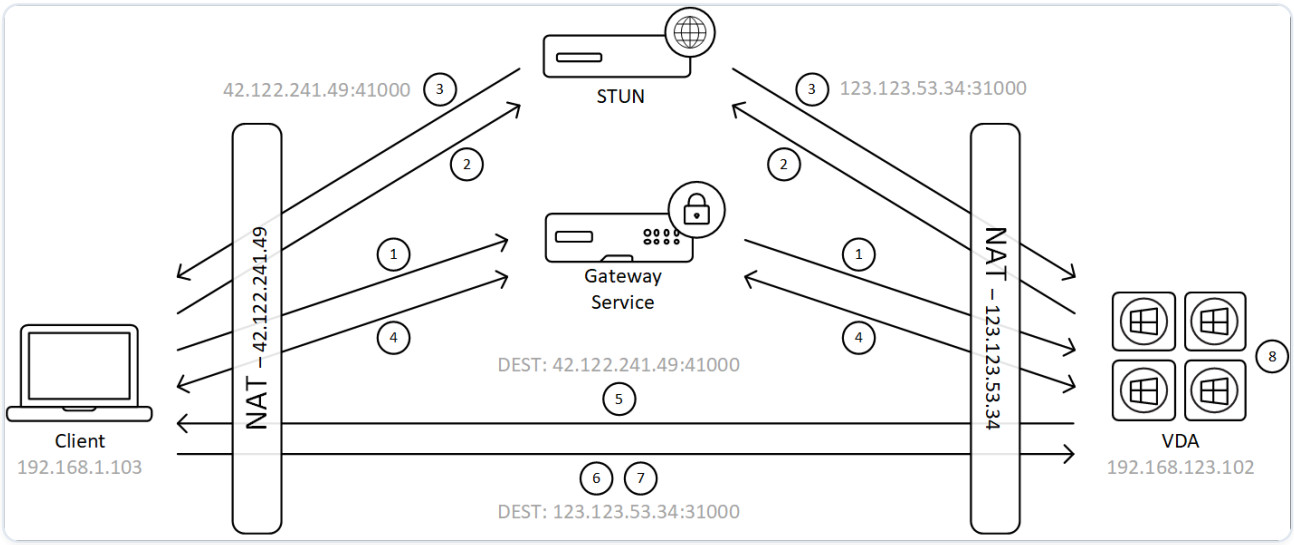
1. O cliente estabelece uma sessão HDX através do Serviço Gateway.
2. Após uma conexão bem-sucedida, o VDA envia ao cliente o FQDN da máquina VDA, uma lista de seus endereços IP e o certificado da máquina VDA via conexão HDX.
3. O cliente sonda os endereços IP para verificar se consegue alcançar o VDA diretamente.
4. Se o cliente conseguir alcançar o VDA diretamente com qualquer um dos endereços IP compartilhados, o cliente estabelece uma conexão direta com o VDA, protegida com (D)TLS usando um certificado que corresponde ao trocado na etapa (2).

5. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço Gateway é encerrada.

> **Observação:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

Usuários externos

O diagrama a seguir descreve a visão geral do processo de conexão HDX Direct para usuários externos:



1. O cliente estabelece uma sessão HDX através do Serviço Gateway.
2. Após uma conexão bem-sucedida, tanto o cliente quanto o VDA enviam uma solicitação STUN para descobrir seus endereços IP públicos e portas.
3. O servidor STUN responde ao cliente e ao VDA com seus respectivos endereços IP públicos e portas.
4. Através da conexão HDX, o cliente e o VDA trocam seus endereços IP públicos e portas UDP, e o VDA envia seu certificado ao cliente.
5. O VDA envia pacotes UDP para o endereço IP público e porta UDP do cliente. O cliente envia pacotes UDP para o endereço IP público e porta UDP do VDA.

6. Ao receber uma mensagem do VDA, o cliente responde com uma solicitação de conexão segura.
7. Durante o handshake DTLS, o cliente verifica se o certificado corresponde ao certificado trocado na etapa (4). Após a validação, o cliente envia seu token de autorização. Uma conexão direta segura é agora estabelecida.
8. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço Gateway é encerrada.

> **Observação:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

Gerenciamento de certificados

Host de sessão

Os dois serviços a seguir na máquina VDA manipular a criação e o gerenciamento de certificados, ambos configurados para serem executados automaticamente na inicialização da máquina:

- Serviço Citrix ClxMtp: Responsável pela geração e rotação de chaves de certificado CA.
- Serviço Citrix Certificate Manager: Responsável por gerar e gerenciar o certificado CA raiz autoassinado e os certificados da máquina.

As etapas a seguir descrevem o processo de gerenciamento de certificados:

1. Os serviços iniciam na inicialização da máquina.
2. `Citrix ClxMtp Service` cria chaves se nenhuma tiver sido criada ainda.
3. O Serviço Citrix Certificate Manager verifica se o **HDX Direct** está ativado. Caso contrário, o serviço se interrompe.
4. Se o **HDX Direct** estiver ativado, o Serviço Citrix Certificate Manager verifica se existe um certificado CA raiz autoassinado. Caso contrário, um certificado raiz autoassinado é criado.
5. Uma vez que um certificado CA raiz esteja disponível, o Serviço Citrix Certificate Manager verifica se existe um certificado de máquina autoassinado. Caso contrário, o serviço gera chaves e cria um novo certificado usando o FQDN da máquina.

6. Se houver um certificado de máquina existente criado pelo Serviço Citrix Certificate Manager e o nome do assunto não corresponder ao FQDN da máquina, um novo certificado será gerado.

> **Observação:**
>
> O Serviço Citrix Certificate Manager gera certificados RSA que utilizam chaves de 2048 bits.

Dispositivo cliente

Para estabelecer com sucesso uma conexão segura **HDX Direct**, o cliente deve confiar nos certificados usados para proteger a sessão. Para facilitar isso, o cliente recebe o certificado da CA para a sessão através do arquivo ICA® (fornecido pelo Workspace), portanto, não é necessário distribuir certificados da CA para os armazenamentos de certificados dos dispositivos cliente.

Compatibilidade NAT

Para estabelecer uma conexão direta entre um dispositivo de usuário externo e o host da sessão, o HDX™ Direct utiliza o hole punching para travessia NAT e o STUN para facilitar a troca do endereço IP público e dos mapeamentos de porta para o dispositivo cliente e o host da sessão. Isso é semelhante ao funcionamento de soluções de VoIP, comunicações unificadas e P2P.

Desde que os firewalls e outros componentes de rede estejam configurados para permitir o tráfego UDP para as solicitações STUN e as sessões HDX, espera-se que o HDX Direct para usuários externos funcione. No entanto, existem certos cenários em que os tipos de NAT das redes do usuário e do host da sessão levam a uma combinação incompatível, fazendo com que o HDX Direct falhe.

Validações

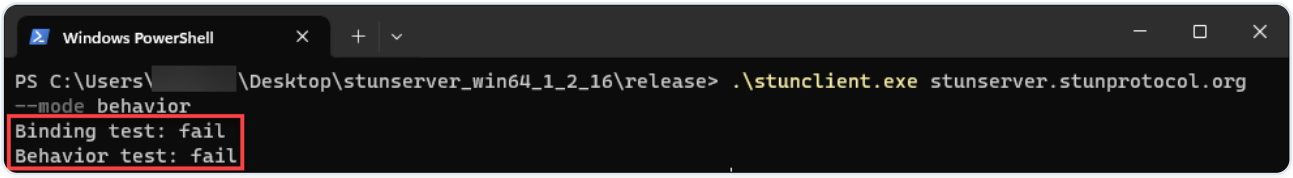
Você pode validar o tipo de NAT no cliente e no host da sessão usando o utilitário cliente STUN do STUNTMAN:

1. Baixe o pacote apropriado para a plataforma de destino em stunprotocol.org e extraia o conteúdo.
2. Abra um prompt de terminal e navegar até o diretório onde o conteúdo foi extraído.
3. Execute o seguinte comando: `.\stunclient.exe stunserver2024.stunprotocol.org --mode behavior`
4. Anote a saída.

Se os testes de binding e comportamento forem bem-sucedidos, tanto o **teste de binding** quanto o **teste de comportamento** relatam o sucesso e um comportamento NAT é especificado:



Se os testes falharem, tanto o **teste de binding** quanto o **teste de comportamento** relatam a falha.



Consulte a tabela a seguir para determinar se o HDX Direct para usuários externos deve funcionar com base nos resultados dos testes do cliente e do host da sessão:

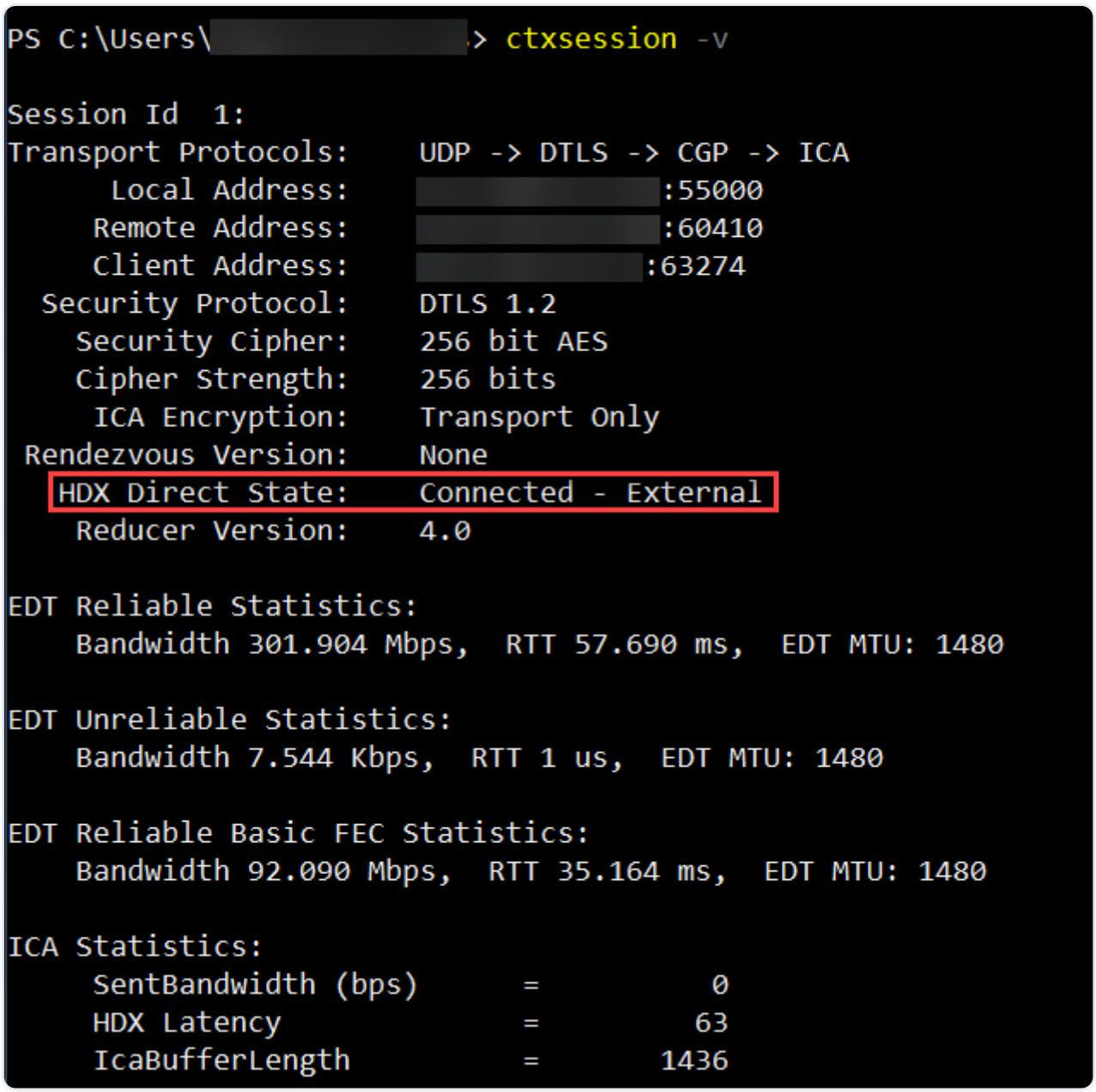
DISPOSITIVO CLIENTE	HOST DE SESSÃO	ESPERA-SE QUE FUNCIONE?
Mapeamento Independente de Endpoint	Mapeamento Independente de Endpoint	Sim
Mapeamento Independente de Endpoint	Mapeamento Dependente de Endpoint	Sim
Mapeamento Dependente de Endpoint	Mapeamento Independente de Endpoint	Sim
Mapeamento Dependente de Endpoint	Mapeamento Dependente de Endpoint	Não
Mapeamento dependente de endereço e porta	Qualquer tipo de NAT	Não
Qualquer tipo de NAT	Mapeamento dependente de endereço e porta	Não
Falha	Qualquer tipo de NAT	Não
Qualquer tipo de NAT	falha	Não

DISPOSITIVO CLIENTE	HOST DE SESSÃO	ESPERA-SE QUE FUNCIONE?
falha	falha	Não

Solução de problemas

Para confirmar que o **HDX Direct** estabeleceu uma conexão direta com sucesso, você pode usar o utilitário `CtxSession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se a conexão **HDX Direct** for estabelecida com sucesso, o **Status do HDX Direct** será `Connected`.



Você também pode consultar os logs de eventos do host da sessão para obter informações sobre se a conexão HDX™ Direct foi estabelecida com sucesso ou falhou. Consulte a seção **Logs de Eventos** para obter detalhes.

> Nota:
>
> Dependendo do ambiente e do número de endereços IP disponíveis para os hosts da sessão, pode levar até 5 minutos para que a conexão HDX Direct seja estabelecida.

Quando o HDX Direct falha ao estabelecer uma conexão direta

Se o HDX Direct estiver falhando ao estabelecer uma conexão direta, revise as seguintes etapas:

1. Certifique-se de que a versão do VDA e a versão do aplicativo Workspace em uso suportam o recurso de acordo com os requisitos do sistema.
2. Confirme se você tem uma política aplicada ao VDA que habilita o HDX Direct e que não há outras políticas com prioridade mais alta desabilitando o recurso.
3. Confirme se você tem uma política aplicada ao VDA que define o modo HDX Direct desejado e que não há outras políticas com prioridade mais alta sobrescrevendo a configuração.
4. Certifique-se de que o Serviço Citrix ClxMtp esteja em execução no host da sessão.
5. Certifique-se de que o Serviço Citrix Certificate Manager esteja em execução no host da sessão. Se não estiver em execução, tente iniciá-lo manualmente. O serviço para automaticamente se o HDX Direct for desabilitado.
6. Verifique se o host da sessão possui seu certificado de CA Raiz autoassinado:
    a. Emitido para: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
7. Verifique se o host da sessão possui seu certificado de servidor autoassinado:
    a. Emitido para: `<host FQDN>` (Por exemplo, FTLW11-001.ctxlab.net)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
8. Se os certificados estiverem ausentes, entre em contato com o Suporte Técnico da Citrix.
9. Se os certificados estiverem presentes:

a. Interrompa o Serviço de Gerenciamento de Certificados da Citrix no host da sessão.
b. Exclua o certificado de CA Raiz autoassinado e o certificado de servidor autoassinado.
c. Inicie o Serviço de Gerenciamento de Certificados da Citrix no host da sessão. O serviço cria novos certificados assim que é iniciado.

10. Para usuários internos:

a. Certifique-se de que o firewall do host da sessão não esteja bloqueando o tráfego de entrada nas portas UDP 443 ou TCP 443, para HDX sobre EDT e HDX sobre TCP, respectivamente.
b. Certifique-se de que o firewall da sua rede não esteja bloqueando o tráfego nas portas UDP 443 e TCP 443 entre a rede dos seus clientes e a rede dos hosts da sessão.

11. Para usuários externos:

a. Verifique o tipo de NAT para o cliente e o host da sessão, e certifique-se de que a combinação deve funcionar. Consulte a seção Compatibilidade de NAT para obter detalhes.
b. Se o teste de NAT falhar no cliente ou no host da sessão:

i. Se houver um firewall em execução no sistema, certifique-se de que ele não esteja bloqueando o tráfego de saída na porta UDP 3478.
ii. Certifique-se de que seus firewalls de rede não estejam bloqueando o tráfego de saída na porta UDP 3478.
iii. Certifique-se de que os firewalls não estejam bloqueando a resposta do servidor STUN.

c. Certifique-se de que seus firewalls de rede tenham as regras apropriadas configuradas para permitir todo o tráfego necessário. Consulte a seção Requisitos de Rede para obter detalhes.
d. Se você alterar o intervalo de portas padrão usando a configuração de política de intervalo de portas HDX Direct, certifique-se de que suas regras de firewall estejam definidas para o intervalo de portas personalizado.

Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA:

LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operacional	1	HDX Direct	Informação	Conexão HDX Direct para o usuário interno `<username>` estabelecida.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operacional	2	HDX Direct	Informação	Conexão HDX Direct para usuário externo `<username>` estabelecida.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	3	HDX Direct	Informações	Conexão HDX Direct para o usuário `<username>` falhou.

Problemas conhecidos

O HDX Direct pode parar de funcionar após a realização de um upgrade in-place do VDA em uma máquina que já tem o **HDX Direct** habilitado. Para resolver o problema, conclua as seguintes etapas:

1. Pare o Serviço de Gerenciador de Certificados Citrix no host da sessão.
2. Exclua o certificado de CA Raiz autoassinado e o certificado de servidor autoassinado.
3. Abra o registro.
4. Exclua a chave `HKLM\Software\Citrix\HDX-Direct`.
5. Vá para `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Defina o valor **SSLEnabled** como `0`.
7. Exclua o conteúdo do valor **SSLThumbprint**.
8. Inicie o **Serviço de Gerenciador de Certificados Citrix**.

Secure HDX™ (Prévia)

O HDX Seguro é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que quaisquer elementos de rede no caminho do tráfego inspecionem o tráfego HDX. Isso é feito fornecendo Criptografia de Ponta a Ponta (E2EE) verdadeira no nível do aplicativo entre o aplicativo Citrix Workspace™ (cliente) e o VDA (host de sessão) usando criptografia AES-256-GCM.

> **Importante:**
>
> O Secure HDX está atualmente em prévia. Este recurso é fornecido sem suporte e ainda não é recomendado para uso em ambientes de produção. Para enviar feedback ou relatar problemas, use este formulário.

Requisitos do sistema

A lista a seguir descreve os requisitos do sistema para usar o HDX Seguro.

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2402 ou posterior
- Host de sessão
  - Sistema operacional
    - Windows 10 22H2
    - Windows 11 22H2 ou posterior
    - Windows Server 2019 ou posterior
  - Virtual Delivery Agent (VDA)
    - Windows: versão 2402 ou posterior
    - Linux: versão 2407 ou posterior
- Aplicativo Workspace
  - Windows: versão 2402 ou posterior
  - Linux: versão 2408 ou posterior

  - Mac: versão 2409 ou posterior
  - Chrome OS: versão 2409 ou posterior
  - HTML5: versão 2408 ou posterior
- Camada de acesso
  - Citrix Workspace
  - Citrix StoreFront™ 2402 ou posterior

> **Observação:**
>
> Para obter detalhes sobre a configuração do Secure HDX com Linux VDA, consulte a documentação do Linux VDA.

Configuração

O Secure HDX está desativado por padrão. Você pode configurar esse recurso usando a configuração Secure HDX na política do Citrix:

Secure HDX: Define se o recurso deve ser habilitado para todas as sessões, apenas para conexões diretas ou desabilitado.

Considerações

A seguir estão as considerações para usar o Secure HDX:

- Se um usuário tentar se conectar a um host de sessão com o Secure HDX ativado usando um cliente que não oferece suporte ao recurso, a conexão será negada.
- A Continuidade do Serviço não é atualmente suportada com o Secure HDX. Se você tiver a Continuidade do Serviço habilitada em seu ambiente Citrix Cloud™, não poderá acessar nenhum host de sessão que tenha o Secure HDX habilitado se houver uma interrupção do serviço Cloud.
- Se você usa o HDX Insight, observe que o uso do Secure HDX impede a coleta de dados do HDX Insight, pois o NetScaler® não consegue inspecionar o tráfego HDX criptografado. Se você precisar usar o HDX Insight, pode configurar o Secure HDX para ser habilitado apenas para conexões diretas.
- Se você usa o SmartControl, observe que o uso do Secure HDX impede o funcionamento do SmartControl, pois o NetScaler não consegue inspecionar o tráfego HDX criptografado. Se

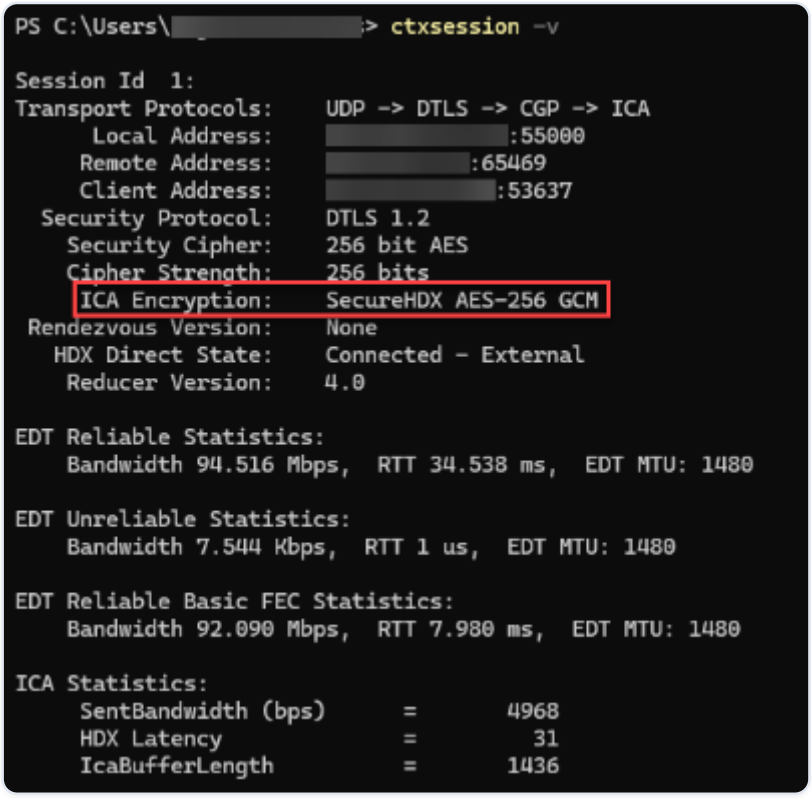
você precisar usar o SmartControl, pode configurar o Secure HDX para ser habilitado apenas para conexões diretas.

- Multi-Stream ICA® não é suportado quando o Secure HDX está habilitado.
- Se você usar soluções de terceiros que dependem da inspeção do tráfego HDX, elas não funcionarão mais se você ativar o Secure HDX, pois o tráfego HDX é criptografado.
- Se você tiver o Secure ICA habilitado nos grupos de entrega nos quais deseja habilitar o Secure HDX, você deve primeiro desabilitar o Secure ICA (Editar grupo de entrega > Configurações do usuário).

Solução de problemas

Para confirmar que o Secure HDX está ativo, você pode usar o utilitário `ctxsession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, abra um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se o Secure HDX estiver em uso, a Criptografia ICA exibirá `SecureHDX AES-256 GCM`.



Quando o Secure HDX não é ativado na sessão

- Certifique-se de que a versão do VDA em uso suporte o recurso de acordo com os requisitos do sistema.

- Confirme se você tem uma política aplicada ao VDA que habilita o Secure HDX e que não há outras políticas com prioridade mais alta desativando o recurso.
- Se o dispositivo cliente estiver se conectando através do NetScaler Gateway ou Gateway Service, certifique-se de que o Secure HDX não esteja configurado como “Somente Conexões Diretas”.
- Se o host da sessão já estava em execução quando você configurou o Secure HDX, reinicie a máquina para garantir que as alterações entrem em vigor.

Lista de permissões de canal virtual

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas os canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

Configuração

A lista de permissões de canal virtual é habilitada por padrão. Você pode configurar esse recurso usando as seguintes configurações na política Citrix:

- **Lista de permissões de canal virtual**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.
- **Limitação de log da lista de permissões de canal virtual**: define o período de limitação para o registro de eventos da lista de permissões de canal virtual.
- **Registro em log da lista de permissões de canal virtual**: define o nível de registro em log para a lista de permissões de canal virtual.

Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando a configuração de política da lista de permissões de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para vários processos

Se houver vários processos, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
    - Permitido: `C:\Program Files\Application*\run1.exe`

  - Não permitido: `C:\Program Files*\run1.exe`

- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`
- Todos os caminhos devem ser locais.

Nota:

- Caminhos de rede não são permitidos.
- O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
- O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

Nota:

> Variáveis de ambiente de usuário não são suportadas.

> O suporte a variáveis de ambiente está disponível a partir do Citrix Virtual Apps and Desktops versão 2209.

Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política de lista de permissões de canais virtuais para o canal virtual e o processo identificados.
5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- Pacote de Otimização HDX RealTime para Skype for Business

Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`
- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

Pacote de Otimização HDX RealTime para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Solução de problemas

Se seu canal virtual personalizado falhar ao abrir, revise as seguintes etapas:

1. Certifique-se de que está usando a versão correta do VDA.
2. Confirme se você tem uma política aplicada ao VDA com o canal virtual personalizado na lista de permissões de canais virtuais e que não há outras políticas com prioridade mais alta sobrescrevendo esta configuração.
3. Verifique o log de eventos no VDA e confirme se o nome do canal virtual relatado corresponde ao definido na lista de permissões.
    a. Se você tiver vários processos, certifique-se de que eles estejam definidos corretamente conforme descrito em Adicionar canais virtuais à lista de permissões.
    b. Se você estiver usando curingas no caminho do processo definido, certifique-se de estar seguindo as diretrizes para Usar curingas.

c. Se você estiver usando variáveis de ambiente no caminho do processo definido, certifique-se de estar seguindo as diretrizes em Usar variáveis de ambiente do sistema.

Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA.

VDA de sessão única

Os seguintes eventos são registrados no log de eventos da máquina VDA de sessão única:

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Sistema	2001	`Picadd`	Informação	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`
Sistema	2002	`Picadd`	Aviso	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>`
Sistema	2003	`Picadd`	Informação	`<username>` abriu o canal virtual personalizado `<vcName>`
Sistema	2004	`Picadd`	Aviso	`<username>` tentou abrir o canal virtual personalizado `<vcName>`
Sistema	2005	`Picadd`	Erro	O caminho fornecido na

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
				política `<pathInPolicy>` não pode ser resolvido para o caminho do processo
Sistema	2007	`Picadd`	Informação	O caminho do processo carregado é `<processPath>`
Sistema	2008	`Picadd`	Erro	Variável de ambiente `<varName>` no caminho da política VC não encontrada

VDA multissessão

Os seguintes eventos são registrados no log de eventos da máquina VDA multissessão:

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Sistema	13	`Rpm`	Informação	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`
Sistema	14	`Rpm`	Aviso	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
				`<processName>`
Sistema	15	`Rpm`	Informações	`<username>` abriu o canal virtual personalizado `<vcName>`
Sistema	16	`Rpm`	Aviso	`<username>` tentou abrir o canal virtual personalizado `<vcName>`
Sistema	17	`Rpm`	Erro	O caminho fornecido na política `<pathInPolicy>` não pode ser resolvido para o caminho do processo
Sistema	18	`Rpm`	Informações	O caminho do processo carregado é `<processPath>`
Sistema	19	`Rpm`	Erro	Variável de ambiente `<varName>` no caminho da política VC não foi encontrada

Canais virtuais de terceiros conhecidos

A seguir estão soluções de terceiros conhecidas que usam canais virtuais Citrix® personalizados. Esta lista não inclui todas as soluções que usam um canal virtual Citrix personalizado.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Software de Desktop Virtual Cisco WebEx Meetings
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Extensões de Cliente Midmark IQPath
- Extensões de Cliente Nuance PowerMic
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings para VDI
- Ultima IA-Connect

Para obter detalhes sobre como adicionar os canais virtuais associados à lista de permissões, entre em contato com os fornecedores das soluções. Alternativamente, siga as etapas descritas na seção Obtendo nomes e processos de canais virtuais.

Lista de Permissão de Canal Virtual para DVC

Você pode usar a lista de permissão de canal virtual para DVC para controlar quais canais virtuais dinâmicos personalizados são permitidos em seu ambiente. Por padrão, nenhum canal virtual dinâmico é permitido. Se houver necessidade de canais virtuais dinâmicos, eles precisam ser adicionados explicitamente à lista de permissão.

Configuração

A lista de permissão de canal virtual para DVC está habilitada por padrão. Você pode configurar esse recurso usando a seguinte configuração na política Citrix®:

- Lista de permissão de canal virtual para DVC: para habilitar ou desabilitar o recurso e adicionar canais virtuais dinâmicos à lista.
- Limitação de log da lista de permissão de canal virtual: define o período de limitação para o registro de eventos da lista de permissão de canal virtual.
- Registro em log da lista de permissão de canal virtual: define o nível de registro em log para a lista de permissão de canal virtual.

Adicionando canais virtuais dinâmicos à lista de permissão

Para adicionar um canal virtual dinâmico à lista de permissão, você precisa das seguintes informações:

1. O nome do plug-in DVC no cliente. Por exemplo, `DvcPlugin1.dll`.
2. O nome do(s) listener(s) DVC. Por exemplo, `ListenerName1`.
3. Os caminhos para os processos que acessam o canal virtual dinâmico na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual dinâmico à lista de permissão usando a configuração de política da lista Permissão de canal virtual para DVC. Para adicionar um canal virtual dinâmico à lista, insira o caminho para o processo que acessa o DVC no host da sessão seguido por uma vírgula, depois o nome do plug-in do lado do cliente seguido por uma vírgula, e o nome do listener usado pelo plug-in. Vários nomes de listener podem ser adicionados separados por vírgulas.

Para um único listener

Usando os exemplos anteriores, adicione a seguinte entrada à lista: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

Para múltiplos listeners

Se houver vários ouvintes, adicione a seguinte entrada à lista: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\App*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\App\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\App\v1.2*.exe`

- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\App\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\App\v1.2\run1.exe`
  - Permitido: `C:\Program Files\App*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\App\v1.2*.exe`
  - Não permitido: `C:\Program Files\App\v1.2*`
- Todos os caminhos devem ser locais.

Dispositivos

O HDX™ oferece uma experiência de usuário de alta definição em qualquer dispositivo, em qualquer local. Os artigos na seção Dispositivos descrevem estes dispositivos:

- Digitalização
- Dispositivo USB genérico
- Mapeamento de Unidade Cliente
- Dispositivos móveis e de tela sensível ao toque
- Dispositivos seriais
- Teclados especiais
- Webcams

Dispositivo USB otimizado vs. genérico

Um dispositivo USB otimizado é aquele para o qual o aplicativo Citrix Workspace™ tem suporte específico. Por exemplo, a capacidade de redirecionar webcams usando o canal virtual HDX Multimedia. Um dispositivo genérico é um dispositivo USB para o qual não há suporte específico no aplicativo Citrix Workspace.

Por padrão, o redirecionamento USB genérico não pode redirecionar dispositivos USB com suporte a canal virtual otimizado, a menos que sejam colocados no modo Genérico.

Em geral, você obtém melhor desempenho para dispositivos USB no modo Otimizado do que no modo Genérico. No entanto, há casos em que um dispositivo USB não possui funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos seus recursos.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados por políticas Citrix®. As principais diferenças são:

Se as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estiverem habilitadas e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidade cliente.

Quando estas condições são verdadeiras, o dispositivo de armazenamento em massa é redirecionado usando o redirecionamento USB genérico:

- Ambas as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estão habilitadas.
- Um dispositivo está configurado para redirecionamento automático.
- Um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão.

Para obter mais informações, consulte `<http://support.citrix.com/article/CTX123015>`.

RECURSO	MAPEAMENTO DE UNIDADE CLIENTE	REDIRECIONAMENTO USB GENÉRICO
Habilitado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado na sessão virtual.	Somente Citrix Virtual Desktops™

Digitalização

Scanner é um dispositivo que digitaliza opticamente imagens, texto impresso, caligrafia ou um objeto e o converte em uma imagem digital.

Se você estiver usando um scanner e seu computador estiver executando o Windows, há uma boa chance de você estar usando o driver de scanner WIA. Este driver é responsável pela comunicação entre seu computador e o scanner.

- **Windows Image Acquisition** (WIA) é o modelo de driver da Microsoft e interface de programação de aplicativos (API) que permite que o software se comunique com hardware de imagem, como scanners.
- **TWAIN** (Windows e Mac) é outro protocolo, que é um protocolo de digitalização que conecta scanners e aplicativos, fornecendo uma interface padrão. O TWAIN permite que os aplicativos adquiram imagens de dispositivos compatíveis com TWAIN (scanners, câmeras digitais, etc.).

Redirecionamento TWAIN

Introdução

TWAIN é um protocolo de digitalização usado para vincular software de imagem a scanners ou câmeras digitais.

Como o TWAIN funciona

- Digitalize seus documentos usando qualquer um dos aplicativos de 32 bits em sua sessão Citrix®.

> **Observação:**
>
> Use um scanner compatível com TWAIN conectado localmente para digitalizar os documentos.

- O módulo de digitalização Citrix redireciona a solicitação TWAIN para o scanner do cliente.
- Assim que a digitalização é concluída, o host da sessão é notificado.

Requisitos

Plano de Controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

Host da Sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11
  - Windows Server 2022 ou posterior
- VDA
  - Versão 1912 ou posterior
- Aplicativo
  - Aplicativo de 32 bits

Dispositivo Cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11
- Aplicativo Workspace
  - Windows: versão 1912 ou posterior
- Scanner
  - Scanner compatível com TWAIN

Configuração

- Instale os drivers TWAIN no endpoint do cliente.
- Configure dispositivos ou aplicativos para selecionar o protocolo de digitalização necessário se eles suportarem TWAIN e WIA.
- Conecte o scanner ao endpoint do cliente localmente (via USB).
- Redirecione dispositivos TWAIN para a sessão via redirecionamento USB, se necessário.

> **Observação:**
>
> Dispositivos TWAIN não funcionam bem com redirecionamento USB, resultando em baixa qualidade de digitalização.

Configurações de Política

Configurações de política para configurar o redirecionamento TWAIN e melhorar a digitalização.

- **Redirecionamento de dispositivo TWAIN do cliente:** para habilitar ou desabilitar o redirecionamento TWAIN.

> **Observação:**
>
> Por padrão, o redirecionamento TWAIN está habilitado.

- **Nível de compactação TWAIN:** para definir os níveis de compactação para imagens do cliente para o host.

Para obter mais detalhes, consulte Configurações de política de dispositivos TWAIN.

Solução de problemas

Experimente o TWAIN com o aplicativo de teste público Twacker, que pode ser baixado neste URL.

Siga os passos para validar o TWAIN em uma sessão de desktop publicada:

1. Instale **Twacker** no VDA.
2. Inicie o **Twacker** (versão de 32 bits).
3. Clique em **Arquivo > Selecionar Origem** e selecione seu scanner na lista.
4. Clique em **Arquivo > Adquirir**.
5. Clique no **botão Digitalizar** para testar seu scanner.

Se o **Twacker** conseguir digitalizar com sucesso, isso confirma que a configuração do **Citrix Virtual Apps and Desktops** está:

- Configurada para redirecionamento USB
- Usando dispositivos TWAIN
- Atendendo a todos os requisitos do dispositivo cliente local

Se você ainda tiver problemas de digitalização em um aplicativo específico, é provável que seja um problema de software.

Dispositivos WIA

Requisitos

- O scanner deve ser compatível com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, via USB).
- Certifique-se de que o scanner esteja usando o serviço local do Windows Image Acquisition e não o driver TWAIN.

- Certifique-se de que nenhuma política seja aplicada à conta de usuário usada para o teste, e que esteja limitando a largura de banda dentro da sessão ICA®. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Lista de permissões de aplicativos de aquisição de imagem do Windows

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento de scanner do Windows Image Acquisition. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém o Windows Image Acquisition. Por padrão, nenhum aplicativo tem acesso ao Windows Image Acquisition.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração Lista de permissões de aplicativos do Windows Image Acquisition na lista de recursos gerenciados através do registro.

Para obter informações sobre as configurações de política, consulte Configurações de política de dispositivos WIA.

Dispositivos USB genéricos

Introdução

O recurso de redirecionamento USB genérico permite o redirecionamento de dispositivos USB de máquinas cliente para sessões HDX™, dando aos usuários finais a capacidade de interagir com uma ampla seleção de dispositivos USB genéricos em sua sessão HDX. Isso é útil em cenários onde os usuários precisam usar dispositivos especializados que não possuem suporte otimizado ou onde é inadequado.

> **Nota:** Dispositivos USB não otimizados para suporte a canal virtual recorrerão ao canal virtual USB Genérico usando redirecionamento USB bruto.

Como funciona?

O redirecionamento USB genérico funciona em um nível baixo e redireciona mensagens de solicitação e resposta USB entre máquinas cliente e o desktop virtual XenDesktop®.

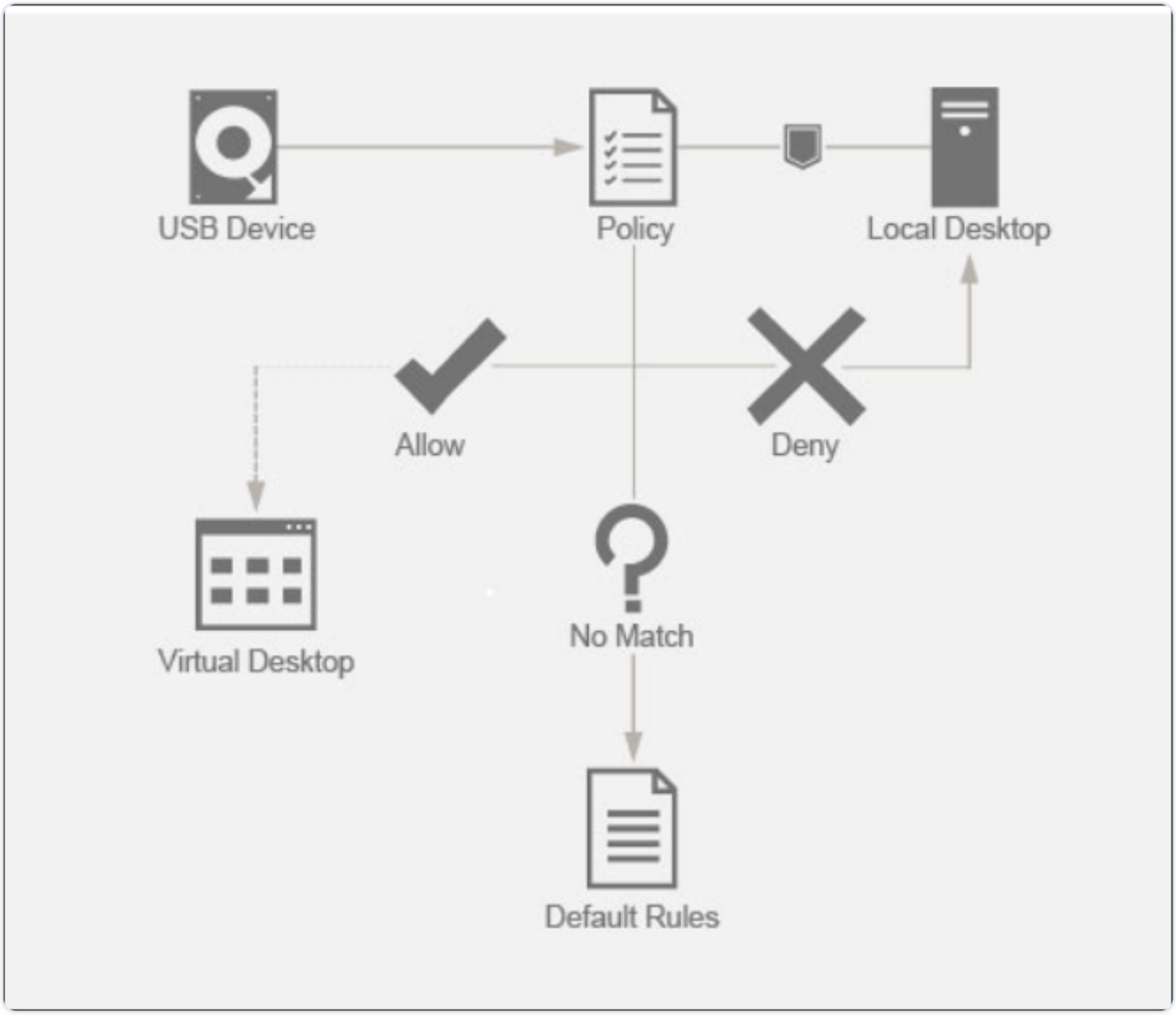
Ele evita a exigência de drivers de dispositivo compatíveis na máquina cliente e espera-se que o driver seja suportado apenas no desktop virtual. As regras de política de redirecionamento USB seguem uma certa ordem de precedência que permitem que políticas do lado do cliente e regras padrão sejam respeitadas depois que as regras de política DDC forem avaliadas e aplicadas. Isso

permite que os administradores Citrix evitem que quaisquer dispositivos não autorizados/falsificados sejam redirecionados dentro de uma sessão.

Além disso, o registro de eventos de dispositivos não autorizados tentando acessar a sessão remota pode ser auditado e sinalizado, e os administradores podem tomar medidas adicionais para evitar a exfiltração de dados.

Quando um usuário conecta um dispositivo USB, o host da sessão o verifica em relação a cada regra de política consecutivamente até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva.

- Se a primeira correspondência for uma regra de Permissão, o dispositivo é redirecionado para o desktop virtual.
- Se a primeira correspondência for uma regra de Negação, o dispositivo não é redirecionado para a sessão e só está disponível para uso no dispositivo do usuário local. Se nenhuma correspondência for encontrada, as regras padrão são usadas.



Configuração

O redirecionamento USB está desabilitado por padrão. Você pode configurar o redirecionamento USB genérico usando as seguintes configurações na política Citrix®:

- **Redirecionamento de dispositivo USB do cliente**: para habilitar ou desabilitar o redirecionamento USB
- **Regras de redirecionamento de dispositivo USB do cliente**: para especificar uma ação de dispositivo específica, ou seja, para permitir ou negar acesso a um dispositivo específico
- **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**: para especificar regras para filtrar, dividir e conectar automaticamente dispositivos USB
- **Regras de otimização de dispositivo USB do cliente**: para desabilitar a otimização ou alterar o modo de otimização
- **Permitir que dispositivos USB existentes sejam conectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB existentes que estão conectados a um endpoint de cliente no início de uma sessão HDX™
- **Permitir que dispositivos USB recém-chegados sejam detectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB que estão conectados a um endpoint de cliente durante uma sessão HDX

Consulte Configurações de Política USB para obter mais detalhes.

Como configurar o redirecionamento USB

Por padrão, a configuração de redirecionamento USB está desabilitada. Para usá-lo, a política de redirecionamento USB e as regras de redirecionamento específicas devem ser habilitadas e configuradas no DDC.

> **Observação:**
>
> Se você estiver usando componentes anteriores à versão 2212 ou estiver usando o Workspace App para Linux/Mac, consulte Configuração de Redirecionamento USB Legado para obter detalhes sobre como configurar o redirecionamento USB.

Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.

3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

Criando Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em relação a cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de **Permitir**, o dispositivo correspondente tem permissão para ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de **Negar**, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão são usadas.

REGRAS DE DISPOSITIVO

Assim como nos dispositivos USB regulares, as regras de dispositivo definidas na política ou na configuração do aplicativo cliente Citrix Workspace™ no endpoint selecionam os dispositivos para encaminhamento. O aplicativo Citrix Workspace usa essas regras para decidir quais dispositivos USB permitir ou impedir de serem encaminhados para a sessão remota.

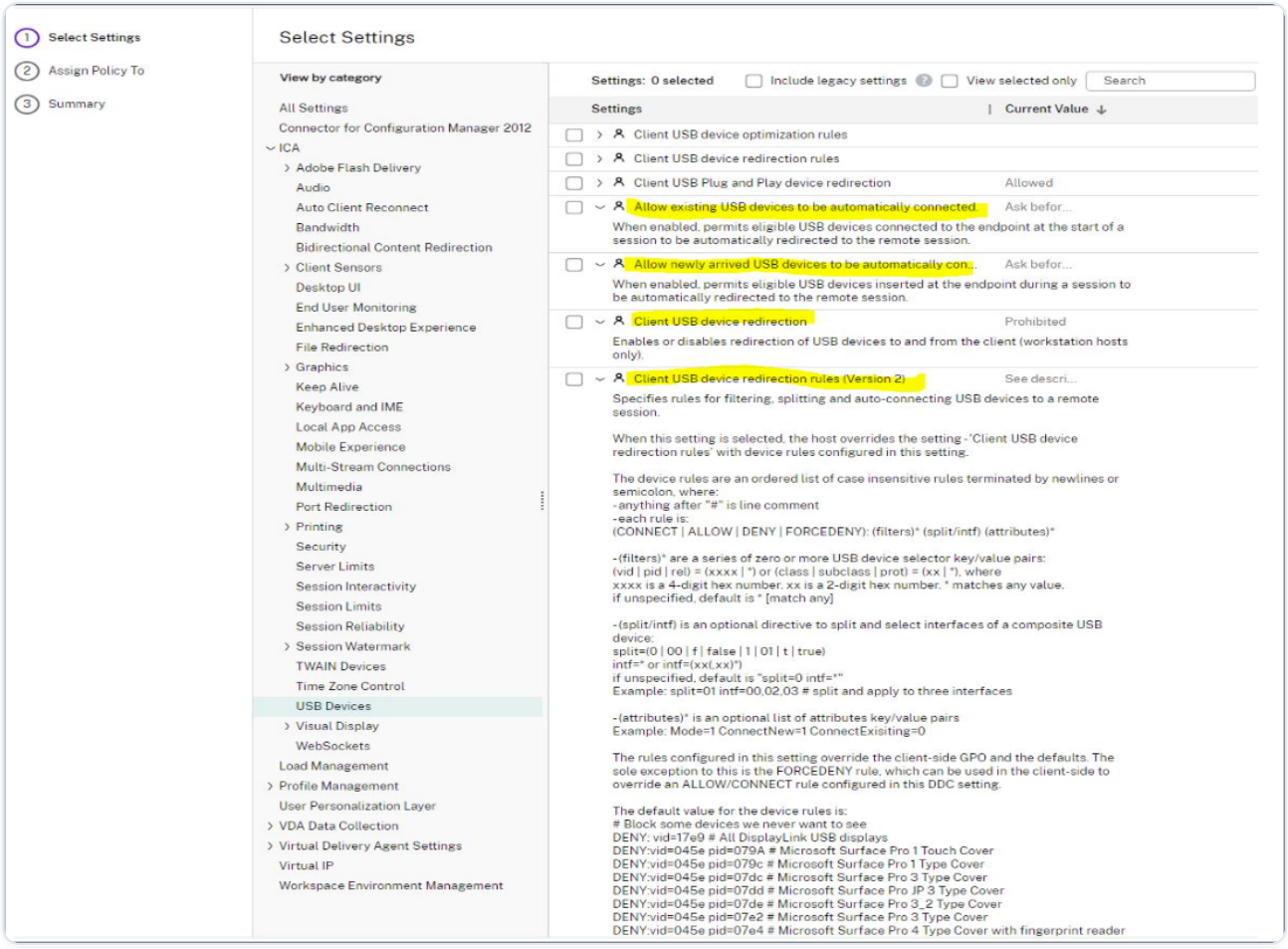
Cada regra consiste em uma palavra-chave de ação (**Permitir, Conectar ou Negar**), dois pontos (:), e zero ou mais parâmetros de filtro que correspondem a dispositivos reais no subsistema USB dos endpoints. Esses parâmetros de filtro correspondem aos metadados do descritor de dispositivo USB usados por cada dispositivo USB para se identificar.

As regras de dispositivo são texto simples, com cada regra em uma única linha e um comentário opcional após um caractere #. As regras são correspondidas de cima para baixo (ordem de prioridade decrescente). A primeira regra que corresponde ao dispositivo ou interface filho é aplicada. Regras subsequentes que selecionam o mesmo dispositivo ou interface são ignoradas.

Exemplo: ALLOW VID=1050 PID=0421 #Device1 **Exemplo:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

PALAVRA-CHAVE	DESCRIÇÃO
CONNECT	Use esta palavra-chave para permitir que os dispositivos sejam redirecionados pelo canal virtual USB, bem como para permitir que sejam redirecionados automaticamente durante o lançamento da sessão e na inserção.

PALAVRA-CHAVE	DESCRIÇÃO
ALLOW	Use esta palavra-chave para permitir que os dispositivos sejam redirecionados pelo canal virtual USB
DENY	Use esta palavra-chave para negar que os dispositivos sejam redirecionados pelo canal virtual USB



Definindo a política no DDC:

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas de ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar.

   Por Exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Armazenamento em Massa

> **Observação:**
>
> Se um administrador Citrix marcar **Usar valor padrão** e clicar em **Salvar**, as regras padrão podem ser encontradas no seguinte registro no VDA.
>
> **Cuidado!**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Observação:**
>
> As políticas ainda podem ser definidas no dispositivo cliente usando regras de dispositivo de política de grupo, mas isso não é mais necessário em versões mais recentes do CVAD e do CWA.
>
> Para configuração legada de dispositivos USB, consulte Configuração de Redirecionamento USB Legado.

Configurar redirecionamento automático de dispositivos USB (Opcional)

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use as DeviceRules no endpoint do cliente ou na política do DDC. Esta política pode ser definida no DDC, no cliente usando um GPO, usando as Preferências do Citrix Workspace ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

Definindo a política no DDC:

Existem duas políticas no DDC que podem ser configuradas para permitir o redirecionamento automático de dispositivos USB-

- Permitir que dispositivos USB existentes sejam conectados automaticamente
- Permitir que dispositivos USB recém-chegados sejam conectados automaticamente

a. Abra **políticas do Citrix Web Studio** e clique na guia **Políticas**.

b. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.

c. Edite a configuração **Permitir** que dispositivos USB existentes sejam conectados automaticamente.

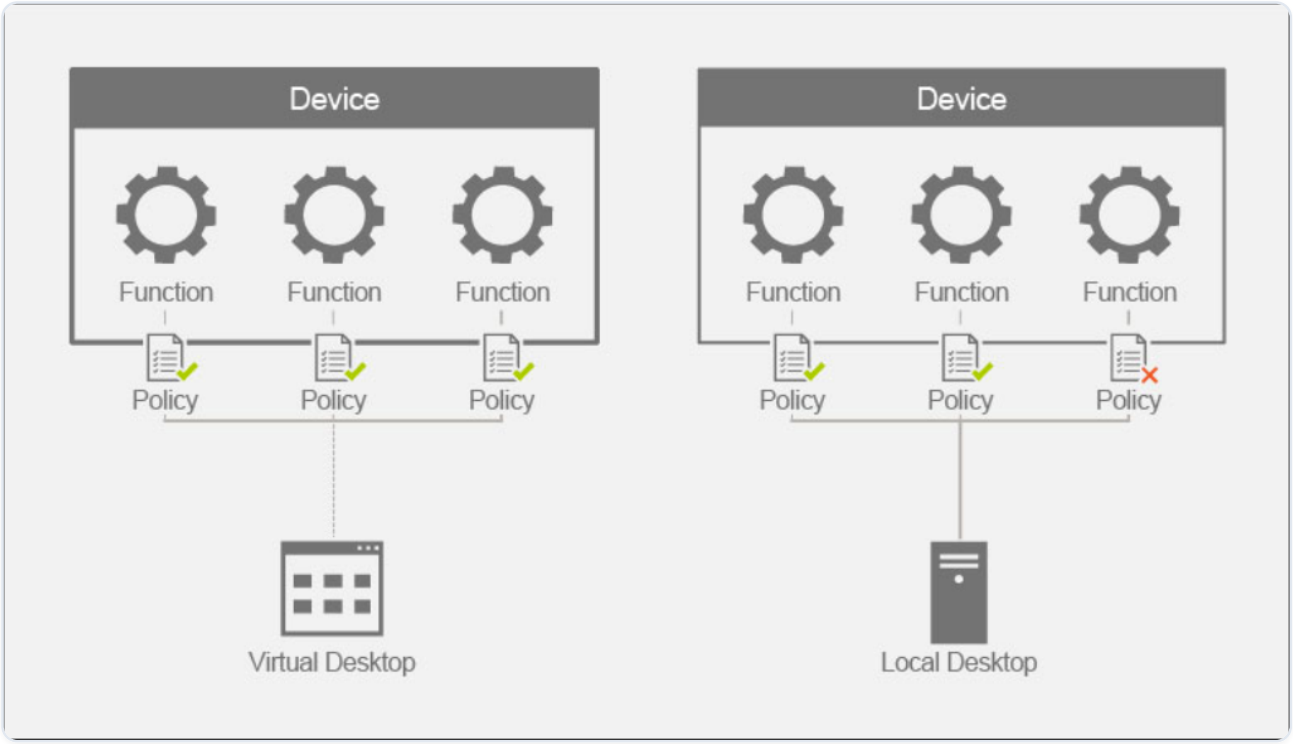
d. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

e. Edite a configuração **Permitir** que dispositivos USB recém-chegados sejam conectados automaticamente.

f. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Dispositivos Compostos e Divisão de Dispositivos

Um dispositivo USB composto é um único dispositivo que age como múltiplos dispositivos USB independentes conectados a um computador. Ele possui um único conector USB, mas pode expor múltiplas interfaces ao computador, cada uma com seu próprio conjunto de funcionalidades. Quando um usuário conecta um dispositivo USB composto, o dispositivo host verifica todas as funções (interfaces) em relação a cada regra de política. Se a primeira correspondência para qualquer função (interface) for uma regra de Negação, a regra é considerada definitiva para o dispositivo composto e o dispositivo é negado. Se a primeira correspondência para uma função (interface) for uma regra de Permissão, o dispositivo host continua a corresponder as regras à próxima função (interface). O dispositivo composto é permitido se nenhuma função (interface) for negada por uma regra de política. Se a correspondência definitiva para o dispositivo composto for uma Regra de Negação, o dispositivo estará disponível apenas para o desktop local; caso contrário, o dispositivo é redirecionado para o desktop virtual. Se nenhuma correspondência for encontrada, as regras padrão são usadas.



Podemos dividir o dispositivo composto usando as regras apropriadas na política de regras de redirecionamento de dispositivo (Versão 2) para permitir apenas funcionalidades específicas de um dispositivo composto. Por exemplo, podemos querer usar apenas as funções HID de uma chave FIDO2, mas não a funcionalidade de smartcard. Nesse caso, definiríamos as regras conforme ilustrado abaixo:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da série 5 da Yubikey.
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Função de smartcard da série 5 da Yubikey bloqueada.

> **Dica:**
>
> Ao criar novas regras de política, consulte os Códigos de Classe USB, disponíveis no site da USB.

Configurando uma mesa digitalizadora de assinaturas

1. Instale o driver de dispositivo apropriado no host VDA.
2. Habilite a configuração de política de **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio™**.

3. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Defina as informações de **VID** e **PID** para a mesa digitalizadora de assinaturas que precisa ser redirecionada e clique em **Salvar**. Por exemplo: **Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. Edite a configuração de política **Regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo juntamente com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=06A8 PID=0057 class=03 #Dispositivo de entrada operando no modo de captura
5. Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
7. Edite a configuração da política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, os lançamentos de sessão subsequentes terão o dispositivo sendo redirecionado automaticamente e não exigirão nenhuma ação adicional do usuário final.

> **Observação:**
>
> Substitua o VID e o PID pelos VID e PID reais do dispositivo a ser redirecionado.

Configurando o teclado Bloomberg usando redirecionamento USB

1. Habilite a configuração da política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Os teclados Bloomberg 5 são definidos por padrão na configuração da política **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)** e nenhuma ação administrativa adicional é necessária.

3. Edite a configuração da política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração da política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, as chaves Bloomberg serão apresentadas automaticamente em sessões HDX™ subsequentes e não exigirão nenhuma ação adicional do usuário final.

Configurando uma chave FIDO2 usando redirecionamento USB

A Citrix recomenda usar o redirecionamento FIDO2 para usar chaves FIDO2 em suas sessões HDX. No entanto, pode haver situações em que você deve redirecionar chaves FIDO2 usando o redirecionamento USB. Isso inclui cenários em que o redirecionamento FIDO2 não está disponível porque o recurso não é compatível com o cliente, o VDA ou o sistema operacional (por exemplo, Windows Server 2016).

Também pode haver situações em que a chave tem vários modos ativados, mas você só quer permitir um subconjunto deles em suas sessões HDX. Por exemplo, você pode querer permitir FIDO2 e OTP, mas bloquear o cartão inteligente.

As etapas a seguir ilustram como você pode configurar uma chave FIDO2 usando o redirecionamento USB (Yubikey vid=1050, pid=0407).

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a configuração de política **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**.
    a. Defina as informações de **VID** e **PID**, bem como a configuração de divisão do dispositivo para que a chave FIDO2 seja redirecionada na sessão e clique em **Salvar**.
    b. **Conectar**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da série 5 do Yubikey.
    c. **Negar**: VID=1050 PID=0407 split=01 intf=02 # Função de cartão inteligente da série 5 do Yubikey bloqueada.

3. Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez configuradas essas configurações, os teclados FIDO2 serão automaticamente apresentados nas sessões HDX subsequentes e não exigirão nenhuma ação adicional do usuário final.

Configurando um mouse 3D usando redirecionamento USB

Atualmente, os drivers do mouse espacial 3dConnexion são suportados apenas em sistemas operacionais de estação de trabalho (Win 10 e Win11). Eles não funcionam em sistemas operacionais de servidor. A seguir estão as etapas para configurar um SpaceMouse Enterprise em um sistema operacional de estação de trabalho (vid=046D, pid=C016).

1. Instale o driver do Windows mais recente no host VDA.
2. Ativar a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
3. Editar a configuração de política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Adicione as informações de **VID** e **PID** para a mesa digitalizadora que precisa ser redirecionada e clique em **Salvar**. Por exemplo: **Conectar**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Editar a configuração de política **Regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo junto com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=046D PID=C016 class=03 #Dispositivo de entrada operando no modo de captura
5. Editar a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

7. Editar a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Configurando dois ou mais dispositivos usando redirecionamento USB com regras de dispositivo diferentes

Vários dispositivos podem ser redirecionados dentro da sessão HDX com regras de dispositivo diferentes. Um administrador pode querer redirecionar um dispositivo automaticamente enquanto oferece uma opção ao usuário final para redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Ativar a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Editar a configuração de política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Adicione as informações de **VID** e **PID** dos dois dispositivos a serem redirecionados com a regra de dispositivo apropriada na sessão e clique em **Salvar**.
    b. **Permitir**: VID=0911 PID=0c1c #Microfone de fala Phillips.
    c. **Conectar**: VID=06A8 PID=0043 class=03 # Bloco de assinatura Topaz HSB
3. Edite a configuração da política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração da política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas configurações estejam configuradas, o bloco de assinatura Topaz HSB será automaticamente apresentado em sessões HDX subsequentes e não exigirá nenhuma ação adicional do usuário final. O microfone de fala Phillips, por outro lado, exigirá que o usuário final habilite o redirecionamento no Connection Center ou na guia Dispositivos do CDViewer.

Solução de problemas

As etapas a seguir devem ser seguidas para solucionar problemas relacionados ao redirecionamento USB:

1. Valide se os requisitos do sistema estão sendo atendidos para o redirecionamento USB. Isso inclui versões corretas do CVAD e CWA, dispositivos suportados e drivers de dispositivo na plataforma do sistema operacional em questão.
2. Certifique-se de que a configuração seja apropriada com base nas versões e plataformas dos componentes em uso em seu ambiente. Consulte a nota em Configuração de Redirecionamento USB Legado para obter detalhes sobre os componentes que exigem configurações de configuração legadas.
3. Valide se o dispositivo está listado entre os dispositivos que o cliente enumerou.

    a. Barra de ferramentas de Preferências do Workspace: Observe os dispositivos enumerados na guia Dispositivos da barra de ferramentas de Preferências do aplicativo Workspace (Clique com o botão direito do mouse em **ícone do CWA > Connection Center > Preferências**… Clique na guia **Dispositivos**).

    b. `CtxUsbDiagnostics.exe` (Recomendado): Execute esta ferramenta em uma janela de prompt de comando. A saída fornece informações específicas do dispositivo para uma sessão específica. Ela informará se um dispositivo está sendo redirecionado ou não. Também informará se um conjunto de regras de dispositivo está impedindo o redirecionamento do dispositivo. Consulte Ferramenta de Diagnóstico para obter mais informações.

    c. USBView ou outras ferramentas de terceiros: Execute uma ferramenta de terceiros como o USBView na máquina do endpoint/cliente para garantir que o dispositivo seja detectado no endpoint.

4. Se você vir o dispositivo sendo enumerado:

    a. Se você vir uma regra de Negação na saída da ferramenta CtxUsbDiagnostics para um dispositivo específico, verifique as políticas configuradas no Studio e certifique-se de que as regras estejam configuradas corretamente na política da Versão 2. Se a regra de negação não aparecer na política do Studio, verifique a política do lado do cliente e, finalmente, os padrões do lado do cliente nessa ordem para encontrar a regra de negação correspondente.

    b. Se não houver uma regra de negação na saída do CtxUsbDiagnostics, o CWA permitirá o redirecionamento do dispositivo marcando/clicando no botão apropriado na guia

dispositivos da janela Preferências (Dispositivos > Gerenciar dispositivos). Um dispositivo, uma vez redirecionado, estará disponível na sessão. Isso pode ser verificado consultando o gerenciador de dispositivos / USBView ou aplicativo similar na sessão HDX.

5. Se você não vir o dispositivo sendo apresentado dentro da sessão:

    a. É possível que o driver de dispositivo correto não esteja instalado corretamente no host VDA. Certifique-se de que as versões mais recentes dos drivers de dispositivo estejam instaladas corretamente no host VDA. Alguns drivers de dispositivo não são suportados em máquinas de servidor de terminal, portanto, certifique-se de que não seja esse o caso com o dispositivo que você está tentando redirecionar.

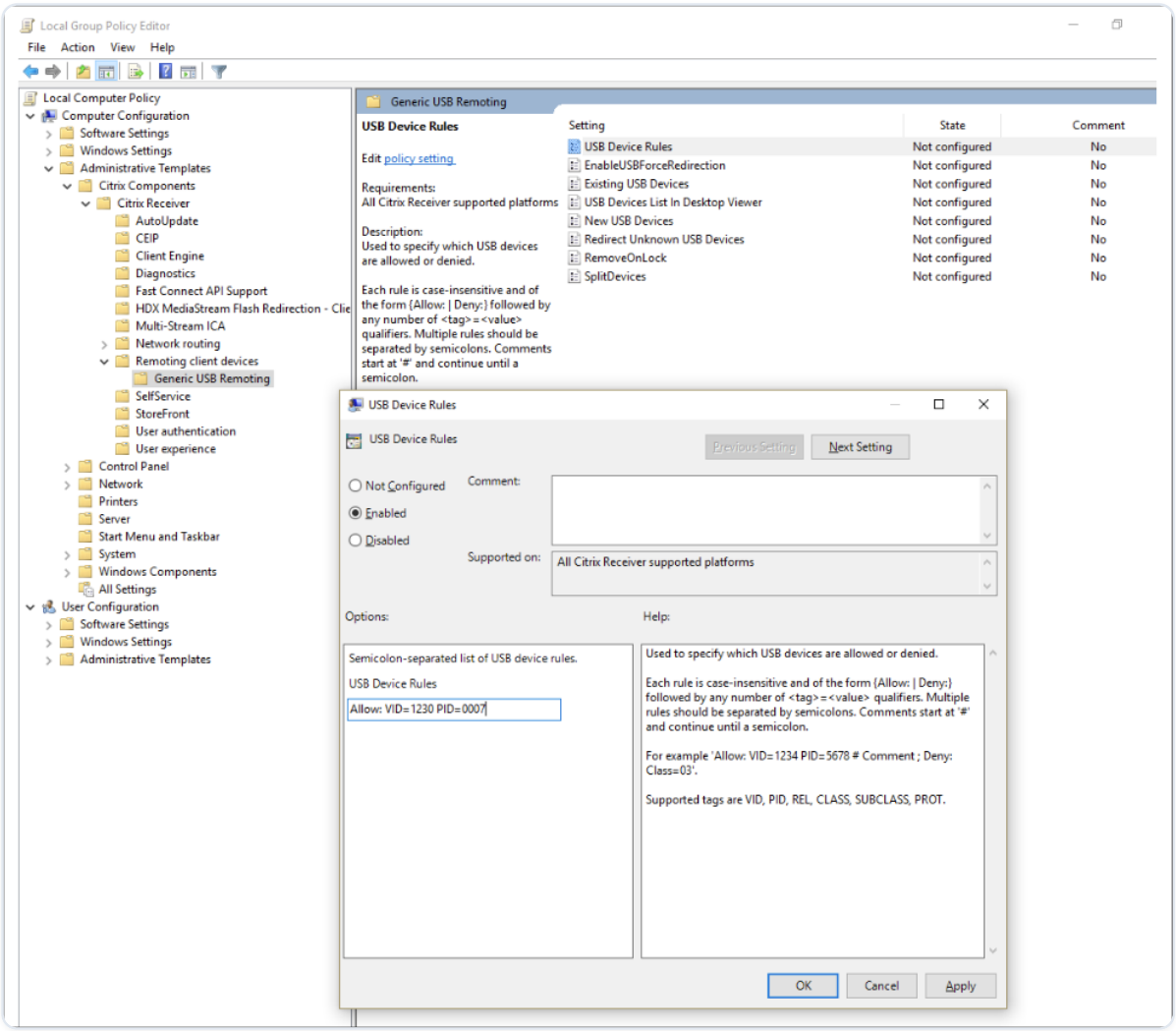
    b. Certifique-se de que o dispositivo não esteja sendo usado no endpoint do cliente. Alguns dispositivos também exigem que os drivers sejam instalados no endpoint do cliente, e isso pode impedir que sejam redirecionados na sessão.

6. Valide se as regras relacionadas ao USB estão configuradas corretamente no endpoint do cliente:

    a. **CWA para Windows** :

        i. Validar se a política de grupo no cliente (adicionar mais detalhes e SS para isso) está configurada apropriadamente e não entra em conflito com as regras definidas no Studio.

        ii. Validar as regras padrão no registro do cliente.



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA para Linux - Para triar problemas do CWA para Linux, consulte a documentação USB para CWA para Linux

c. CWA para Mac - Para triar problemas do CWA para Mac, consulte CWA para Mac

Observação:

- No TSVDA, os dispositivos de áudio são bloqueados por padrão para usar o redirecionamento USB. A maneira recomendada de usar esses dispositivos é utilizando o VC de Áudio otimizado.
- Às vezes, dispositivos USB compostos podem não ser divididos automaticamente, mesmo que uma regra de redirecionamento de dispositivo correta esteja configurada para dividir o dispositivo. Esse problema ocorre porque o dispositivo está em modo de

baixo consumo de energia. Nesses casos, o dispositivo filho que entra no modo de baixo consumo de energia pode não estar presente na lista de dispositivos. Você pode usar as seguintes soluções alternativas para resolver esse problema:

  - Desconecte a sessão, insira o dispositivo USB e reconecte-se à sessão.
  - Desconecte o dispositivo USB e conecte-o novamente. Essa ação faz com que o dispositivo saia do modo de baixo consumo de energia.

- Às vezes, as configurações de economia de bateria USB podem estar ativadas para otimizar a vida útil da bateria. Se o endpoint do cliente entrar em suspensão, o dispositivo USB poderá ser desconectado. Nesse cenário, talvez seja necessário desconectar e reconectar o dispositivo para apresentá-lo novamente na sessão.

Logs de Eventos

Os administradores agora podem monitorar dispositivos não autorizados que os usuários podem tentar redirecionar e tomar as ações apropriadas. Aqui estão algumas das mensagens de evento que serão registradas no Visualizador de Eventos no host VDA para dispositivos que podem ser redirecionados e para dispositivos que não podem.

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

Ferramenta de Diagnóstico USB

`CtxUsbDiagnostics.exe` é uma ferramenta de linha de comando no VDA para ajudar os administradores Citrix a diagnosticar e resolver problemas de redirecionamento de dispositivos USB experimentados no cliente de forma expedita. Esta ferramenta utilitária coleta informações vitais necessárias para triar problemas de configuração associados a dispositivos USB conectados ao cliente que estão falhando ao redirecionar dentro de uma sessão HDX.

```
> **Note :**
>
> Running Command Prompt or Powershell as an administrator is required to
```

```
ensure the tool has the necessary permissions to perform system-level
operations.
```

Requisitos

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ Versão 2311 ou posterior

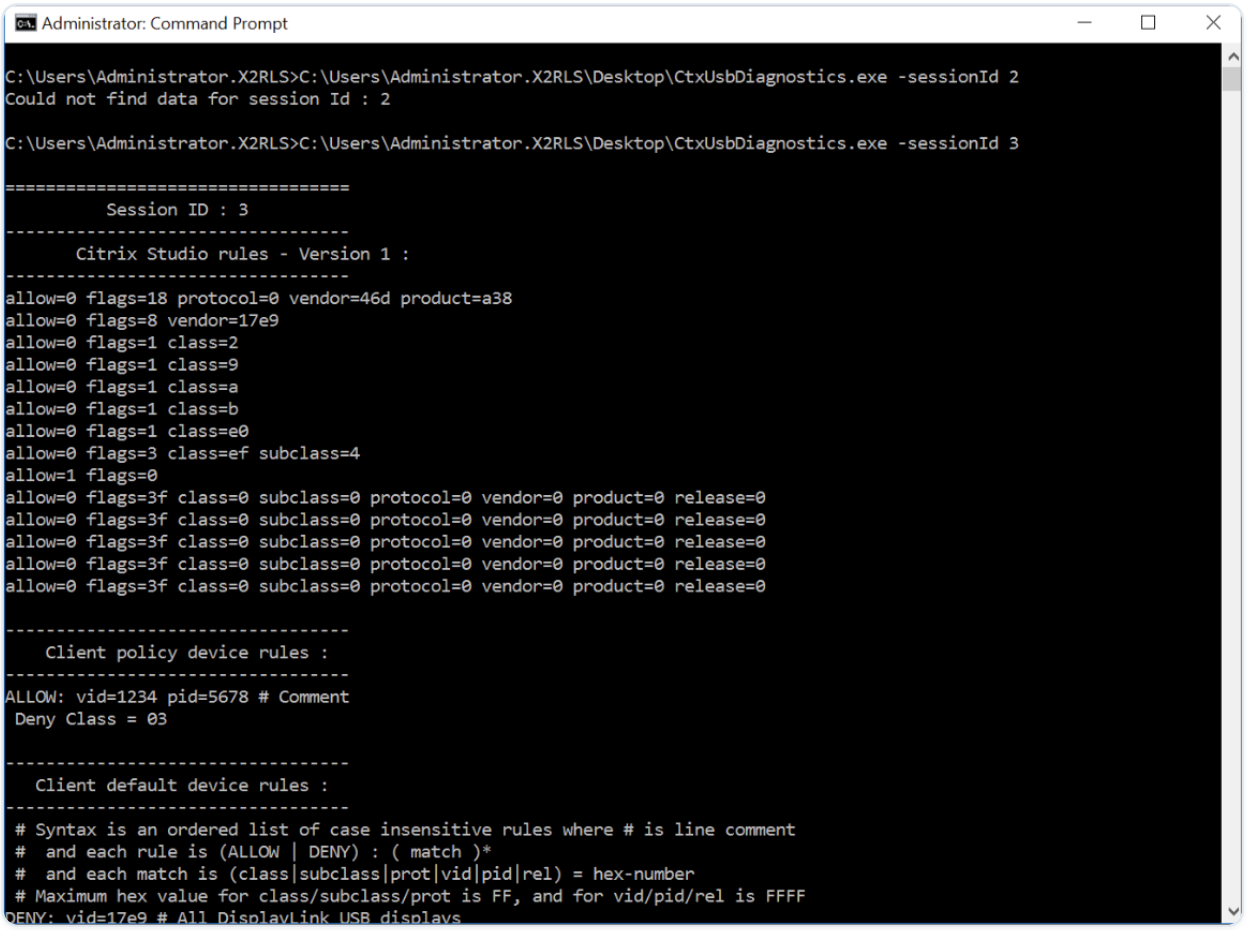
Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Workspace App
  - Windows: versão 2311 ou posterior

O que a ferramenta faz?

A ferramenta atualmente fornece:

- ID da Sessão
- Políticas de dispositivo VDA (regras de dispositivo definidas no Studio)
- Dispositivos cliente e políticas de dispositivo cliente (regras de dispositivo)
- Lista de dispositivos, seu estado de redirecionamento e por que foram permitidos ou negados



> **Nota :**
>
> O administrador pode ver informações do dispositivo para todas as sessões ativas.

Informações Exibidas

- **Regras do Citrix Studio - Versão 1/2**
  - As regras DDC indicam o uso da política legada “**Regras de redirecionamento de dispositivo USB do cliente**” ou “**Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**” no Studio. As informações listadas nesta seção listam todas as regras configuradas pelo administrador Citrix®.

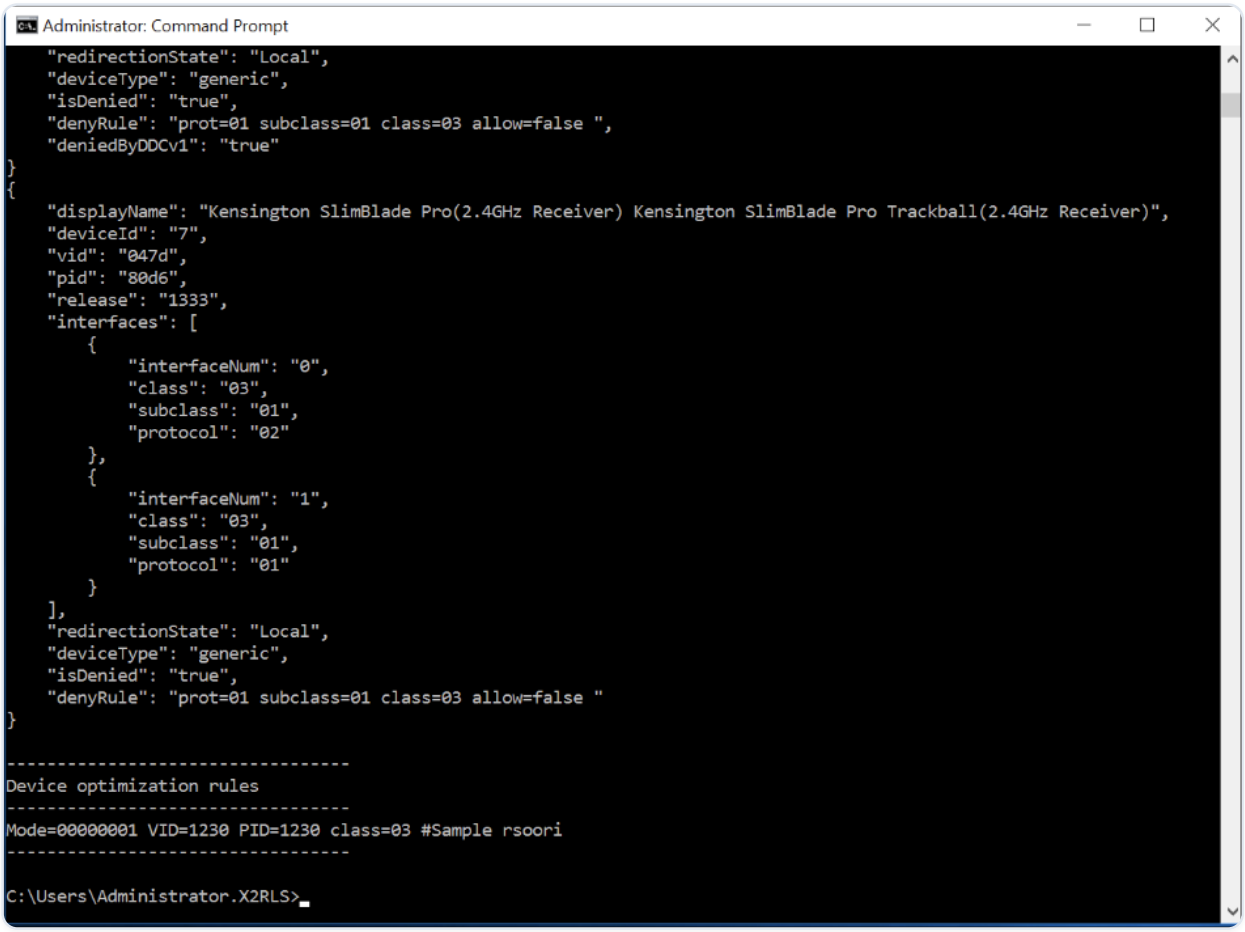
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Regras Padrão de Dispositivo do Cliente**
  - Esta seção lista as regras que são definidas no registro do cliente.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Regras de otimização de dispositivo**
  - A seção lista as regras de otimização de dispositivo conforme definido em "Regras de otimização de dispositivo USB do cliente.



Lista de Dispositivos

Esta seção lista informações valiosas sobre cada dispositivo conectado ao endpoint do cliente, as informações de hardware, se está sendo redirecionado ou não, se a regra de redirecionamento de dispositivo correta está definida ou não, e assim por diante.

NOME DA TAG	DESCRIÇÃO
displayName	Lista o nome comum do dispositivo.
ID do Fornecedor	ID do Fornecedor
ID do Produto	ID do Produto
Interfaces	Esta subseção lista todas as interfaces caso o dispositivo composto tenha sido dividido em vários dispositivos filhos.
InterfaceNum	Indica o índice do descritor da interface
classe	Código da Classe

NOME DA TAG	DESCRIÇÃO
subclasse	Código da Subclasse
protocolo	Protocolo
redirectionState	**Local** indica que o dispositivo não é redirecionado na sessão ICA®. **ThisSession** indica que o dispositivo é redirecionado na sessão ICA. **OtherSession** indica que o dispositivo é redirecionado em outra sessão ICA.
optiEnabled	**true** indica que o dispositivo está otimizado. **false** indica que o dispositivo não está otimizado e a transferência de dados ocorre através do canal virtual USB.
deviceType	**genérico** indica que o dispositivo não possui um canal virtual otimizado e o tráfego está fluindo através do canal virtual USB. **otimizado** implica que a transferência de dados associada ao dispositivo está ocorrendo através de um canal virtual dedicado.
isDenied	**true** indica que o dispositivo não é redirecionado devido a uma regra de política definida pelo administrador. `false` indica que o dispositivo é redirecionado devido à política aplicada.
denyRule	Este campo é útil se **isDenied** estiver definido como `true`. Ele informa ao administrador o conjunto de regras específico na política que está resultando no não redirecionamento do dispositivo.

Configuração de Redirecionamento USB Legado

Se você estiver usando componentes anteriores à versão 2212 ou se estiver usando o CWA para Linux, siga este guia para configurar o redirecionamento USB em seu ambiente.

Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.
3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

Criando Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em relação a cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de Permissão, o dispositivo correspondente terá permissão para ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

Definindo a política no DDC:

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente**.
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar. Por exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Mass Storage

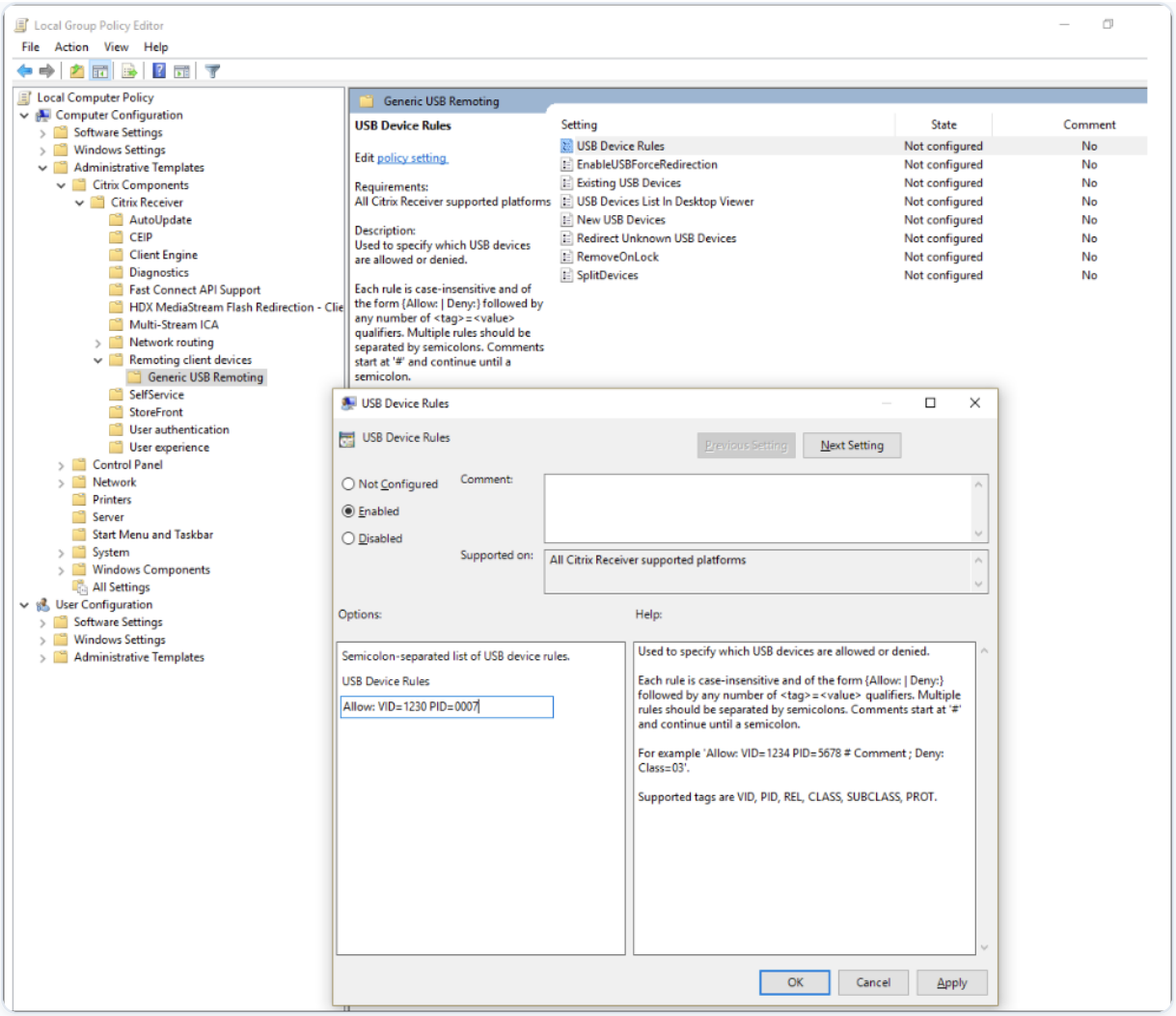
> **Observação:**
>
> Se um administrador Citrix® marcar Usar valor padrão e clicar em Salvar, as regras padrão podem ser encontradas no seguinte registro no VDA.
>
> **Cuidado!:**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

Usando GPOs no cliente:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos de cliente de acesso remoto > Acesso Remoto USB Genérico**.
2. Abra a **configuração Regras de Dispositivo USB** e ative a configuração. Adicione a regra de Dispositivo USB como neste exemplo, A regra Permitir: VID=1230 PID=0007 permite o dispositivo com ID de Fornecedor 1230 e ID de Produto 0007.

Observação:

Use a regra Permitir: VID=xxxx PID=xxxx quando um dispositivo específico deve estar no topo da lista de regras de dispositivo.



Observação:

> Uma ferramenta como USBView ou até mesmo a barra de ferramentas Conexão pode ser usada para determinar os detalhes do dispositivo, como VID e PID.

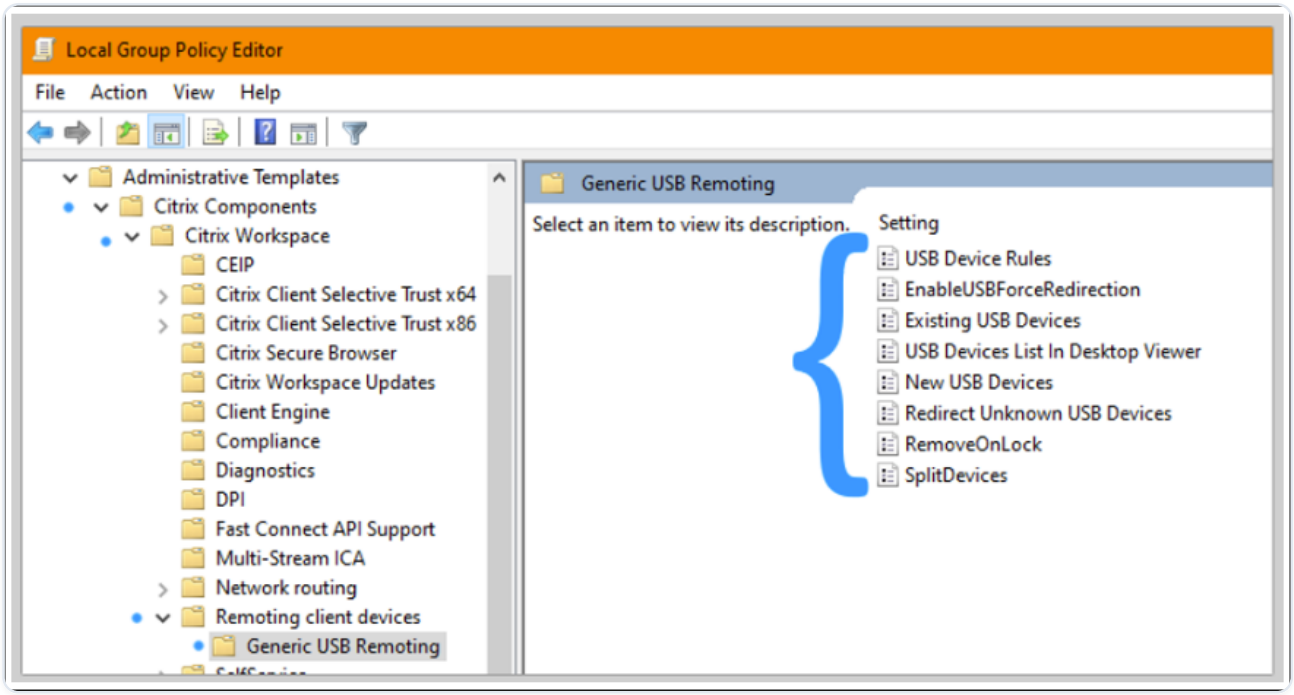
Configurar o redirecionamento automático de dispositivos USB

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use a configuração da política DeviceRules no endpoint do cliente.

Esta política pode ser definida no cliente usando um GPO, registro do lado do cliente, usando as Preferências do Citrix Workspace™ ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

Usando GPOs no cliente:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos de cliente de acesso remoto > Acesso Remoto USB Genérico**.
2. Abra **Novos Dispositivos USB**, selecione **Ativado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Ativado** e clique em **OK**.

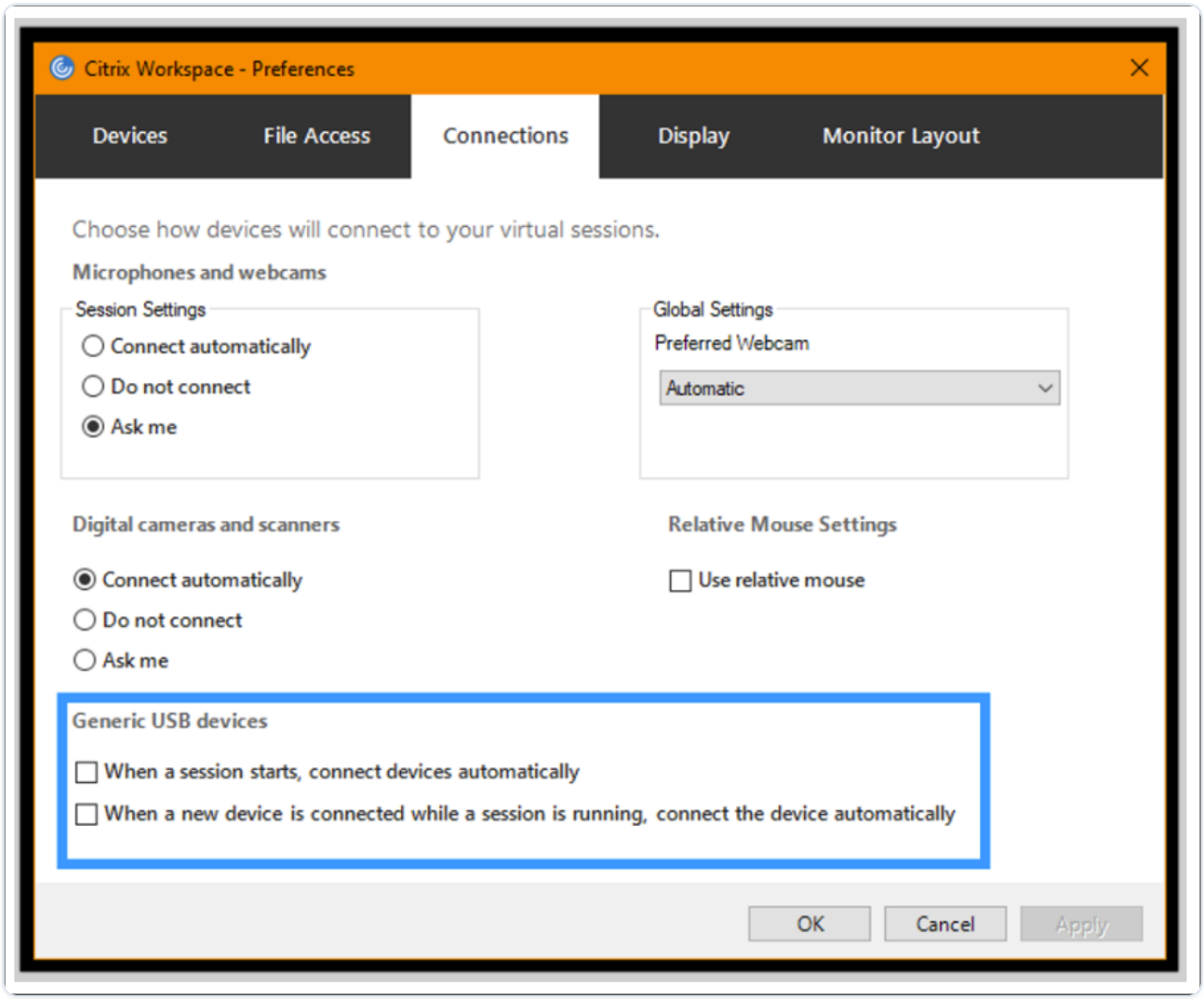


Usando o Citrix Connection Center:

1. Vá para **Preferências do Citrix Workspace > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão é iniciada, conectar dispositivos automaticamente
    b. Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

Usando a barra de ferramentas de conexão do CDViewer:

1. Após o início de uma sessão, clique no menu suspenso **CDViewer** e selecione a guia **Preferências do Citrix Workspace > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão é iniciada, conectar dispositivos automaticamente
    b. Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **Aplicar** e **OK** para salvar a política.



Para as configurações baseadas no cliente, as chaves de registro são definidas no dispositivo cliente no seguinte local:

> **Cuidado!:**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

Configurando dois ou mais dispositivos usando o redirecionamento USB com regras de dispositivo diferentes

Vários dispositivos podem ser redirecionados dentro da sessão HDX™ com regras de dispositivo diferentes. Um administrador pode querer redirecionar um dispositivo automaticamente, enquanto oferece uma opção ao usuário final para redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Habilite a configuração de política **Redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a configuração **Regras de dispositivo USB** no GPO do lado do cliente.
    a. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
    b. Abra a **configuração de Regras de Dispositivo USB** e habilite a configuração. Adicione a regra de Dispositivo USB como neste exemplo: A regra **Permitir: VID=0911 PID=0c1c** permite o dispositivo com **ID de Fornecedor 0911** e **ID de Produto 0c1c**, mas ele não será redirecionado automaticamente. A regra **Conectar: VID=06A8 PID=0043** redirecionará automaticamente o dispositivo com **ID de Fornecedor 06A8** e **ID de Produto 0043**, desde que as políticas de redirecionamento automático mencionadas na etapa 3 estejam definidas.
    c. **Permitir**: VID=0911 PID=0c1c #Microfone de fala Phillips.
    d. **Conectar**: VID=06A8 PID=0043 class=03 # Mesa digitalizadora Topaz HSB
3. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
4. Abra **Novos Dispositivos USB**, selecione **Habilitado** e clique em **OK**.
5. Abra **Dispositivos USB Existentes**, selecione **Habilitado** e clique em **OK**.

Uma vez que essas configurações estejam configuradas, a mesa digitalizadora Topaz será redirecionada automaticamente dentro da sessão HDX e será necessária uma ação adicional do usuário final (selecionar a opção Redirecionar no Centro de Conexão ou na guia Dispositivos do Visualizador de CD) para redirecionar o microfone de fala Phillips na sessão.

> **Observação:**

> As configurações acima nas etapas 2 e 3 poderiam ser aplicadas diretamente no valor do registro do lado do cliente **DeviceRules** sob a chave GenericUSB (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB), mas essa não é a maneira recomendada.

Mapeamento de Unidade Cliente

O Mapeamento de Unidade Cliente disponibiliza unidades de armazenamento no endpoint do cliente dentro de uma sessão Citrix HDX™ para permitir que arquivos e pastas sejam transferidos do cliente para o host da sessão e vice-versa. Este recurso é habilitado por padrão com privilégios de leitura e gravação. Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, habilite a configuração de política **Acesso somente leitura à unidade cliente**. Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja definida como **Permitido** e também seja adicionada à política.

Como precaução de segurança, as unidades de endpoint são mapeadas sem a permissão de execução por padrão. Para permitir que os usuários executem arquivos executáveis diretamente das unidades cliente mapeadas, edite o valor do registro **ExecuteFromMappedDrive** no host da sessão. Para obter detalhes, consulte Unidades cliente mapeadas na seção **Recursos HDX gerenciados através do registro**.

Requisitos

A seguir estão os requisitos para usar o CDM:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2016 ou posterior
  - Linux: Consulte os requisitos de sistema do Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 ou posterior
  - Linux: Consulte a documentação do VDA Linux

Dispositivo cliente

- Sistema operacional

- Windows 10 1809 ou posterior
- Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux

Políticas Relacionadas

Consulte a seção Referência de configurações de política para configurações de CDM.

Cenários de salto duplo

O CDM é compatível em cenários de salto duplo. Por padrão, a unidade do endpoint do cliente é mapeada para a sessão do segundo salto e as unidades do primeiro salto não estão disponíveis. No entanto, isso pode ser configurado para que as unidades do primeiro salto sejam mapeadas na sessão do segundo salto, em vez das unidades do endpoint do cliente.

Para configurar esta funcionalidade, edite o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- Nome do valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Dados do valor:
  - Verdadeiro - Mapeia as unidades da sessão do primeiro salto na sessão do segundo salto
  - Falso - Mapeia as unidades do endpoint do cliente na sessão do segundo salto

> **Observação:**

> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Dispositivos móveis e com tela sensível ao toque

O Citrix Virtual Apps and Desktops™ permite que os usuários acessem seus aplicativos e desktops publicados a partir de dispositivos cliente móveis e com tela sensível ao toque.

Requisitos

Plano de controle Citrix®

- Citrix Virtual Apps and Desktops 1912 ou posterior
- Citrix DaaS™

Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows 11 21H2 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops versão 7.15 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
- Aplicativo Citrix Workspace™ para Windows versão 1808 ou posterior

Modo tablet para dispositivos com tela sensível ao toque usando o Windows Continuum

Continuum é um recurso do Windows 10 que se adapta à forma como o dispositivo cliente é usado. Quando o VDA detecta a presença de um teclado ou mouse em um cliente habilitado para toque, ele coloca o cliente no modo desktop. Se um teclado ou mouse não estiver presente, o VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão da sessão e também durante a sessão quando o teclado ou mouse é conectado ou desconectado.

O recurso é habilitado por padrão. Para desabilitar este recurso, configure as configurações de política Configurações de política de alternância do modo tablet.

Além dos requisitos para dispositivos com tela sensível ao toque mencionados acima, os seguintes são necessários para o Windows Continuum:

XenServer (anteriormente Citrix Hypervisor™)

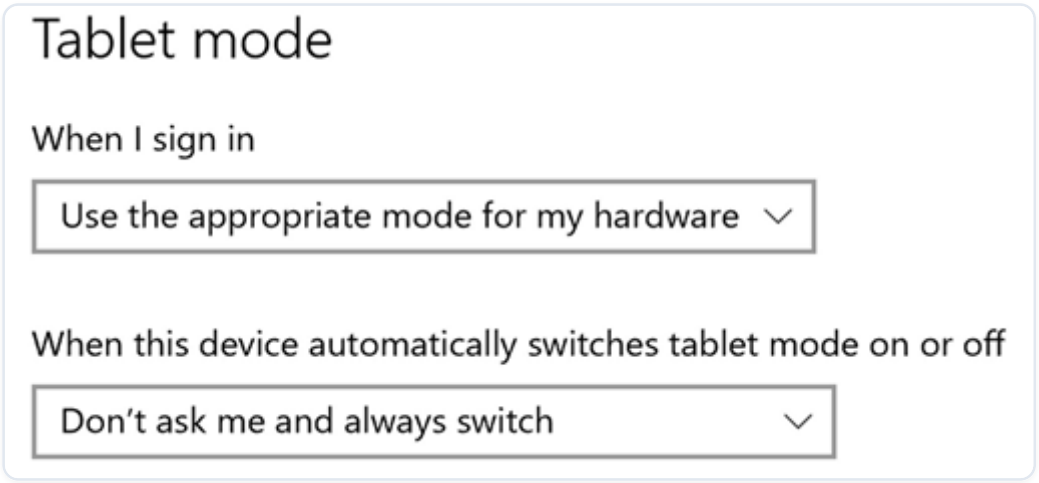
- Citrix Hypervisor 8.2 ou superior
- Execute o comando CLI do XenServer para permitir a alternância entre laptop/tablet: **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **Importante:**

> A atualização da imagem base para um catálogo de máquinas existente após a alteração da configuração de metadados não afeta nenhuma VM provisionada anteriormente. Após alterar a imagem base da VM do XenServer, crie um catálogo, escolha a imagem base e provisione uma nova máquina do Machine Creation Services™ (MCS).

Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows 11 21H2 ou posterior
- VDA
  - Windows: versão 7.16 ou posterior
  - **Devido às limitações atuais nas configurações do sistema operacional, o usuário terá que definir as seguintes opções nos menus suspensos depois de iniciar a primeira sessão ICA® e reiniciar o VDA:**
    - **Configurações > Sistema > Modo Tablet**
      - Usar o modo apropriado para meu hardware
      - Não me perguntar e sempre alternar



O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores.
- A tela Iniciar e todos os aplicativos que você inicia são abertos em tela cheia.
- A barra de tarefas contém um botão Voltar.
- Ícones excluídos da barra de tarefas.

Você tem acesso ao Explorador de Arquivos.



O Windows 10 carrega o driver GPIO na máquina virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro da máquina virtual.

O aplicativo Citrix Workspace para HTML5 não oferece suporte aos recursos do Windows Continuum.

O **modo desktop** oferece a interface de usuário tradicional, onde você interage da mesma forma que usando um PC com teclado e mouse.

Canetas Microsoft Surface Pro e Surface Book

Oferecemos suporte à funcionalidade padrão da caneta com aplicativos baseados em Windows Ink. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e do modelo da caneta. Por exemplo, a pressão da caneta pode ter até 4096 níveis. Este recurso é ativado por padrão.

A seguir estão os requisitos para o suporte à funcionalidade da caneta:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 1903 ou posterior
- Citrix DaaS

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1903 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
- Citrix Workspace app para Windows versão 1902 ou posterior

Para uma demonstração do Windows Ink e da funcionalidade da caneta, clique nesta imagem:



Para desabilitar ou habilitar esse recurso, consulte Canetas Microsoft Surface Pro e Surface Book na lista de recursos gerenciados pelo registro.

Problemas conhecidos

A seguir estão os problemas conhecidos com o suporte à caneta:

- Devido a limitações do SO no Windows Server 2k22, os usuários não conseguirão definir atalhos de caneta ou fazer ajustes nas configurações de caneta/tinta no Painel de Controle ao se conectar a aplicativos ou desktops do servidor 2k22.
- Os atalhos de caneta não estão sendo respeitados de um cliente Windows 11 habilitado para caneta devido a uma limitação do sistema operacional.

Portas seriais

A maioria dos PCs novos não possui portas seriais (COM) integradas. As portas são fáceis de adicionar usando conversores USB. Aplicativos adequados para portas seriais geralmente envolvem sensores, controladores, leitores de cheque antigos, pads e assim por diante. Alguns dispositivos USB de porta COM virtual usam drivers específicos do fornecedor em vez dos drivers fornecidos pelo Windows (usbser.sys). Esses drivers permitem que você force a porta COM virtual do dispositivo USB para que ela não mude mesmo se conectada a diferentes soquetes USB. Isso pode ser feito em **Gerenciador de Dispositivos > Portas (COM e LPT) > Propriedades** ou no aplicativo que controla o dispositivo.

O mapeamento de porta COM do cliente permite que dispositivos conectados às portas COM no endpoint do usuário sejam usados durante sessões virtuais. Você pode usar esses mapeamentos como qualquer outro mapeamento de rede.

Para cada porta COM, um driver no sistema operacional atribui um nome de link simbólico, como COM1 e COM2. Os aplicativos então usam o link para acessar a porta.

Importante:

O fato de um dispositivo poder ser conectado ao endpoint usando USB diretamente não significa que ele possa ser redirecionado usando o redirecionamento USB genérico. Alguns dispositivos USB funcionam como portas COM virtuais, que os aplicativos podem acessar da mesma forma que uma porta serial física. O sistema operacional pode abstrair portas COM e tratá-las como compartilhamentos de arquivos. Dois protocolos comuns para COM virtual são CDC ACM ou MCT. Quando conectados por meio de uma porta RS-485, os aplicativos podem não funcionar. Obtenha um conversor RS-485 para RS232 para usar RS-485 como uma porta COM. **Importante:**

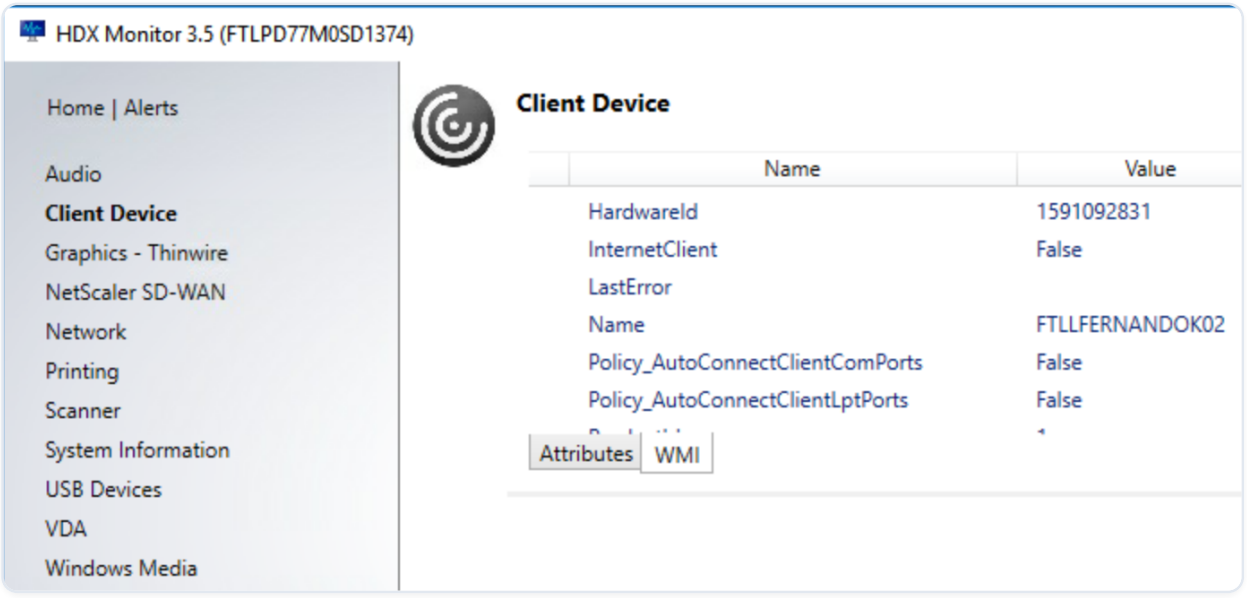
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um pad de assinatura) de forma consistente apenas se ele estiver conectado a COM1 ou COM2 na estação de trabalho cliente.

Mapear uma porta COM do cliente para uma porta COM do servidor

Você pode mapear portas COM do cliente para uma sessão Citrix® de três maneiras:

- Políticas do Studio. Para obter mais informações sobre políticas, consulte Configurações de política de redirecionamento de porta.
- Prompt de comando do VDA.
- Ferramenta de configuração da Área de Trabalho Remota (Serviços de Terminal).

1. Habilite as políticas **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente do Studio**. Após aplicadas, algumas informações estarão disponíveis no HDX™ Monitor.



2. Se a **Conexão automática de portas COM do cliente** falhou ao mapear a porta, você pode mapear a porta manualmente ou usar scripts de logon. Faça logon no VDA e, em uma janela de prompt de comando, digite:

   NET USE COMX: `\CLIENT\COMZ`:

   Ou

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

X é o número da porta COM no VDA (as portas de 1 a 9 estão disponíveis para mapeamento). **Z** é o número da porta COM do cliente que você deseja mapear.

Para confirmar que a operação foi bem-sucedida, digite **NET USE** em um prompt de comando do VDA. A lista que aparece contém unidades mapeadas, portas LPT e portas COM mapeadas.



3. Para usar esta porta COM em um desktop ou aplicativo virtual, instale o aplicativo do seu dispositivo de usuário e aponte-o para o nome da porta COM mapeada. Por exemplo, se você mapear COM1 no cliente para COM3 no servidor, instale o aplicativo do seu dispositivo de porta COM no VDA e aponte-o para COM3 durante a sessão. Use esta porta COM mapeada como usaria uma porta COM no dispositivo do usuário.

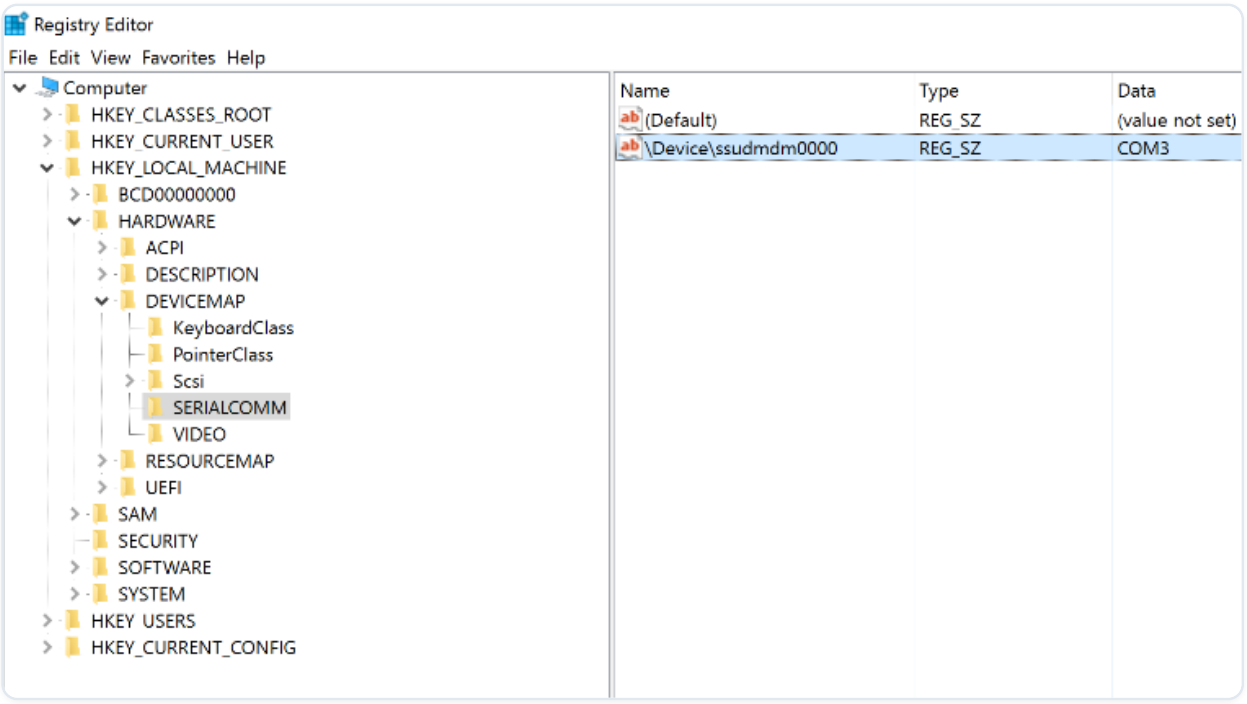
Importante:

O mapeamento de porta COM não é compatível com TAPI. Você não pode mapear dispositivos da Interface de Programação de Aplicativos de Telefonia do Windows (TAPI) para portas COM do cliente. TAPI define uma maneira padrão para os aplicativos controlarem as funções de telefone para chamadas de dados, fax e voz. TAPI gerencia a sinalização, incluindo discagem, atendimento e encerramento de chamadas. Além disso, serviços suplementares como retenção, transferência e chamadas em conferência.

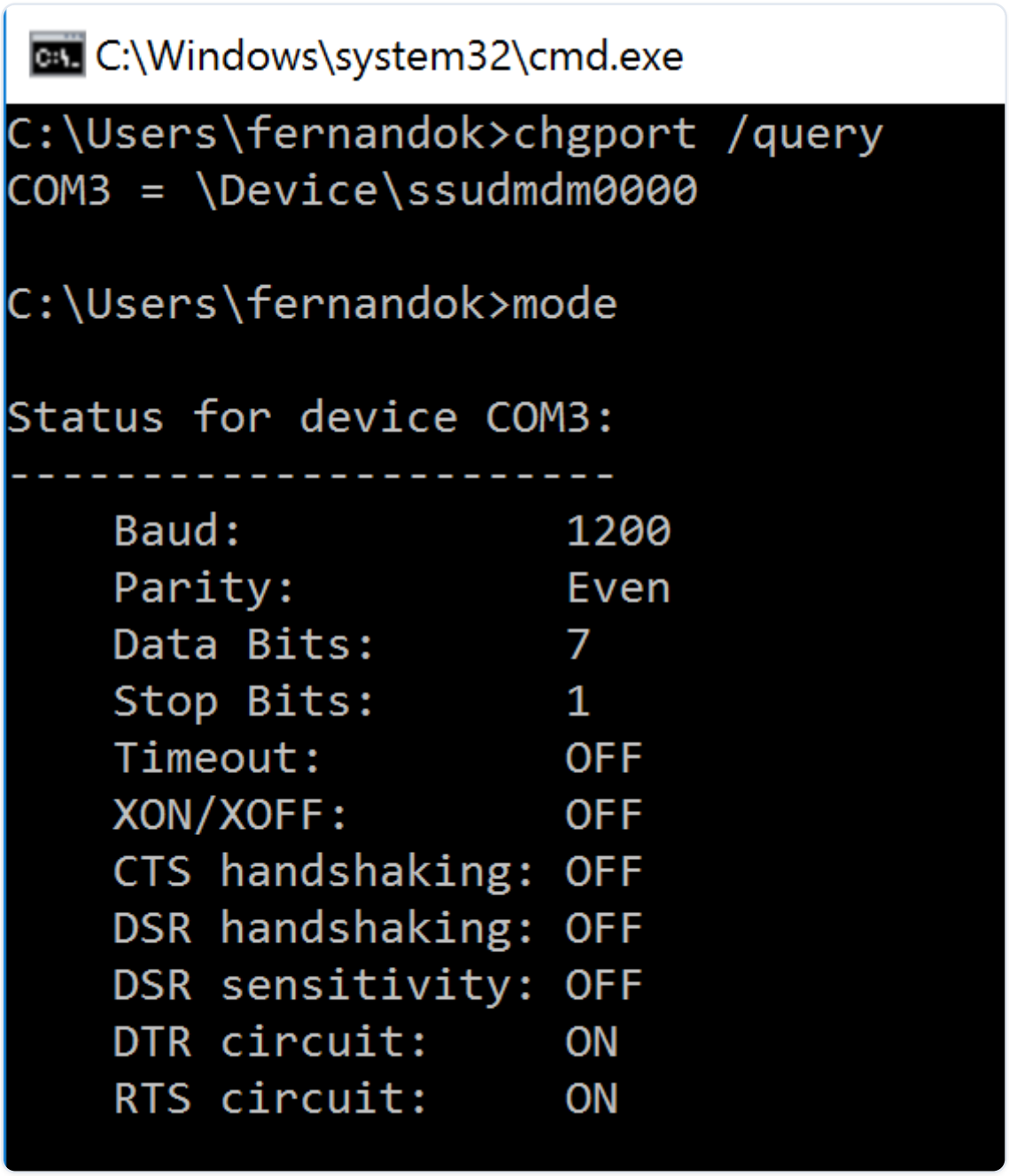
Solução de problemas

1. Certifique-se de que você pode acessar o dispositivo diretamente do endpoint, ignorando o Citrix. Enquanto a porta não estiver mapeada para o VDA, você não estará conectado a uma sessão Citrix. Siga todas as instruções de solução de problemas que vieram com o dispositivo e verifique se ele funciona localmente primeiro. Quando um dispositivo é conectado a uma

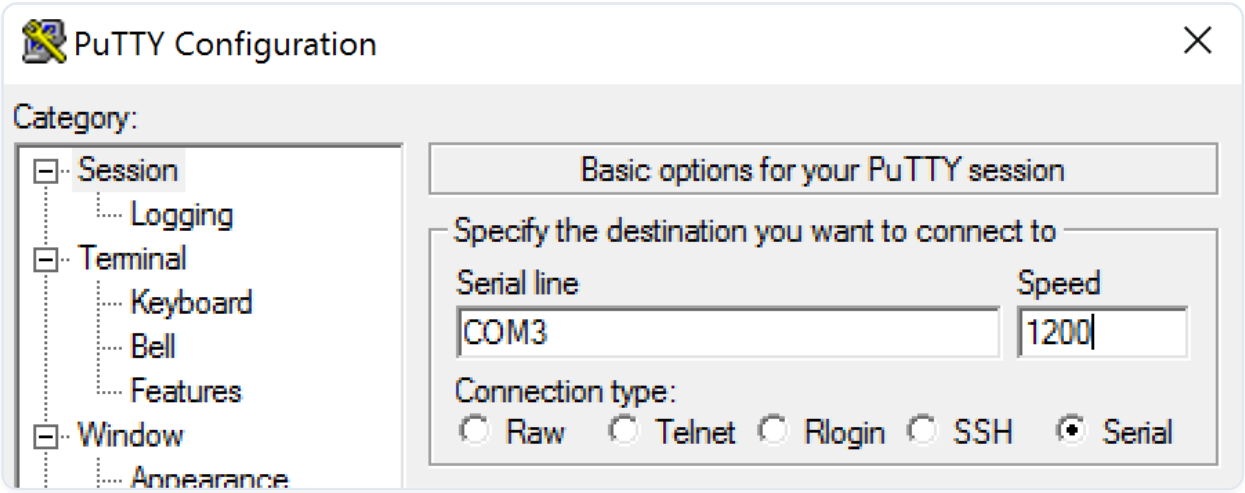
porta COM serial, uma chave de registro é criada no hive mostrado aqui:



Você também pode encontrar essas informações no prompt de comando executando **chgport /query**.



Se as instruções de solução de problemas para o dispositivo não estiverem disponíveis, tente abrir uma sessão PuTTY. Escolha **Session** e em **Serial line** especifique sua porta COM.



Você pode executar **MODE** em uma janela de comando local. A saída pode exibir a porta COM em uso e os valores de Baud/Paridade/Bits de Dados/Bits de Parada, que você precisa em sua sessão PuTTY. Se a conexão PuTTY for bem-sucedida, pressione **Enter** para ver o feedback do dispositivo. Quaisquer caracteres que você digitar podem ser repetidos na tela ou respondidos. Se esta etapa não for bem-sucedida, você não poderá acessar o dispositivo a partir de uma sessão virtual.

2. Mapeie a porta COM local para o VDA (usando políticas ou **NET USE COMX: `\CLIENT\COMZ` :**) e repita os mesmos procedimentos do PuTTY da etapa anterior, mas desta vez a partir do PuTTY do VDA. Se o PuTTY não conseguir exibir o erro **Unable to open connection to COM1. Unable to open serial port**, outro dispositivo pode estar usando a COM1.
3. Execute **chgport /query**. Se o driver serial integrado do Windows no VDA estiver atribuindo automaticamente \Device\Serial0 a uma porta COM1 do seu VDA, faça o seguinte: A. Abra o CMD no VDA e digite **NET USE.**

   B. Exclua qualquer mapeamento existente (por exemplo, COM1) no VDA.

   NET USE COM1 /DELETE

   C. Mapeie o dispositivo para o VDA.

   NET USE COM1: `\CLIENT\COM3` :

   D. Aponte seu aplicativo no VDA para COM3.

   Por fim, tente mapear sua porta COM local (por exemplo, COM3) para uma porta COM diferente no VDA (que não seja a COM1, por exemplo, COM3). Certifique-se de que seu aplicativo esteja apontando para ela: **NET USE COM3: `\CLIENT\COM3`**
4. Se agora você vir a porta mapeada, o PuTTY estiver funcionando, mas nenhum dado estiver sendo transmitido, pode ser uma condição de corrida. O aplicativo pode se conectar e abrir a porta antes que ela seja mapeada, impedindo que seja mapeada. Tente uma das seguintes opções:

   - Abra um segundo aplicativo publicado no mesmo servidor. Aguarde alguns segundos para que a porta seja mapeada e, em seguida, abra o aplicativo real que tenta usar a porta.
   - Habilite as políticas de redirecionamento de porta COM no Editor de Política de Grupo no Active Directory em vez do Studio. Essas políticas são **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente**. As políticas aplicadas dessa forma podem ser processadas antes das políticas do Studio, garantindo que a porta

COM seja mapeada. As políticas Citrix são enviadas para o VDA e armazenadas em: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- Use este script de logon para o usuário ou, em vez de publicar o aplicativo, publique um script .bat que primeiro exclui qualquer mapeamento no VDA, mapeia novamente a porta COM virtual e, em seguida, inicia o aplicativo:

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1`: NET USE COM2: `\CLIENT\COM2`: MODE COM1: BAUD=1200 (ou qualquer valor necessário) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (ou qualquer valor necessário) START `C:\Program Files\<Your Software Path>\<your_software.exe>`

5. O Process Monitor da Sysinternals é a ferramenta de último recurso. Ao executar a ferramenta no VDA, localize e filtre objetos como COM3, picaser.sys, CdmRedirector, mas especialmente \<your_app\>.exe. Quaisquer erros podem aparecer como Acesso Negado ou similar.

Teclados especiais

Teclados Bloomberg

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

O Citrix Virtual Apps and Desktops™ suporta o teclado Bloomberg modelo 5, modelo 4 Starboard (e o modelo 3 anterior). Este teclado permite que clientes do setor financeiro usem os recursos especiais do teclado para acessar dados do mercado financeiro e realizar negociações rapidamente.

> **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 é um dispositivo composto USB composto por vários dispositivos USB em um único invólucro físico:

- Teclado.
- Leitor de impressão digital.
- Dispositivo de áudio com teclas para aumentar e diminuir o volume e silenciar o alto-falante e o microfone. Este dispositivo inclui alto-falante e microfone integrados, e entrada para 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 suportar dispositivos USB.
- Mínimo de Citrix Workspace app 2207 para Linux para suportar o teclado Bloomberg modelo 5.
- Mínimo de Citrix Workspace app 2109 para Windows para suportar o teclado Bloomberg modelo 5.
- Mínimo de Citrix Workspace app 1808 para Windows ou Citrix Receiver para Windows 4.8 para suportar os teclados Bloomberg modelos 3 e 4.
- Mínimo de Citrix Workspace app 1808 para Windows ou Citrix Receiver para Windows 4.12 para usar o modo KVM (dois cabos USB, um roteado através do KVM) para o Modelo 4.

Para obter informações sobre como configurar teclados Bloomberg no aplicativo Citrix Workspace para Windows, consulte Configurando teclados Bloomberg.

Para habilitar o suporte ao teclado Bloomberg, consulte Teclados Bloomberg na lista de recursos gerenciados através do registro.

Verificar 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 ao teclado Bloomberg estiver habilitado, o Desktop Viewer mostrará três dispositivos sob o ícone USB:

Para teclado Bloomberg 5:

- Bloomberg LP Bloomberg Biometric Module
- Bloomberg LP Keyboard (Dispositivo composto com duas interfaces)
- Bloomberg LP Keyboard Audio (Dispositivo composto com três interfaces)

Para teclados Bloomberg 3 e 4:

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Cenário somente de aplicativo contínuo:

Abra o menu **Connection Center** no ícone da área de notificação do aplicativo Citrix Workspace. Se o suporte ao teclado Bloomberg estiver habilitado, os três dispositivos aparecerão no menu **Devices**.

A marca de seleção ao lado de cada um desses dispositivos indica que eles estão conectados remotamente à sessão.

Windows - Ferramenta de Suporte para Teclado e IME

Esta é uma ferramenta de linha de comando de autoatendimento que pode diagnosticar problemas relevantes relacionados ao teclado e ao Editor de Método de Entrada.

Para atender a uma variedade de requisitos do usuário, fornecer versatilidade de plataforma e oferecer aos usuários necessidades personalizadas, as funções do teclado e do Editor de Método de Entrada (IME) dependem de diferentes configurações e capacidades em VDAs e aplicativos Citrix Workspace™.

Uma configuração incorreta no VDA ou no lado do cliente pode resultar em comportamentos de entrada inesperados.

No entanto, a Citrix® fornece as configurações recomendadas para alguns cenários de uso comuns, e essas recomendações também estão incluídas nos resultados do diagnóstico.

Com esta ferramenta, as categorias de problemas abaixo podem ser identificadas:

- **Inconsistência do tipo de teclado:** verificará o tipo de teclado do VDA e o tipo de teclado do cliente para confirmar se há inconsistência. Por exemplo, o VDA está usando teclados ingleses

de 101 teclas, mas o cliente está usando um teclado japonês de 106 teclas. Este diagnóstico é direcionado para casos de uso de teclado JP 106/109 e KO 103/106.

- **Inconsistência do modo de sincronização do layout do teclado:** verificará as configurações de sincronização do layout do teclado, as configurações de registro, as políticas de grupo e resolverá problemas nas configurações do modo de sincronização em um determinado ambiente.
- **Inconsistência do layout do teclado do cliente e do layout do teclado do VDA:** verificará se o layout do teclado do cliente é o mesmo que o layout do teclado do VDA
- **A Barra de Idiomas Remota está sendo exibida para sessões de aplicativo:** verificará se a barra de idiomas remota está sendo exibida quando os usuários finais iniciam uma sessão de aplicativo e estão usando mais de 1 layout de teclado.

Esta ferramenta de linha de comando está hospedada no Windows VDA - `CtxKbImeDiagnostics.exe`. As interfaces de linha de comando são as seguintes:

INTERFACE	DESCRIÇÃO	OBSERVAÇÃO
`CtxKbimeDiagnostics`	mostrar resultado do diagnóstico apenas para a sessão ICA® atual	Se o usuário tiver privilégio de administrador, ele mostra o diagnóstico para todas as sessões ICA ativas. Se o usuário não tiver privilégio de administrador, ele mostra o diagnóstico para as sessões ICA do usuário atual.
`CtxKbimeDiagnostics [-v]`	mostrar informações de configuração e resultado de diagnóstico para a sessão atual	Se o usuário tiver privilégio de administrador, ele mostrará o diagnóstico para todas as sessões ICA ativas
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	mostrar informações de configuração e resultado de diagnóstico para esta sessão	
`CtxKbimeDiagnostics [-s Session_Id]`	especificar uma sessão e mostrar o resultado de diagnóstico respectivo para esta sessão	O privilégio de administrador pode consultar outras sessões ICA/O usuário normal só pode consultar suas próprias sessões ICA

INTERFACE	DESCRIÇÃO	OBSERVAÇÃO
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	especificar uma sessão e mostrar todas as informações de configuração e resultado de diagnóstico para esta sessão	O privilégio de administrador pode consultar outras sessões ICA. O usuário normal só pode consultar suas próprias sessões ICA
`CtxKbimeDiagnostics [-h]`	mostrar argumentos/ parâmetros suportados e exemplo	interface de “ajuda”
`CtxKbimeDiagnostics [-V]`	mostrar a versão atual da ferramenta	

Observação:

Nesta versão, apenas o CWA Windows como cliente é suportado.

Webcams

Streaming de webcam de alta definição

Webcams podem ser usadas por aplicativos de videoconferência em execução na sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo de videoconferência. Quando a webcam e o aplicativo suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos resoluções de webcam de até 1920x1080.

Este recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para obter uma lista das plataformas do aplicativo Citrix Workspace que suportam o redirecionamento de webcam HDX, consulte Matriz de recursos do aplicativo Citrix Workspace.

Para obter mais informações sobre streaming de webcam de alta definição, consulte Videoconferência HDX e compressão de vídeo de webcam.

Você pode usar uma chave de registro para desabilitar e habilitar o recurso e, em seguida, configurar uma resolução específica. Para obter informações, consulte Streaming de webcam de

alta definição e Resolução de webcam de alta definição na lista de recursos gerenciados através do registro.

Gráficos

Os gráficos Citrix HDX incluem um extenso conjunto de tecnologias de aceleração e codificação de gráficos que otimizam a entrega de aplicativos gráficos avançados do Citrix Virtual Apps and Desktops. As tecnologias gráficas proporcionam a mesma experiência de usar um desktop físico ao trabalhar remotamente com aplicativos virtuais que são intensivos em gráficos.

Você pode usar software ou hardware para renderização gráfica. A renderização por software requer uma biblioteca de terceiros chamada rasterizador de software. Por exemplo, o Windows inclui o rasterizador WARP para gráficos baseados em DirectX. Às vezes, você pode querer usar um renderizador de software alternativo. A renderização por hardware (aceleração de hardware) requer um processador gráfico (GPU).

O HDX™ Graphics oferece uma configuração de codificação padrão otimizada para os casos de uso mais comuns. Usando as políticas Citrix, os administradores de TI também podem configurar várias configurações relacionadas a gráficos para atender a diferentes requisitos e fornecer a experiência de usuário desejada.

Thinwire

Thinwire é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição. Os gráficos são gerados como resultado da entrada do usuário, por exemplo, pressionamentos de tecla ou ações do mouse.

HDX 3D Pro

Os recursos do HDX 3D Pro no Citrix Virtual Apps and Desktops permitem que você entregue desktops e aplicativos que têm o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta aceleração de GPU apenas para DirectX.

Aceleração de GPU para SO de sessão única do Windows

Ao usar o HDX 3D Pro, você pode entregar aplicativos graficamente intensivos como parte de desktops ou aplicativos hospedados em máquinas com SO de sessão única. O HDX 3D Pro suporta computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de Passthrough de GPU e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere e Hyper-V (somente passthrough).

Usando o Passthrough de GPU, você pode criar VMs que têm acesso exclusivo a hardware de processamento gráfico dedicado. Você pode instalar várias GPUs no hipervisor e atribuir VMs a cada uma dessas GPUs em uma base um-para-um.

Usando a virtualização de GPU, várias máquinas virtuais podem acessar diretamente o poder de processamento gráfico de uma única GPU física.

Aceleração de GPU para SO de múltiplas sessões do Windows

O HDX 3D Pro permite que aplicativos com muitos gráficos executados em sessões do SO de múltiplas sessões do Windows sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor. Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais suportado. Em vez disso, use Thinwire com transporte adaptável ativado.

> Framehawk é uma tecnologia de acesso remoto de exibição para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE). O Framehawk supera os desafios de interferência espectral e propagação multicaminho e oferece uma experiência de usuário fluida e interativa aos usuários de aplicativos e desktops virtuais.

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e permitir o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você

pode especificar uma marca d'água que é uma camada de texto. A marca d'água pode ser exibida em toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte VDA.

Taxa de Atualização Adaptável

Com as novas melhorias de escalabilidade, o HDX corresponde à taxa de atualização dos monitores virtuais para corresponder à política de FPS de destino definida. A Taxa de Atualização Adaptável (ARR) está disponível para VDAs de sessão única e multissessão, e funciona para cenários acelerados por GPU e não-GPU.

modo tolerante a perdas

O modo tolerante a perdas foi completamente reformulado para garantir que a sessão permaneça interativa quando a perda de pacotes for detectada.

Informações relacionadas

- HDX 3D Pro
- Aceleração de GPU para SO Windows de sessão única
- Aceleração de GPU para SO Windows de multissessão
- Framehawk
- Thinwire
- Marca d'água de sessão baseada em texto

Alto Alcance Dinâmico de 10 bits (HDR)

Com sessões de área de trabalho virtual de Alto Alcance Dinâmico (HDR) de 10 bits, você pode usar recursos aprimorados de codificação e decodificação para renderizar imagens e vídeos de alta qualidade com uma ampla gama de cores e maior contraste e brilho. Além disso, você pode personalizar o nível de luminância branca, os Dados de Identificação de Tela Estendidos (EDID) e a qualidade visual para melhorar a experiência do usuário.

Requisitos do sistema

Endpoint:

- Aplicativo Citrix Workspace™ para Windows 2209 ou posterior para GPUs NVIDIA
- GPUs NVIDIA com suporte para decodificação HEVC (H.265) 444 de 10 bits no endpoint

- Monitores com suporte a HDR de 10 bits, o HDR de 10 bits deve ser ativado em todos os monitores usando as configurações de exibição.

Servidor:

- VDA de SO de sessão única do Windows 2209 ou posterior para GPUs NVIDIA, e VDA 2308 ou posterior para GPUs Intel
- GPUs NVIDIA com suporte para codificação HEVC 444 de 10 bits no VDA

Políticas necessárias

Endpoint:

- Habilitar decodificação H.265 para gráficos

Servidor:

- Otimizar para carga de trabalho de gráficos 3D
- Indicador de Status Gráfico (opcional)

Configurações do servidor

Iniciar uma sessão Citrix® em um monitor de endpoint com HDR de 10 bits ativado habilita a sessão HDR por padrão. Em sessões HDR com vários monitores, todos os monitores de endpoint devem ter HDR de 10 bits ativado. As sessões HDR são suportadas nos modos janela e tela cheia.

Nível de Branco de Referência

Essa configuração define o nível de luminância branca pelo valor em nits. Ela controla o brilho relativo da tela HDR dentro da sessão. O valor padrão é 80 nits. Defina a seguinte chave de registro para definir um valor de nit diferente:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_DWORD
- Name: RefWhiteLevel

Para ativar a configuração, você deve redimensionar sua sessão ou desconectar e reiniciar a sessão.

Substituição de EDID

Você pode configurar o VDA para usar o EDID do monitor de endpoint para suas sessões HDR. Isso permite que você utilize totalmente os recursos de exibição do monitor, combinando a gama de cores e o intervalo de luminância. Por padrão, as sessões HDR assumem um monitor compatível com HDR1000. Você pode exportar o EDID do monitor de endpoint usando NVIDIA ou outras ferramentas. Aplique-o ao VDA usando a seguinte chave de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type: REG_BINARY
- Name: EDIDOverride

Ao armazenar o EDID no registro, ele não deve conter vírgulas, espaços ou caracteres especiais. Para ativar a substituição de EDID, saia e inicie uma nova sessão.

Experiência visual sem perdas

Habilite as seguintes políticas para uma experiência visualmente sem perdas:

- Permitir Compressão Visual Sem Perdas
- Qualidade Visual: Sempre Sem Perdas ou Construir para Sem Perdas

Depois que as políticas forem definidas, você poderá controlar a qualidade da sessão HDR usando o Indicador de Status Gráfico, usando o Controle Deslizante de Qualidade da Imagem ou alternando para o modo pixel-perfect.

Permitir bloqueio de tela do Windows

Você pode usar esta política para permitir que todos os tempos limite de exibição do Windows, incluindo o bloqueio de tela, se apliquem a uma sessão do Citrix Virtual Desktop no SO Workstation. Essa configuração pode ser definida usando um Objeto de Política de Grupo do Citrix no Citrix Studio.

Por padrão, quando esta configuração não está habilitada, um Citrix Virtual Desktop não responde a tempos limite para bloqueio de sessão, protetor de tela ou desligamento da tela, durante uma sessão ativa.

Quando um protetor de tela protegido por senha é configurado em um VDA de Workstation, esta configuração deve ser habilitada para permitir que a sessão do Citrix Virtual Desktop seja bloqueada automaticamente quando o tempo limite do protetor de tela for atingido.

Habilitar esta configuração quando um tempo limite de desligamento da tela é configurado no VDA faz com que a expiração desse tempo limite resulte em uma sessão que não é atualizada até que o usuário retome a interação com a sessão. Por exemplo, qualquer tempo exibido não é atualizado e novas notificações não são exibidas.

Outras considerações

- Você pode iniciar sessões HDR de 10 bits em até quatro monitores em GPUs virtuais.
- A sessão Citrix reverte para um modo de 8 bits, não-HDR, nas seguintes instâncias:
  - Se quaisquer monitores de endpoint não tiverem HDR de 10 bits habilitado
  - Habilitar o compartilhamento de tela.
  - Definir um layout de exibição virtual no VDA.
  - Alternar para o modo pixel-perfect sem definir a política **Permitir Compressão Visual Sem Perdas**.

HDX™ 3D Pro

Os recursos HDX 3D Pro do Citrix Virtual Apps and Desktops™ permitem que você forneça desktops e aplicativos que apresentam o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta aceleração de GPU apenas para DirectX.

Para as configurações de política do HDX 3D Pro, consulte Otimizar para carga de trabalho de gráficos 3D.

Todos os aplicativos Citrix Workspace compatíveis podem ser usados com gráficos 3D. Para obter o melhor desempenho com cargas de trabalho 3D complexas, monitores de alta resolução, configurações de vários monitores e aplicativos de alta taxa de quadros, recomendamos as versões mais recentes do Citrix Workspace app para Windows e do Citrix Workspace app para Linux. Para obter mais informações sobre as versões compatíveis do Citrix Workspace app, consulte Marcos do ciclo de vida do Citrix Workspace app.

Exemplos de aplicativos profissionais 3D incluem:

- Aplicativos de design, fabricação e engenharia assistidos por computador (CAD/CAM/CAE)
- Software de Sistema de Informação Geográfica (GIS)
- Sistema de Comunicação e Arquivamento de Imagens (PACS) para imagens médicas

- Aplicativos que usam as versões mais recentes de OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL
- Aplicativos não gráficos computacionalmente intensivos que usam GPUs NVIDIA Compute Unified Device Architecture (CUDA) para computação paralela

O HDX 3D Pro oferece a melhor experiência do usuário em qualquer largura de banda:

- Em conexões WAN: Ofereça uma experiência de usuário interativa em conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de um desktop local em conexões LAN.

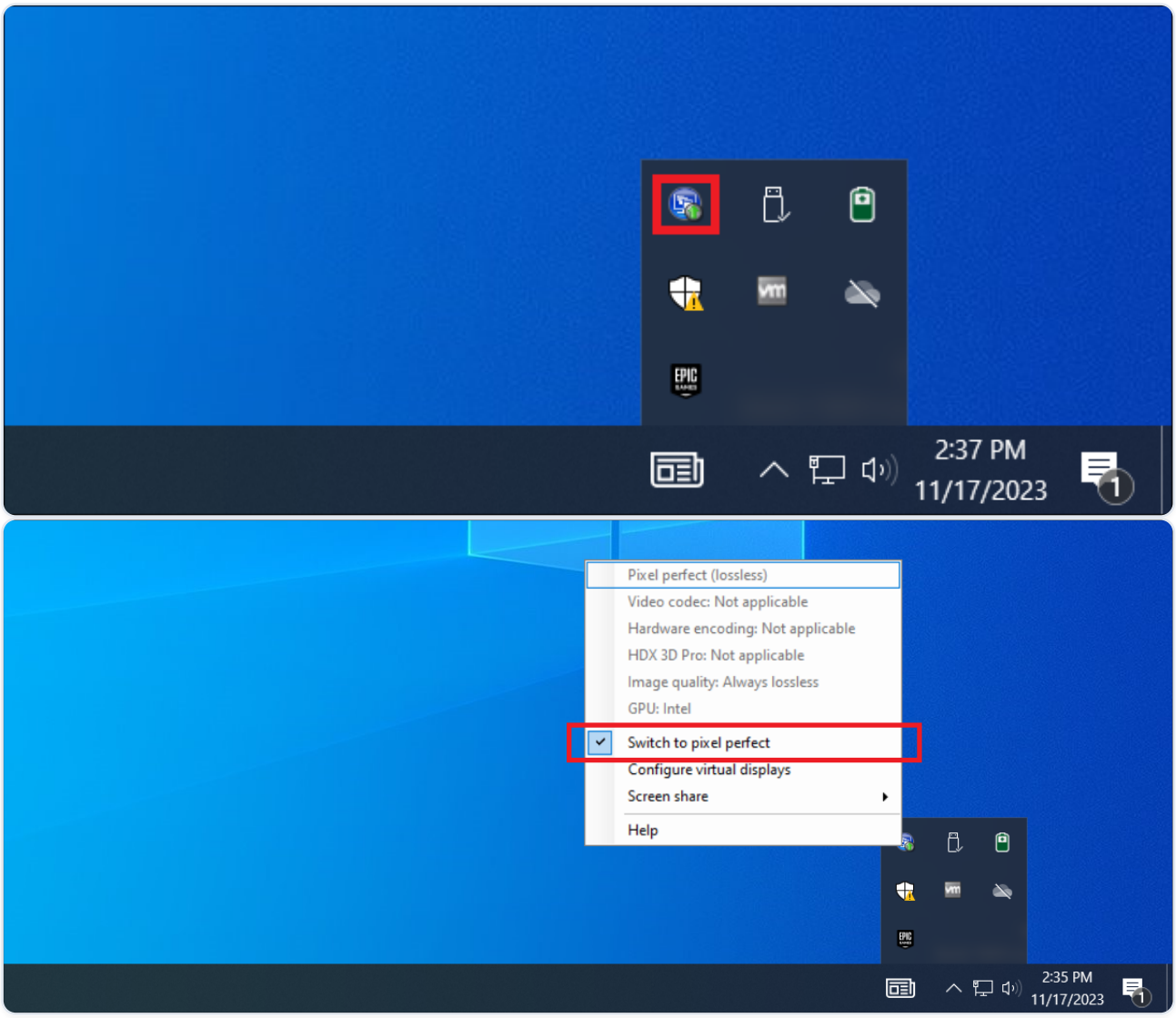
  Você pode substituir estações de trabalho complexas e caras por dispositivos de usuário mais simples, movendo o processamento gráfico para o data center para gerenciamento centralizado.

Opção de compactação sem perdas para casos de uso especializados

O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixel são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

Ao usar a compressão sem perdas:

- O indicador sem perdas no Indicador de Status Gráfico, um ícone na área de notificação, informa ao usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração de política **Qualidade Visual** especifica **Construir para sem perdas**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.



- O switch sem perdas permite ao usuário mudar para o modo **Sempre Sem Perdas** a qualquer momento dentro da sessão. Para selecionar ou desmarcar **Sem Perdas** dentro de uma sessão, clique com o botão direito do mouse no ícone e clique em **Mudar para pixel perfeito** ou use o atalho ALT+SHIFT+1.
    - Para compressão sem perdas: O HDX 3D Pro usa o codec sem perdas para compressão, independentemente do codec selecionado por meio da política.
    - Para compressão com perdas: O HDX 3D Pro usa o codec original, seja o padrão ou o selecionado através da política. As configurações do switch sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Sempre sem perdas** na configuração da política de **qualidade visual**.

Você pode substituir o atalho padrão, ALT+SHIFT+1, para selecionar ou desmarcar Sem Perdas dentro de uma sessão. Configure uma nova configuração de registro em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

- Nome: HKEY_LOCAL_MACHINE_HotKey, Tipo: String
- O formato para configurar uma combinação de atalho é C=0|1, A=0|1, S=0|1, W=0|1, K=val. As chaves devem ser separadas por vírgula “,”. A ordem das chaves não importa.
- A, C, S, W e K são chaves, onde C=Control, A=ALT, S=SHIFT, W=Win, e K=uma chave válida. Os valores permitidos para K são 0–9, a–z e qualquer código de chave virtual.
- Por exemplo: Para F10, defina K=0x79 Para Ctrl + F10, defina C=1, K=0x79 Para Alt + A, defina A=1, K=a ou A=1, K=A ou K=A, A=1 Para Ctrl + Alt + 5, defina C=1, A=1, K=5 ou A=1, K=5, C=1 Para Ctrl + Shift + F5, defina A=1, S=1, K=0x74

Otimizar a experiência do usuário do HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política de limite de largura de banda geral da sessão para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que ela não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações nela ao longo das sessões do usuário podem impactar negativamente o desempenho. Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a largura de banda necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre. Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo CTX128190 da Central de Conhecimento. 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. A ferramenta está disponível na pasta **Support** na mídia de instalação do Citrix Virtual Apps and Desktops.

Aceleração de GPU para SO multi-sessão do Windows

O Citrix Virtual Apps and Desktops™ oferece suporte a aplicativos com muitos gráficos executados em sessões do SO multi-sessão do Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a CPU do servidor pode ser usada com mais eficiência.

Como o Windows Server é um sistema operacional multiusuário, vários usuários podem compartilhar uma GPU acessada pelo Citrix Virtual Apps™ sem a necessidade de virtualização de GPU (vGPU).

Para procedimentos que envolvem a edição do registro, use cautela: Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Compartilhamento de GPU

O Compartilhamento de GPU permite a renderização de hardware de GPU de aplicativos OpenGL e DirectX em sessões de área de trabalho remota. Ele tem as seguintes características:

- Pode ser usado em máquinas bare metal ou virtuais para aumentar a escalabilidade e o desempenho do aplicativo.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não exige o desempenho de renderização de uma GPU dedicada).
- Não requer configurações especiais.

Uma GPU pode ser atribuída à máquina virtual do Windows Server nos modos de pass-through completo ou GPU virtual (vGPU), seguindo os requisitos do Hypervisor e do fornecedor da GPU. Implantações bare-metal em máquinas físicas do Windows Server também são suportadas.

O Compartilhamento de GPU não depende de nenhuma placa gráfica específica.

- Para máquinas virtuais, selecione uma placa gráfica compatível com o Hypervisor em uso. Para uma lista de compatibilidade de hardware do XenServer, consulte Lista de Compatibilidade de Hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de vídeo habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desabilite todas, exceto uma, usando o Gerenciador de Dispositivos.

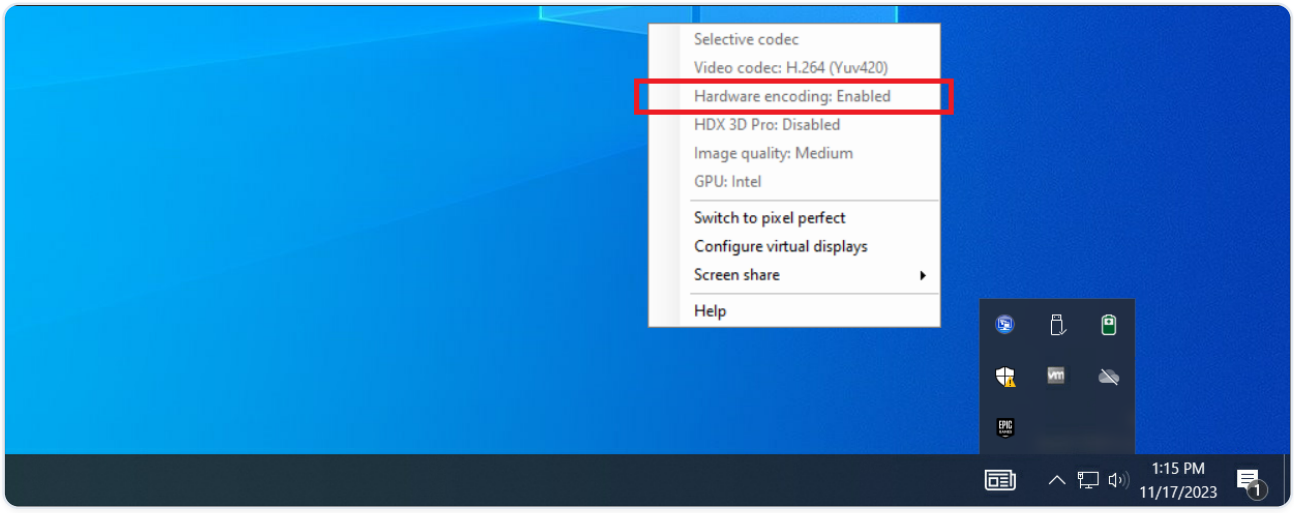
A escalabilidade usando o Compartilhamento de GPU depende de vários fatores:

- Os aplicativos em execução
- A quantidade de RAM de vídeo que consomem
- O poder de processamento da placa gráfica

Alguns aplicativos manipular a escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha do driver da placa gráfica. Limite o número de usuários simultâneos para evitar tais problemas.

- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso e permite o uso de codificação de hardware para codificação H.264 (onde disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para mais informações, consulte Configurações de política gráfica.

Para confirmar que a aceleração da GPU está ocorrendo, o Indicador de Status Gráfico pode ser usado:



Renderização DirectX, Direct3D e WPF

A renderização DirectX, Direct3D e WPF está disponível apenas em servidores com uma GPU que suporte uma interface de driver de vídeo (DDI) versão 9ex, 10 ou 11.

- No Windows Server 2016 e posterior, as sessões dos Serviços de Área de Trabalho Remota (RDS) no servidor Host da Sessão RD usam o Microsoft Basic Render Driver como adaptador padrão. Para usar a GPU em sessões RDS no Windows Server 2016 e posterior, habilite a configuração **Usar o adaptador gráfico padrão de hardware para todas as sessões dos Serviços de Área de Trabalho Remota** na política de grupo **Política de Computador Local** \> **Configuração do Computador** \> **Modelos Administrativos** \> **Componentes do Windows** \> **Serviços de Área de Trabalho Remota** \> **Host da Sessão da Área de Trabalho Remota** \> **Ambiente de Sessão Remota**.
- Para permitir que aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no registro do servidor que executa sessões do SO Windows Multi-session.

Para obter informações sobre a configuração do registro, consulte Renderização do Windows Presentation Foundation (WPF) na lista de recursos gerenciados através do registro.

Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos de aceleração CUDA, habilite as configurações do registro. Para obter informações, consulte Aceleração de GPU para aplicativos CUDA ou OpenCL na lista de recursos gerenciados através do registro.

Aceleração de GPU para SO de sessão única do Windows

Com o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de desktops hospedados ou aplicativos em máquinas de SO de sessão única. O HDX 3D Pro oferece suporte a computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de Passthrough de GPU e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere, Nutanix e Hyper-V (somente passthrough).

O HDX™ 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para desempenho ideal de WAN e sem fio. O HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que suportam NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que suportam NVENC.
- Opção de compressão sem perdas para casos de uso especializados. O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixels são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

Cuidado:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

- Suporte a múltiplos monitores e monitores de alta resolução. Para máquinas de SO de sessão única, são suportados até 8 monitores 4K. Os usuários podem organizar seus monitores em qualquer configuração e podem misturar monitores com diferentes resoluções e orientações. O número de monitores é limitado pelas capacidades da GPU do computador host, do dispositivo do usuário e da largura de banda disponível. O HDX 3D Pro suporta todas as resoluções de monitor e é limitado apenas pelas capacidades da GPU no computador host.
- Resolução dinâmica. Você pode redimensionar a área de trabalho virtual ou a janela do aplicativo para qualquer resolução. **Nota:** O único método suportado para alterar a resolução é redimensionando a janela da sessão VDA. Alterar a resolução de dentro da sessão VDA (usando **Painel de Controle > Aparência** e **Personalização > Vídeo > Resolução da Tela) não é suportado**.
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro oferece suporte a placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passthrough de GPU e compartilhamento de GPU. O NVIDIA vGPU permite que várias VMs tenham acesso simultâneo e direto a uma única GPU física, usando os mesmos drivers gráficos NVIDIA que são implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar o HDX 3D Pro com vDGA para cargas de trabalho RDS e VDI.
- Suporte para VMware vSphere/ESX.
- Suporte para Microsoft HyperV usando Atribuição de Dispositivo Discreto no Windows Server 2016.
- Suporte para Data Center Graphics com Intel Xeon Processor E3 Family e Intel Data Center GPU Flex Series. Para obter mais informações, consulte `<https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`.
- Suporte para GPUs AMD.

> Nota:
>
> O suporte para AMD MxGPU (virtualização de GPU) funciona apenas com vGPUs do VMware vSphere. O Citrix Hypervisor e o Hyper-V são suportados com passthrough de GPU. Para obter mais informações, consulte `<https://www.amd.com/en/graphics/workstation-virtual-graphics>`.

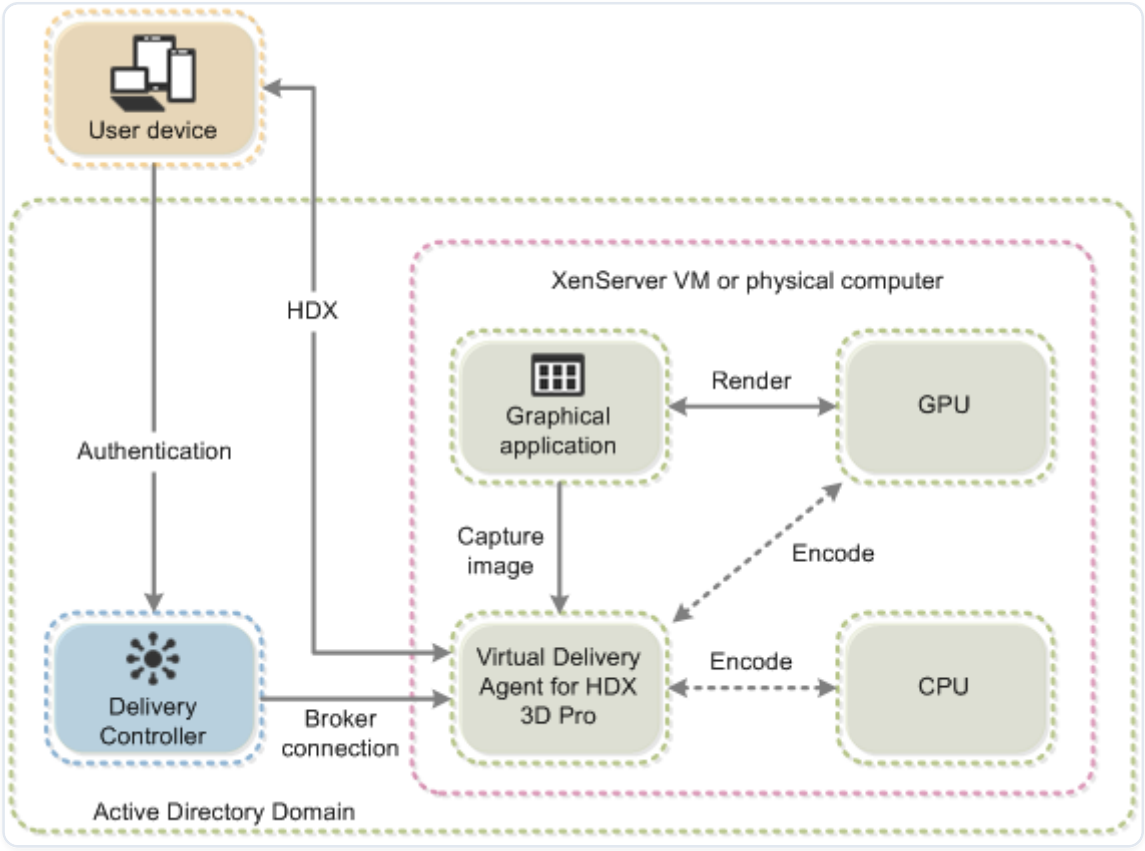
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e GPUs Intel. Uma configuração de política (habilitada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para H.264, H.265 ou codificação AV1 (quando disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política de gráficos.

Conforme mostrado na figura a seguir:

- Quando um usuário faz login no aplicativo Citrix Workspace™ e acessa o aplicativo ou área de trabalho virtual, o Controller autentica o usuário. O Controller então entra em contato com o VDA para HDX 3D Pro para intermediar uma conexão com o computador que hospeda o aplicativo gráfico.

O VDA para HDX 3D Pro usa o hardware apropriado no host para compactar as visualizações do desktop completo ou apenas do aplicativo gráfico.

- As visualizações do desktop ou aplicativo e as interações do usuário com eles são transmitidas entre o computador host e o dispositivo do usuário. Essa transmissão é feita por meio de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



Otimizar a experiência do usuário do HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política **Limite geral de largura de banda da sessão** para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que a largura de banda disponível não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações na largura de banda disponível ao longo das sessões do usuário podem impactar negativamente o desempenho.

Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a largura de banda necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre.

Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo da Central de Conhecimento CTX128190.

Compressão sem perdas

Ao usar a compressão sem perdas:

- O indicador sem perdas, um ícone na área de notificação, notifica o usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração da política de **Qualidade Visual** especifica **Construir para sem perdas**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.
- O switch sem perdas permite ao usuário mudar para o modo **Sempre sem perdas** a qualquer momento dentro da sessão. Para selecionar ou desmarcar Sem perdas a qualquer momento dentro de uma sessão, clique com o botão direito do mouse no ícone e clique em **Mudar para pixel perfeito** ou use o atalho **ALT+SHIFT+1**.
- Para compressão sem perdas: O HDX 3D Pro usa o codec sem perdas para compressão, independentemente do codec selecionado por meio da política.
- Para compressão com perdas: O HDX 3D Pro usa o codec original, seja o padrão ou o selecionado por meio da política.
- As configurações do switch sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Sempre sem perdas** na configuração da política de **Qualidade visual**.

Tecla de atalho sem perdas

Você pode usar uma tecla de atalho para selecionar ou desmarcar **Sem perdas** a qualquer momento dentro de uma sessão, usando o atalho padrão **ALT+SHIFT+1**.

Você pode substituir o atalho padrão, **ALT+SHIFT+1**, no Registro do Windows. Para configurar uma nova configuração de Registro, defina os seguintes valores de registro:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **Nome**: `HKLM_HotKey`
- **Tipo**: `String`

O formato para configurar uma combinação de atalho é `C=0|1, A=0|1, S=0|1, W=0|1, K=val`. As teclas devem ser separadas por vírgula “,” sem espaço. A ordem das teclas não importa.

A, C, S, W e K são teclas, onde C=Control, A=ALT, S=SHIFT, W=Win, e K=uma tecla válida onde os valores permitidos para K são 0–9, a–z e qualquer código de tecla 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

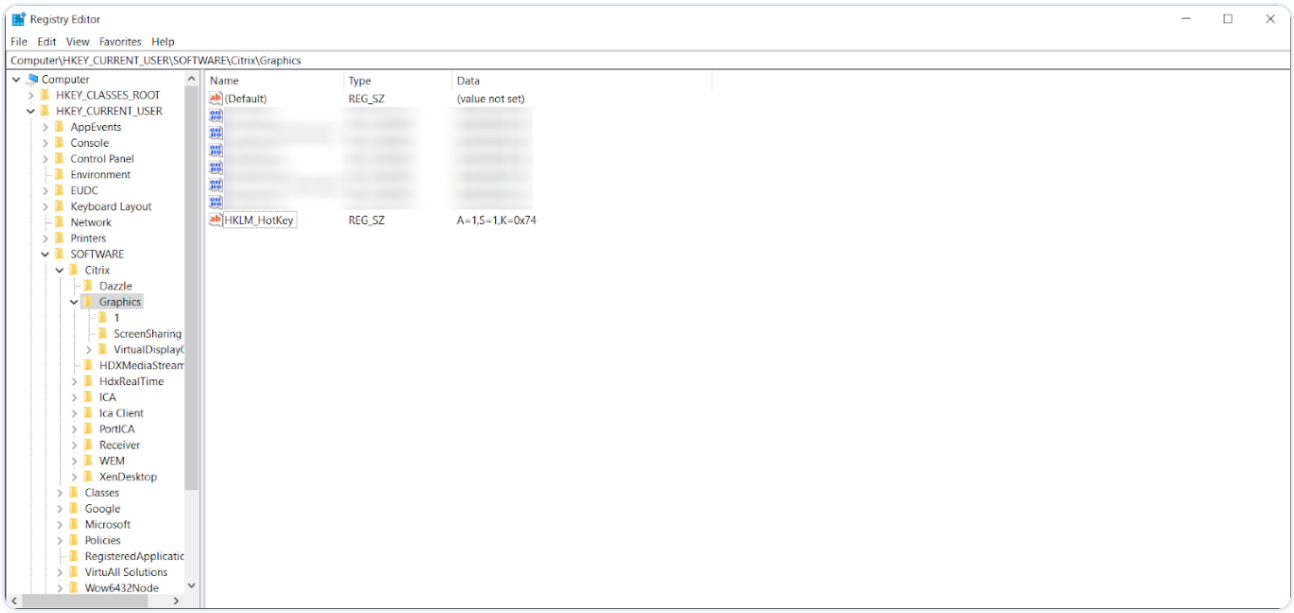
A tabela a seguir descreve a lista de exemplo de códigos de tecla virtual:

TECLA	VALOR
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74

TECLA	VALOR
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79
F11	0x7A
F12	0x7B
tecla PAGE UP	0x21
tecla PAGE DOWN	0x22
tecla END	0x23
tecla HOME	0x24
tecla SETA PARA A ESQUERDA	0x25
Tecla SETA PARA CIMA	0x26
Tecla SETA PARA A DIREITA	0x27
Tecla SETA PARA BAIXO	0x28

Certifique-se de que não há espaço entre as combinações de atalho. Por exemplo:

Correto: C=1,K=0x74 Incorreto: C=1, K=0x74



Cuidado:

A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Thinwire

Introdução

Thinwire, parte da tecnologia Citrix HDX, é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição.

Uma solução de exibição remota bem-sucedida oferece uma experiência de usuário altamente interativa, semelhante à de um PC local. O Thinwire alcança essa experiência usando uma variedade de técnicas complexas e eficientes de análise e compressão de imagem. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de exibição remota.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso de negócios gerais e é usado como a tecnologia de exibição remota padrão no Citrix Virtual Apps and Desktops.

HDX™ 3D Pro

Em sua configuração padrão, o Thinwire pode fornecer gráficos 3D ou altamente interativos e usar uma unidade de processamento gráfico (GPU), se presente. No entanto, recomendamos habilitar o modo HDX 3D Pro usando as políticas **Otimizar para carga de trabalho de gráficos 3D** ou **Qualidade visual > Construir para sem perdas** para cenários em que GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264, H.265 ou AV1) para codificar a tela inteira usando aceleração de hardware se uma GPU estiver presente. Fazer isso proporciona uma experiência mais fluida para gráficos profissionais 3D. Para obter mais informações, consulte H.264 Build to lossless, HDX 3D Pro e GPU acceleration for Windows Single-session OS.

Requisitos

O Thinwire é otimizado para sistemas operacionais modernos, incluindo Windows Server 2022, Windows Server 2019, Windows 10 e Windows 7. Para Windows Server 2008 R2, o modo gráfico legado é recomendado. Use os modelos de política Citrix integrados, Alta Escalabilidade de Servidor-SO Legado e Otimizado para WAN-SO Legado para fornecer as combinações recomendadas pela Citrix das configurações de política para esses casos de uso.

- A configuração de política que impulsiona o comportamento do Thinwire - **Usar codec de vídeo para compressão** está disponível em versões VDA no Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.6 FP3 e posterior. A opção **Usar codec de vídeo quando preferido** é a configuração padrão em versões VDA do Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.9 e posterior.
- Todos os aplicativos Citrix Workspace™ suportam Thinwire. Alguns aplicativos Citrix Workspace podem suportar recursos do Thinwire que outros não suportam, por exemplo, gráficos de 8 ou 16 bits para uso reduzido de largura de banda. O suporte para tais recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos do servidor (CPU, memória) em cenários de múltiplos monitores e alta resolução. É possível ajustar a quantidade de recursos que o Thinwire usa, no entanto, o uso da largura de banda pode aumentar como resultado.
- Em cenários de baixa largura de banda ou alta latência, considere habilitar gráficos de 8 ou 16 bits para melhorar a interatividade. A qualidade visual pode ser afetada, especialmente 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 com JPEG Adaptativo Configuração da política **Usar codec de vídeo para compressão**: **Não usar codec de vídeo**
- Thinwire com H.264, H.265 ou AV1 Seletivo Configuração da política **Usar codec de vídeo para compactação**: **Usar codec de vídeo quando preferencial** ou **Para regiões em alteração ativa**
- Thinwire com H.264, H.265 ou AV1 em Tela Cheia Configuração da política **Usar codec de vídeo para compactação**: **Para a tela inteira**

H.265

High Efficiency Video Coding (HEVC), também conhecido como H.265, é o sucessor do H.264. A codificação de hardware com o codec de vídeo H.265 é suportada nas seguintes GPUs:

- GPUs baseadas em NVIDIA Maxwell e superiores
- GPUs Intel de 6ª geração e superiores
- GPUs baseadas em AMD Raven e superiores

AV1

A Citrix adicionou suporte para o codec de vídeo AV1. O benefício do AV1 é que ele possui compactação de imagem superior, melhor qualidade de imagem e menor uso de largura de banda em comparação com H.264 e H.265.

Os seguintes requisitos para AV1 devem ser atendidos:

- VDA 2305 ou superior para GPUs NVIDIA, ou
- VDA 2308 ou superior para GPUs Intel

As seguintes GPUs são compatíveis para codificação:

- GPU baseada em NVIDIA Ada Lovelace
- GPUs Intel ARC ou Intel Data Center GPU Flex Series

Para obter mais informações sobre as GPUs Ada Lovelace da NVIDIA, consulte arquitetura ADA.

Para obter mais informações sobre as GPUs Flex Series para estações de trabalho e data centers ARC da Intel, consulte série Flex e Visão geral.

Seleção automática de codec de vídeo

Você pode detectar automaticamente o melhor codec de vídeo a ser usado quando a política **Usar codec de vídeo** para compactação estiver ativada ou Otimizar para carga de trabalho de gráficos 3D estiver ativada no VDA. Durante a instalação do aplicativo Citrix Workspace para Windows, os recursos de decodificação do endpoint são avaliados. Com base nessas informações, o aplicativo Citrix Workspace para Windows negocia o melhor codec a ser usado com o VDA na conexão. A lista a seguir descreve a ordem em que os codecs de vídeo são avaliados:

- AV1
- H.265
- H.264

A seleção automática se aplica apenas a variantes 4:2:0 desses codecs. Se a configuração **Qualidade Visual** estiver definida como 'Build-to-Lossless' ou 'Always Lossless' e quando Permitir Visualmente Sem Perdas estiver definida como 'ativado', a seleção automática do codec de vídeo será desativada.

Ao se conectar a um recurso, o aplicativo Citrix Workspace testa a capacidade do endpoint de decodificar H.265 e AV1 e salva os recursos no registro. O aplicativo Citrix Workspace seleciona automaticamente o melhor codec de vídeo a ser usado e o negocia com o VDA. Se tanto o VDA quanto o cliente puderem usar H.265 e AV1, o AV1 será selecionado como o codec de vídeo. Se o AV1 não estiver disponível no VDA ou no cliente, o H.265 será negociado. Se o H.265 também não estiver disponível em nenhum dos dois, a sessão usará o H.264 como codec de vídeo.

> **Observação:**
>
> Este recurso está ativado por padrão. Esse comportamento pode ser alterado definindo a nova configuração de registro do lado do cliente `DisableDecoderCaps`.
>
> Para desativar a seleção automática do codec de vídeo, defina 'DisableDecoderCaps' como `HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1` ou `HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`.

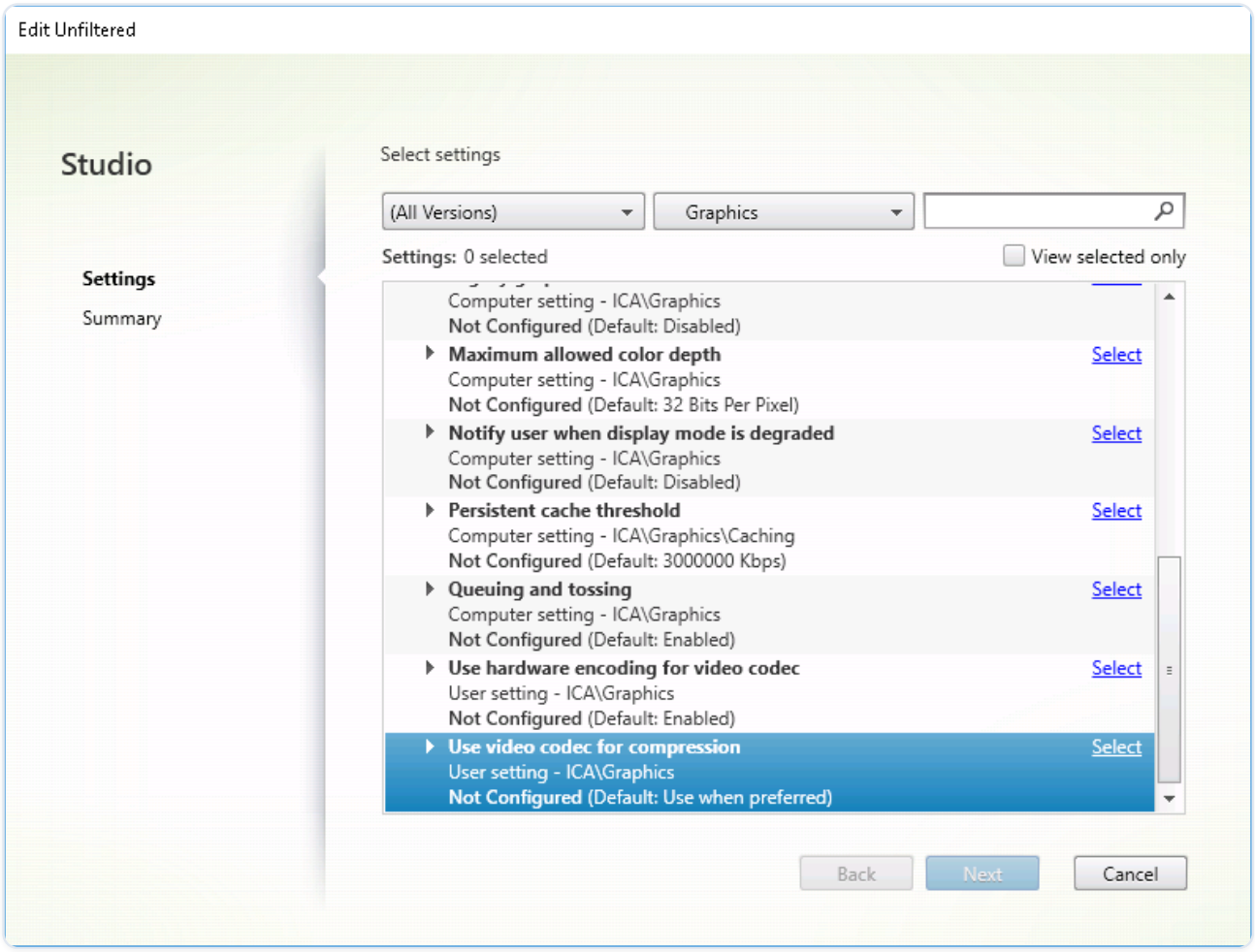
Se qualquer um desses valores for definido como 1, a seleção automática do codec de vídeo não será usada. O indicador de status gráfico e o monitor HDX podem monitorar o codec de vídeo.

Configuração

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:

- Usar codec de vídeo para compactação
  - **Usar codec de vídeo quando preferencial**. Esta é a configuração padrão. Nenhuma configuração adicional é necessária. Manter esta configuração como padrão garante que o Thinwire seja selecionado para todas as conexões Citrix e seja otimizado para escalabilidade, largura de banda e qualidade de imagem superior para cargas de trabalho de desktop típicas. Isso é funcionalmente equivalente a **Para regiões em mudança ativa**.
- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:
  - **Para regiões em mudança ativa**. A tecnologia de exibição adaptativa no Thinwire identifica imagens em movimento (vídeo, 3D em movimento) e usa H.264, H.265 ou AV1 apenas na parte da tela onde a imagem está se movendo.
  - **Para a tela inteira**. Oferece Thinwire em tela cheia com H.264, H.265 ou AV1 para otimizar a experiência do usuário e a largura de banda em casos de uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visualmente sem perdas** está desabilitada), a imagem final não é perfeita em pixels (sem perdas) e pode não ser adequada para certos cenários. Nesses casos, considere usar H.264 Build to lossless ou H.265 Build to lossless em vez disso.



Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de exibição remota. O Thinwire as suporta todas.

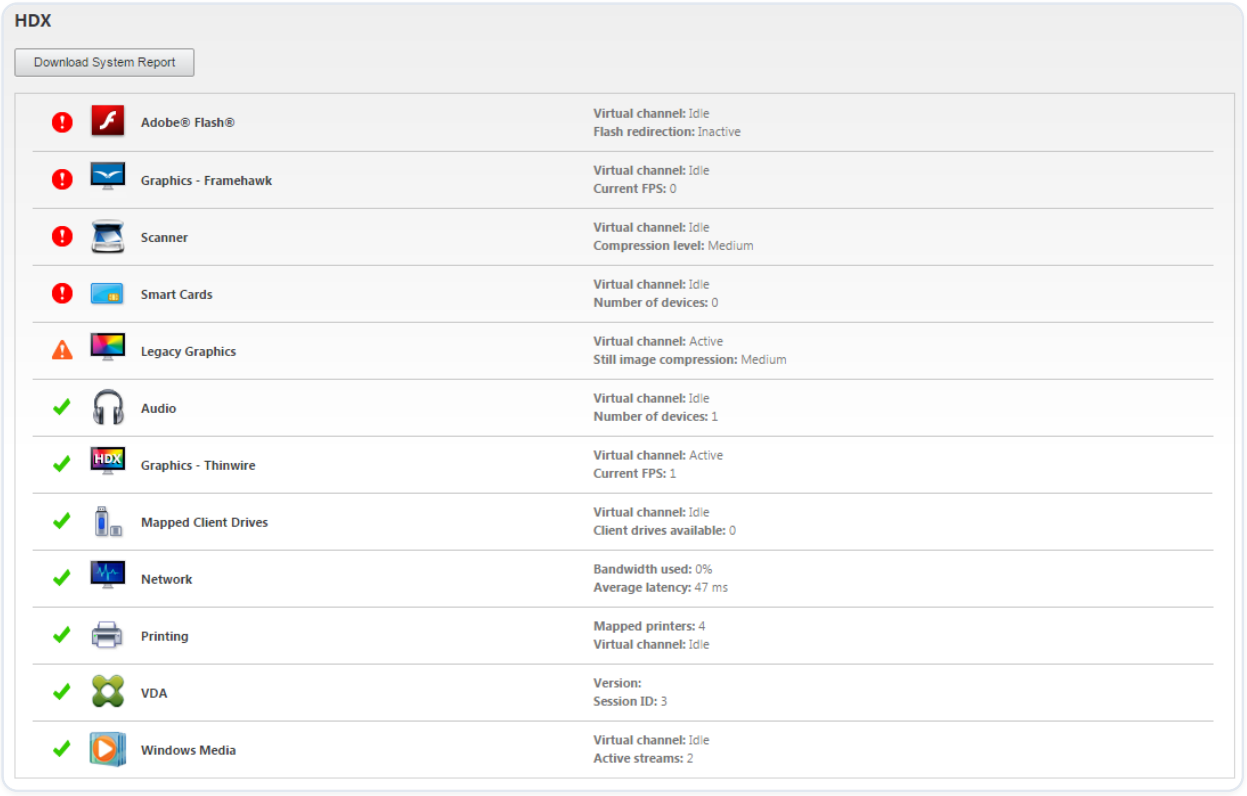
- Profundidade de cor preferencial para gráficos simples
- Taxa de quadros alvo
- Qualidade visual

Para obter as combinações de configurações de política recomendadas pela Citrix para diferentes casos de uso de negócios, use os modelos de política Citrix integrados. Os modelos **Alta Escalabilidade de Servidor** e **Experiência de Usuário de Altíssima Definição** usam o Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos seus usuários.

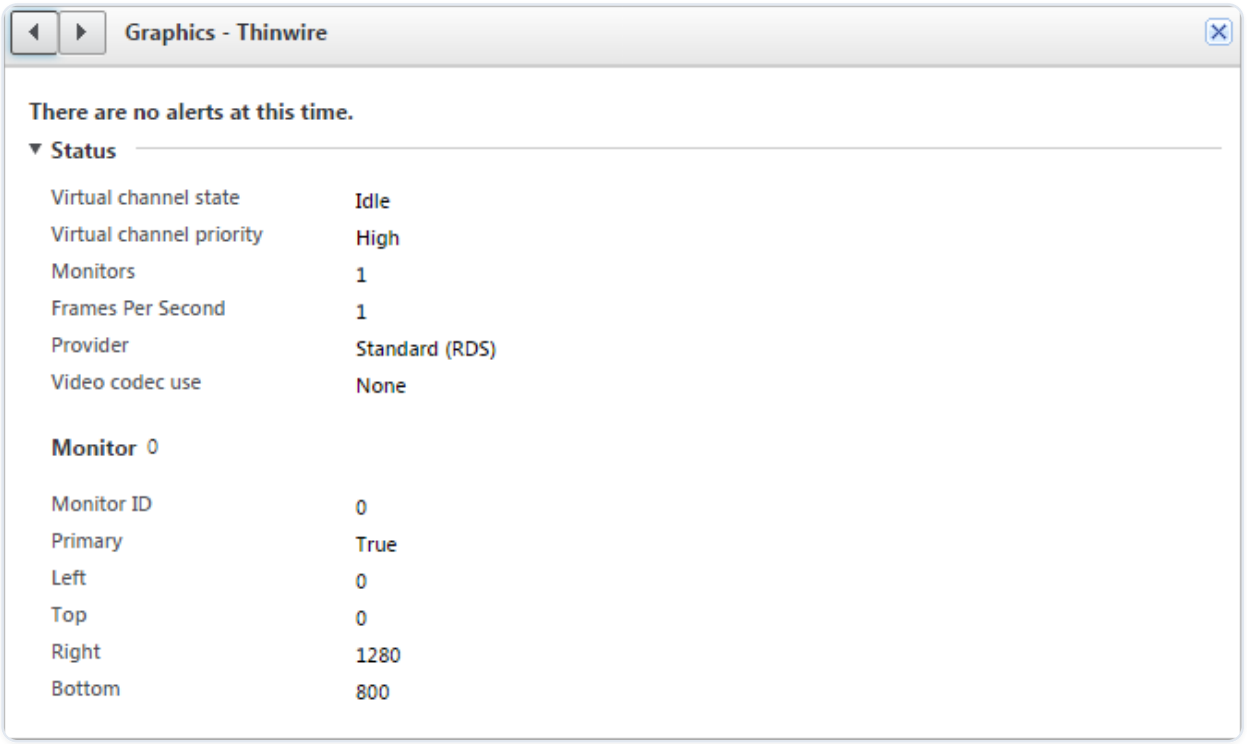
Monitorando o Thinwire

Você pode monitorar o uso e o desempenho do Thinwire a partir do Citrix Director. A visualização de detalhes do canal virtual HDX contém informações úteis para solucionar problemas e monitorar o Thinwire em qualquer sessão. Para visualizar métricas relacionadas ao Thinwire:

1. No Director, procure um usuário, máquina ou endpoint, abra uma sessão ativa e clique em **Detalhes**. Ou, você pode selecionar **Filtros** > **Sessões** > **Todas as Sessões**, abrir uma sessão ativa e clicar em **Detalhes**.
2. Role para baixo até o painel **HDX**.



3. Selecione **Graphics - Thinwire**.



Codec de compressão sem perdas (MDRLE)

Em uma sessão de desktop típica, a maioria das imagens são gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas usando o codec 2DRLE. No lado do cliente do aplicativo Citrix Workspace, esses elementos são decodificados usando o decodificador 2DRLE do lado do aplicativo Citrix Workspace para exibição da sessão.

No XenApp e XenDesktop 7.17, adicionamos um codec MDRLE com taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este novo codec não afeta a escalabilidade do servidor.

Menor largura de banda geralmente significa interatividade de sessão aprimorada (especialmente em links compartilhados ou restritos) e custos reduzidos.

A configuração não é necessária para o codec MDRLE. Se o aplicativo Citrix Workspace suportar a decodificação MDRLE, o VDA usa a codificação MDRLE do VDA e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA retorna automaticamente para a codificação 2DRLE.

Requisitos do MDRLE:

- Citrix Virtual Apps and Desktops versão mínima 7 1808 VDAs
- XenApp e XenDesktop versão mínima 7.17 VDAs
- Citrix Workspace app para Windows versão mínima 1808
- Citrix Receiver para Windows versão mínima 4.11

Modo Progressivo

O Citrix Virtual Apps and Desktops 1808 introduziu o modo progressivo e o habilitou por padrão. Em condições de rede restritas (padrão: largura de banda < 2 Mbps ou latência > 200 ms), o Thinwire aumentou a compressão de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens altamente compactados são então progressivamente aprimorados, de forma aleatória em blocos, quando a atividade da tela para. Embora compactar e aprimorar dessa forma melhore a interatividade geral, isso reduz a eficiência do cache e aumenta o uso da largura de banda.

A partir do Citrix Virtual Apps and Desktops 1906, o modo progressivo está desabilitado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada nas condições da rede e flutua entre um valor mínimo e máximo predefinido para cada configuração de **Qualidade visual**. Como não há uma etapa de aprimoramento explícita, o

Thinwire otimiza a entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

Alterando o comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a chave do registro. Para obter informações, consulte Modo progressivo na lista de recursos gerenciados por meio do registro.

Construção para sem perdas

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 de **Qualidade visual** como **Build to lossless**.

O Build to lossless compacta a tela usando H.264, H.265 ou AV1 durante a atividade da tela e aprimora para pixel perfeito (sem perdas) quando a atividade para. A qualidade da imagem com perdas se adapta aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de aprimoramento é realizada gradualmente. Por exemplo, selecionar um modelo e girá-lo.

Build to lossless oferece todas as vantagens de usar um codec de vídeo para a tela inteira, 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 pixel perfeito. Por exemplo, manipular imagens médicas. Além disso, o H.264 **Build to lossless** usa menos recursos do que o H.264 4:4:4 em tela cheia. Como resultado, usar o **Build to lossless** geralmente resulta em uma taxa de quadros mais alta do que o H.264 4:4:4 visualmente sem perdas.

> **Observação:**
>
> Você pode desabilitar o uso de um codec de vídeo ao usar um build to lossless. Basta definir a política **Usar codec de vídeo** como `Do not use video codec`. Isso resulta em imagens em movimento sendo codificadas com JPEG Adaptativo em vez disso.

Codificação visualmente sem perdas

A codificação visualmente sem perdas usa o espaço de cores YUV 4:4:4 em vez do espaço de cores YUV 4:2:0 com subamostragem de croma para compressão de codec de vídeo. Isso garante que nenhuma informação de cor seja perdida durante a conversão do espaço de cores e, uma vez decodificada, seja visualmente imperceptível da imagem RGB original.

Considere o seguinte exemplo. Se usar um codec de vídeo para compactar a tela inteira, a compressão de cor 4:2:0 pode degradar detalhes de alto contraste, como texto, tornando-os borrados e mais difíceis de ler. Em contraste, o 4:4:4 preserva quase todas as informações de cor e não exibe nenhuma degradação visualmente perceptível.



Cargas de trabalho que exigem qualidade de pixel perfeita ou exibição de cores precisas podem se beneficiar da codificação visualmente sem perdas.

A codificação visualmente sem perdas está disponível com H.264 e H.265. A codificação H.264 4:4:4 é uma solução puramente baseada em software e, como resultado, pode haver um impacto significativo na utilização da CPU tanto no VDA quanto no cliente. Isso também pode afetar a taxa de quadros.

O suporte a H.265 4:4:4 foi adicionado com o lançamento do Citrix Workspace app 2305, permitindo que o Thinwire use uma GPU no VDA e no cliente para codificação H.265 4:4:4, melhorando significativamente o desempenho.

Para permitir a codificação visualmente sem perdas 4:4:4, duas políticas precisam ser habilitadas:

- **Qualidade Visual**: Definido como `Build to Lossless` ou `Always Lossless`
- **Permitir Sem Perda Visual**: Definido como `Enabled`

> **Observação:**

> Se **Permitir Sem Perda Visual** não estiver ativado, mudamos para nosso codificador Thinwire em `Build to lossless` ou `Always Lossless`.

> H.265 4:4:4 sem perda visual tem os requisitos adicionais:

- GPUs NVIDIA exigem a versão VDA 2209 ou superior
- GPUs Intel exigem a versão VDA 2308 ou superior

As seguintes GPUs são suportadas para H.265 4:4:4:

- GPUs NVIDIA de geração Pascal e posteriores
- GPUs Intel de 10ª geração e posteriores

Para o cliente, é necessária a versão 2305 do Citrix Workspace app para Windows (a versão 2309.1 é recomendada).

A decodificação de hardware de H.265 4:4:4 é possível com as seguintes GPUs de dispositivo cliente:

- GPUs NVIDIA de geração Turing e posteriores
- GPUs Intel de 10ª geração e posteriores

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e a permitir o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que é uma camada de texto, exibida sobre toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte de VDA.

> **Importante:**

> A marca d'água de sessão baseada em texto não é um recurso de segurança. A solução não impede completamente o roubo de dados, mas oferece algum nível de dissuasão e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar esse recurso, recomendamos que você o combine com outras soluções de segurança, conforme aplicável.

> A marca d'água da sessão é um texto e é aplicada à sessão entregue ao usuário. A marca d'água da sessão contém informações para rastrear o roubo de dados. Os dados mais importantes são a identidade do usuário de logon da sessão atual na qual a imagem da tela foi capturada. Para rastrear o vazamento de dados de forma mais eficaz, inclua outras informações, como o endereço IP do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as configurações de política de marca d'água da sessão para configurar o posicionamento e a aparência da marca d'água na tela.

Requisitos:

Agentes de Entrega Virtual:

SO multissessão 7.17 SO de sessão única 7.17

Limitações:

- As marcas d'água de sessão não são suportadas em sessões onde são usados Acesso a Aplicativos Locais, redirecionamento de mídia do Windows, MediaStream, redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5. Para usar a marca d'água de sessão, certifique-se de que esses recursos estejam desabilitados.
- A marca d'água de sessão não é suportada e não aparece se a sessão estiver sendo executada em modos acelerados por hardware em tela cheia (codificação H.264 ou H.265 em tela cheia).
- Se você definir estas políticas HDX™, as configurações de marca d'água não terão efeito e uma marca d'água não será exibida na tela da sessão.

Usar codificação de hardware para codec de vídeo para **Ativado Usar codec de vídeo para compactação** para **Para a tela inteira**

- Se você definir estas políticas HDX, o comportamento é indeterminado e a marca d'água pode não ser exibida.

  Usar codificação de hardware para codec de vídeo para **Ativado Usar codec de vídeo para compactação** para **Usar codec de vídeo quando preferencial**

  Para garantir que a marca d'água seja exibida, defina **Usar codificação de hardware para codec de vídeo** como **Desativado**, ou defina **Usar codec de vídeo para compactação** como **Para regiões em mudança ativa** ou **Não usar codec de vídeo**.
- A marca d'água de sessão suporta apenas o modo gráfico Thinwire.
- Se você usa Gravação de Sessão, a sessão gravada não inclui a marca d'água.
- Se você usa assistência remota do Windows, a marca d'água não é exibida.
- Se um usuário pressionar a tecla **Print Screen** para capturar a tela, a tela capturada no lado do VDA não inclui as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

Compartilhamento de tela

O compartilhamento de tela permite que um usuário compartilhe uma sessão do Citrix Virtual Desktop com outras pessoas, incluindo o conteúdo da tela, teclado e controles do mouse.

Requisitos do sistema

- Windows: VDA de SO de sessão única ou multi-sessão
- Linux: Consulte a documentação do Linux VDA para obter mais informações sobre o compartilhamento de sessões Linux.
- Somente sessões de desktop podem ser compartilhadas.
- Deve haver conectividade de rede entre o VDA que hospeda a sessão e as máquinas que se conectam às sessões compartilhadas. Os requisitos de porta de rede são baseados nas portas ICA em uso (TCP/UDP 1494 ou 2598) e na configuração da política de compartilhamento de tela (TCP 52525 a 52625 por padrão).

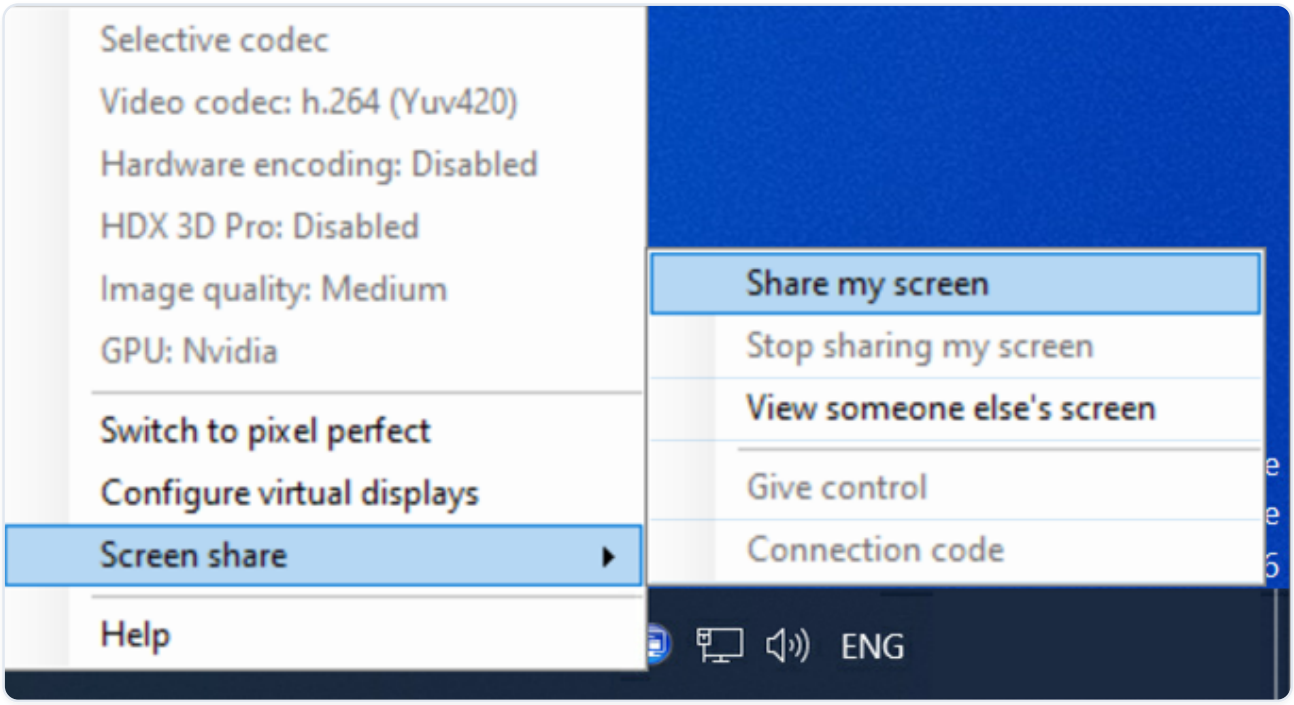
Configuração

O compartilhamento de tela deve ser habilitado usando políticas Citrix. O compartilhamento de tela é desabilitado por padrão. Configure a política de compartilhamento de tela para habilitar ou desabilitar a função e atribuir o intervalo de portas de rede utilizáveis.

Habilite a política de indicador de status gráfico para exibir a interface do usuário que inclui controles para compartilhar e conectar-se a sessões.

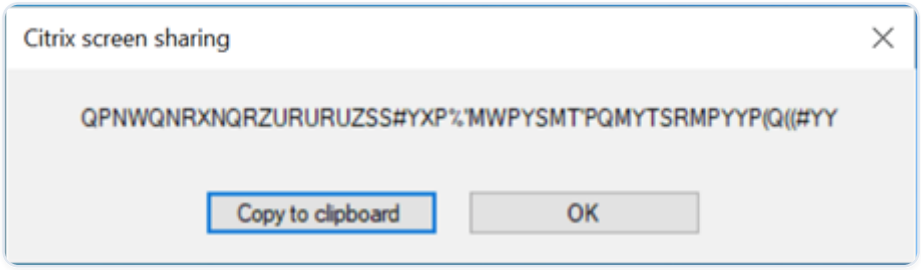
Compartilhando uma sessão

Para compartilhar uma sessão, procure o ícone do indicador de status gráfico HDX™ na área de notificação do Windows. Clique com o botão direito do mouse para exibir o menu e selecione **Compartilhar tela > Compartilhar minha tela**.



Clique em **Copiar para a área de transferência** ou selecione e copie manualmente a string inteira mostrada na caixa de diálogo. A string pode então ser colada no aplicativo de sua escolha, como um cliente de e-mail ou IM, para ser distribuída a outros usuários.

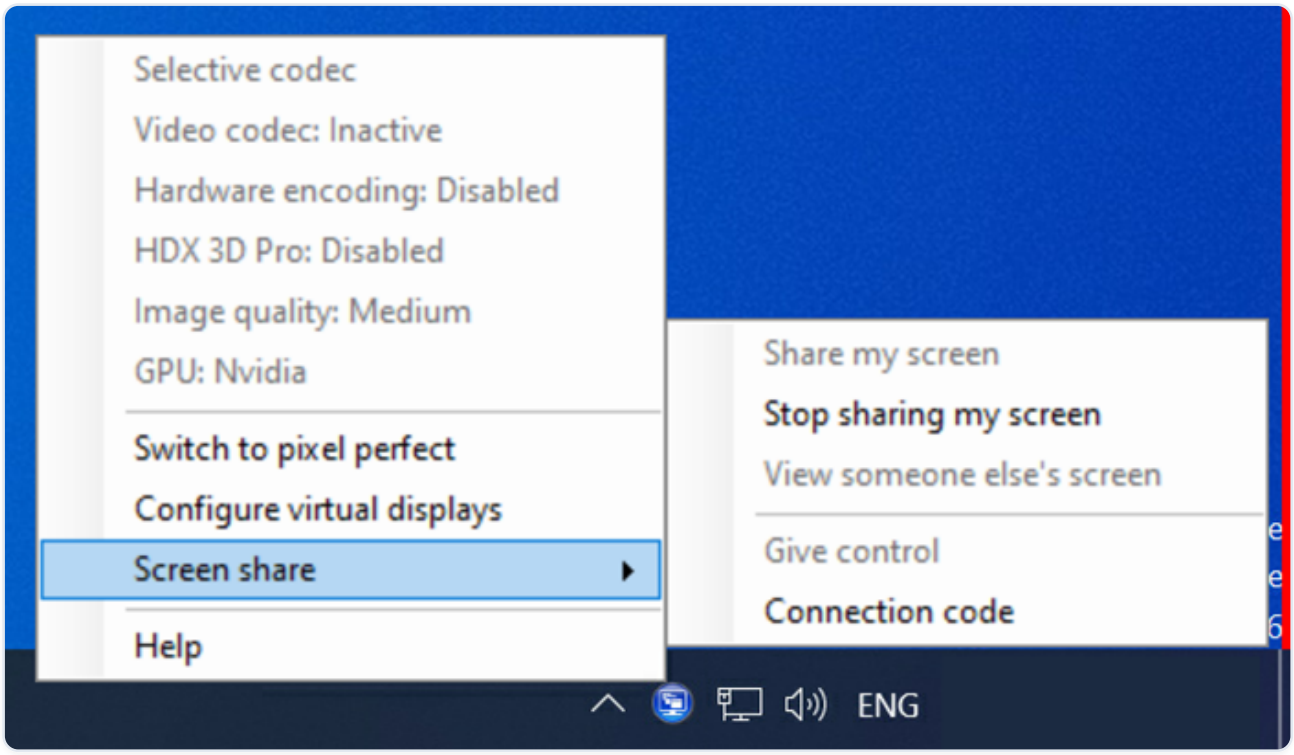
Clique em **OK** ou no **x** para fechar a caixa de diálogo. O código de conexão pode ser recuperado na opção de menu **Compartilhar tela > Código de conexão** a qualquer momento enquanto a sessão estiver sendo compartilhada.



Um contorno vermelho aparece ao redor da tela como um indicador de que a sessão está sendo compartilhada e é visível para outras pessoas.

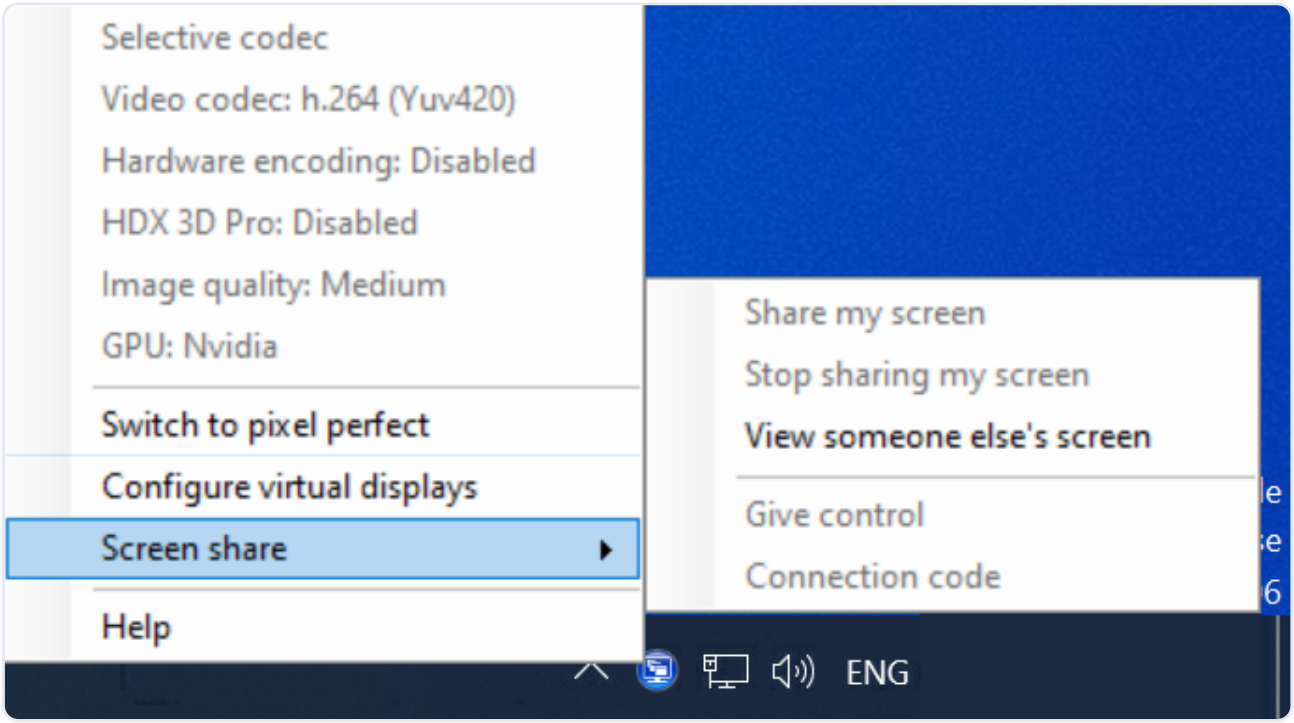
Os controles de teclado e mouse também podem ser compartilhados com outros usuários usando a opção de menu **Compartilhar tela > Conceder controle**.

Use a opção de menu **Compartilhar tela > Parar de compartilhar minha tela** para parar de compartilhar a sessão e desconectar todos os usuários.

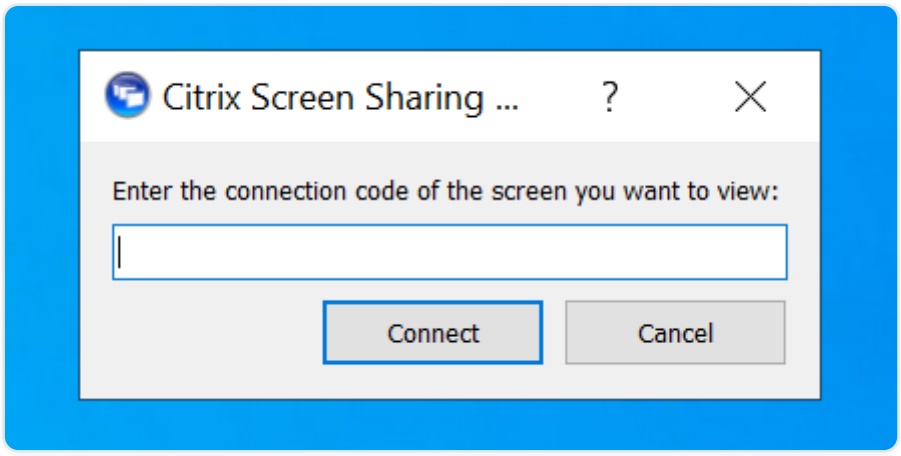


Conectando a uma sessão compartilhada

Para se conectar às sessões de outra pessoa, procure o ícone do indicador de status gráfico HDX na área de notificação do Windows. Clique com o botão direito nele para exibir o menu e selecione **Compartilhar tela > Visualizar a tela de outra pessoa**.

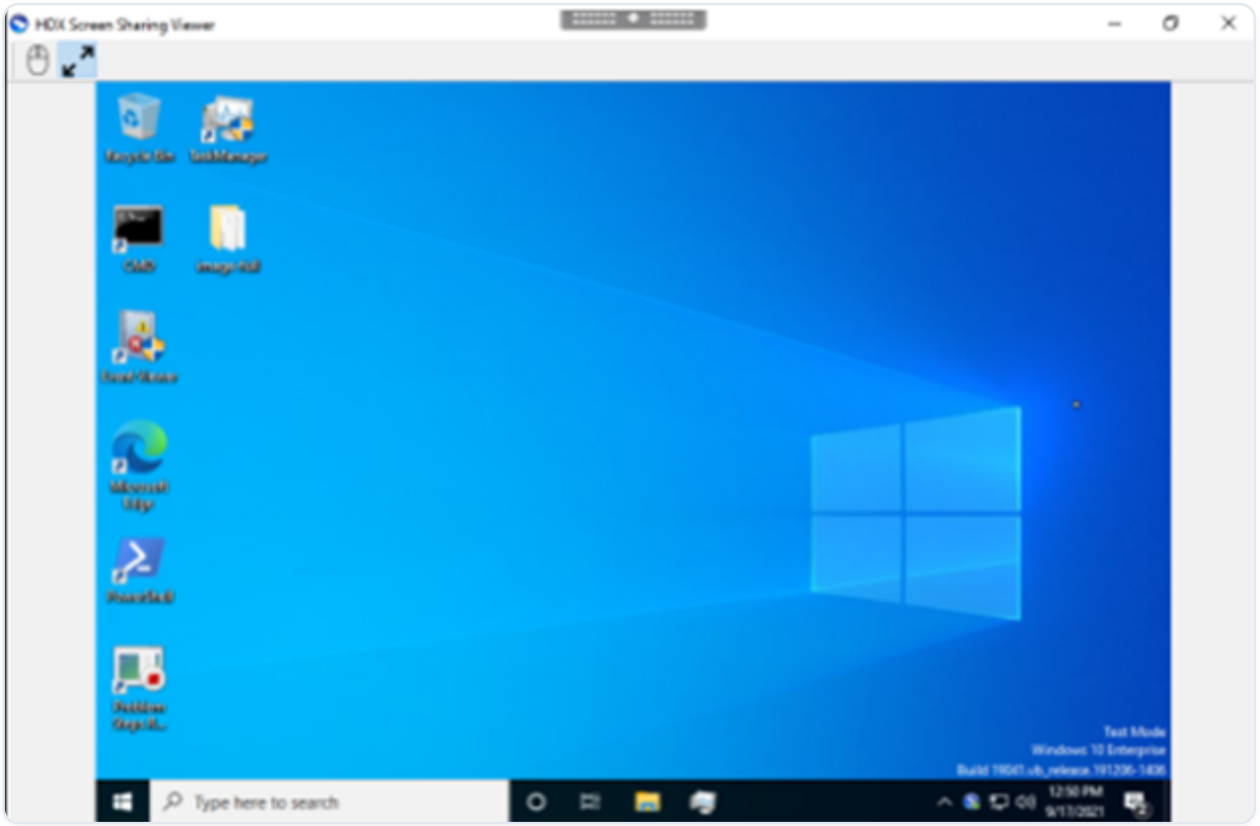


Insira ou cole a string de conexão fornecida pelo usuário que está compartilhando a sessão na caixa de texto. Clique em **Conectar** para estabelecer a conexão.



Você pode solicitar controles de teclado e mouse clicando no ícone do mouse no canto superior esquerdo da janela **HDX Screen Sharing Viewer**.

Feche a janela **HDX Screen sharing Viewer** para desconectar-se da sessão compartilhada a qualquer momento.



Outras considerações

- O aplicativo visualizador de compartilhamento de tela está incluído no VDA em *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* e pode ser implantado como um aplicativo publicado usando um Virtual Apps Server. Este modelo de implantação alternativo permite a colaboração com usuários que não têm acesso a um desktop virtual.

- O número de usuários permitidos para se conectar a uma sessão compartilhada pode ser limitado usando o intervalo de portas de rede na política de compartilhamento de tela. Uma porta é necessária por usuário. O intervalo padrão permite no máximo 100 usuários.
- Todos os monitores conectados à sessão são compartilhados. Não é possível selecionar monitores individuais.
- O codec de vídeo H.265 não é suportado.

Layout de exibição virtual

A interface do usuário de configuração de exibição virtual permite definir um layout de exibição virtual por monitor de sessão no VDA, dentro de uma sessão ativa. Esse recurso permite dividir cada monitor de sessão independentemente em vários monitores virtuais. Você pode dividir em um total de 8 monitores virtuais na área de trabalho remota. Além disso, você pode atualizar o monitor primário da sessão e as configurações de DPI para as exibições.

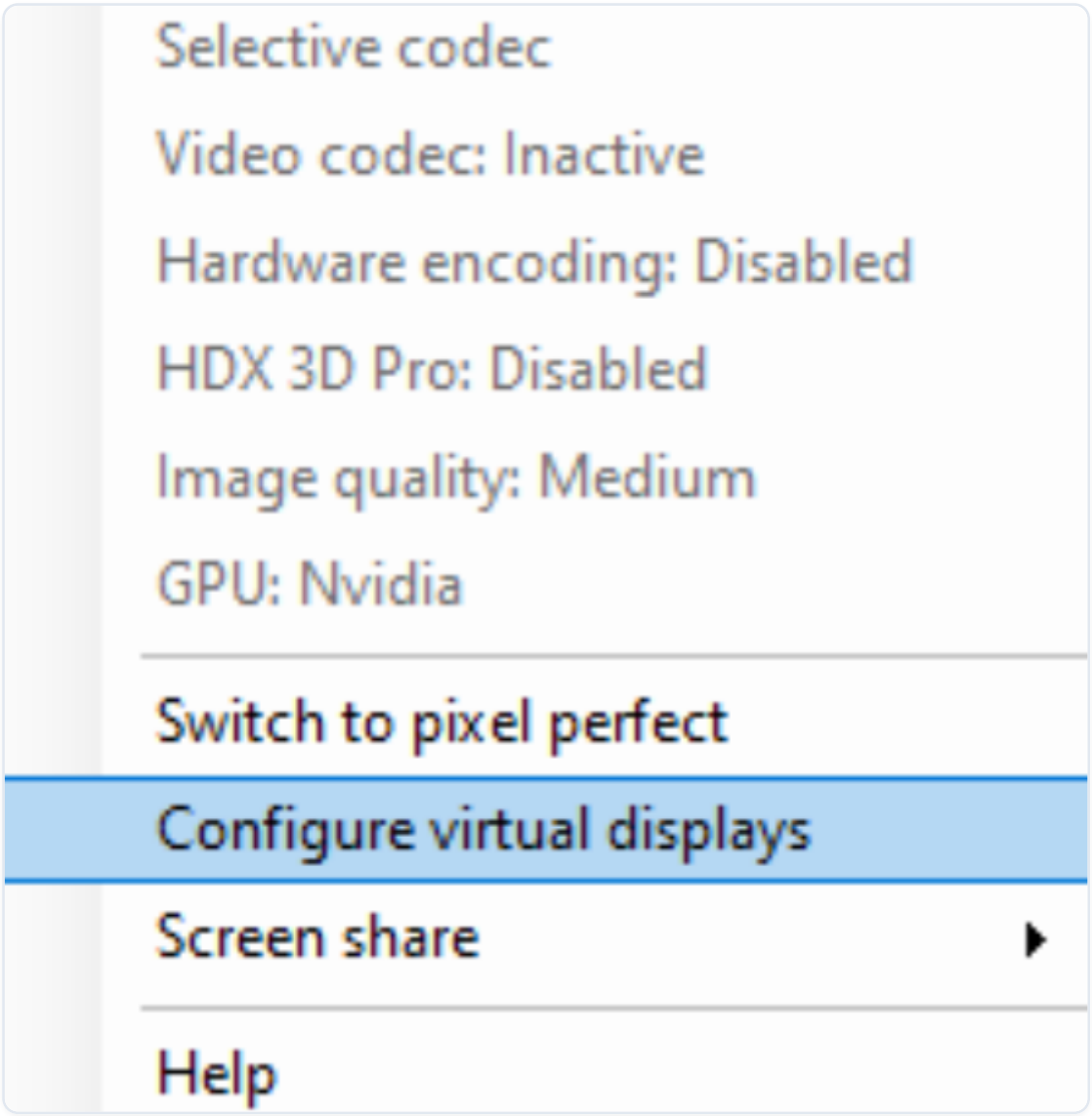
A configuração de exibição virtual é armazenada por usuário por dispositivo cliente. A configuração se aplica a todas as conexões subsequentes de um determinado cliente para um usuário específico. Ela é persistida durante o redimensionamento da sessão, desconexão ou reconexão da sessão e logoff ou logon da sessão. A redefinição do layout de exibição virtual configurado ocorre no redimensionamento da sessão e na alteração do número de monitores de sessão.

Requisitos do sistema

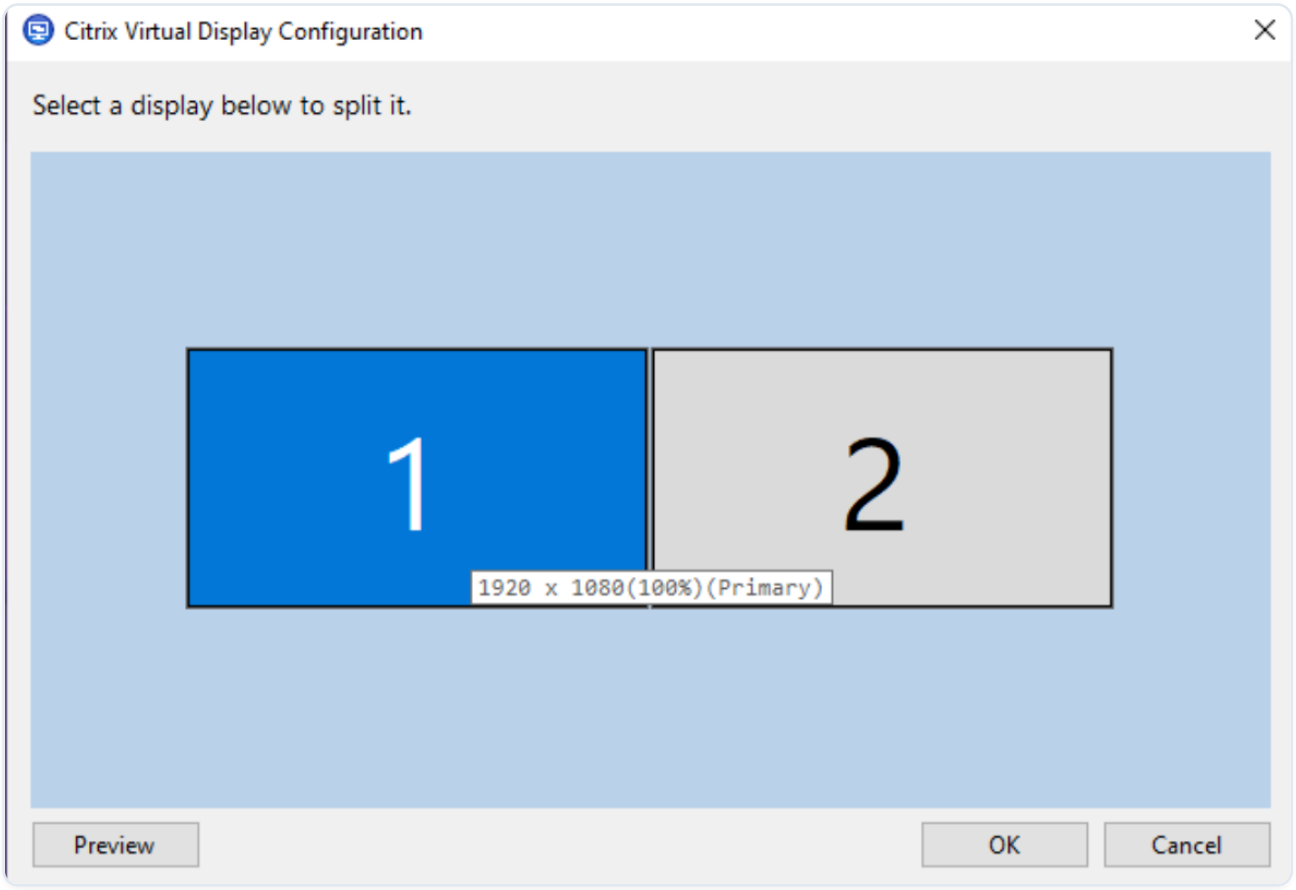
- Windows: VDA de SO de sessão única ou multi-sessão
- A política de (/pt-br/citrix-virtual-apps-desktops/2407/policies/reference/ica-policy-settings/graphics-policy-settings.html#graphics-status-indicator) deve estar habilitada
- Somente sessões de área de trabalho podem ser configuradas.

Configuração

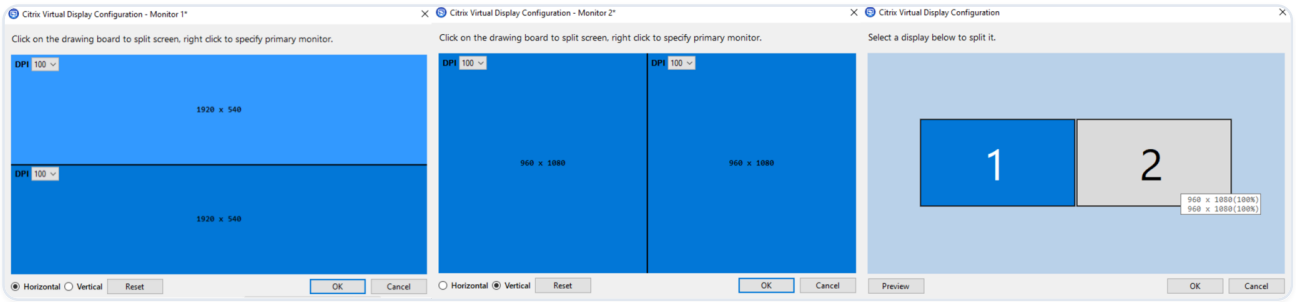
Para configurar o layout de exibição virtual, clique com o botão direito do mouse no ícone do indicador de status gráfico e selecione a opção Configurar exibições virtuais. A interface do usuário de configuração de exibição virtual é iniciada.



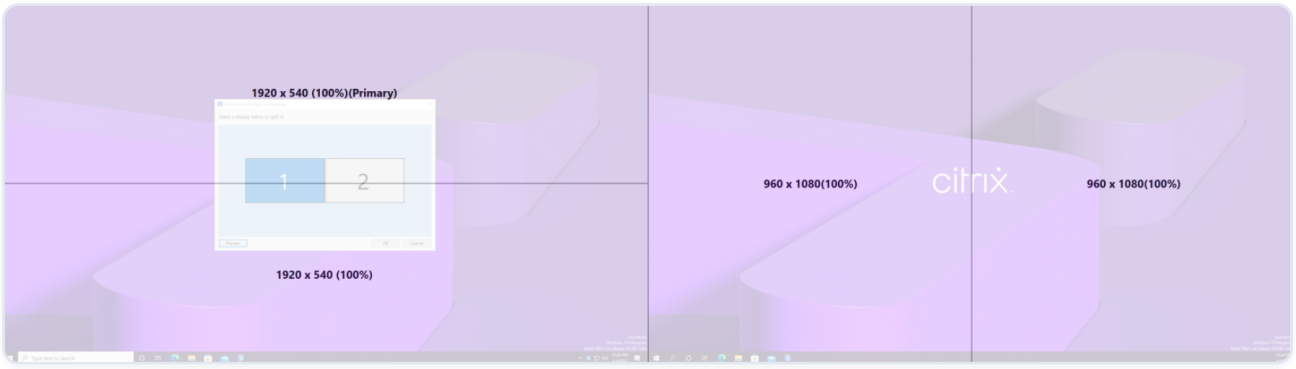
A interface do usuário mostra o layout de exibição da sessão atual, com o azul indicando o monitor primário da sessão. Você pode ver a dica de ferramenta de configurações de exibição ao passar o mouse sobre uma exibição. A dica de ferramenta fornece informações sobre o layout de exibição virtual atual definido em um determinado monitor de sessão.



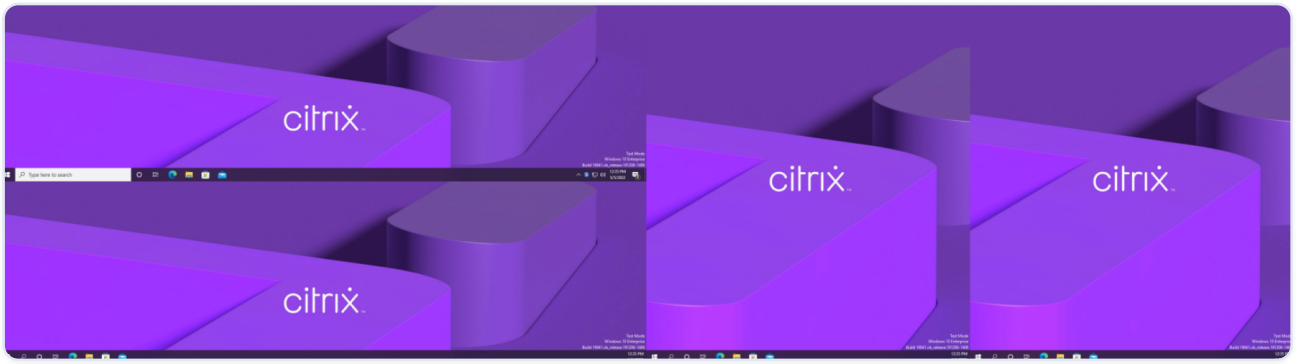
Selecione uma exibição para fazer a transição para uma interface do usuário interativa, que permite configurar exibições virtuais para o monitor de sessão selecionado. Você pode desenhar linhas horizontais ou verticais para separar a tela em monitores virtuais. A tela é dividida de acordo com as porcentagens especificadas das resoluções do monitor de sessão. Clique com o botão direito do mouse em uma exibição virtual para marcá-la como monitor primário e use a lista suspensa de DPI para definir um fator de escala preferencial para a exibição virtual. Depois de definir um layout de exibição virtual, clique em **OK** para salvar temporariamente o layout ou em **Cancelar** para descartar quaisquer alterações. Você pode usar **Redefinir** para desfazer a configuração e restaurar o layout original para o monitor de sessão.



Para visualizar o layout de exibição virtual configurado atualmente, clique no botão **Visualizar**. Uma janela aparece para destacar a posição e a resolução esperadas das exibições virtuais na sessão.



Clique em **OK** para aplicar e salvar imediatamente o layout de exibição virtual. Clique em **Cancelar** para fechar a interface do usuário e descartar todas as alterações.

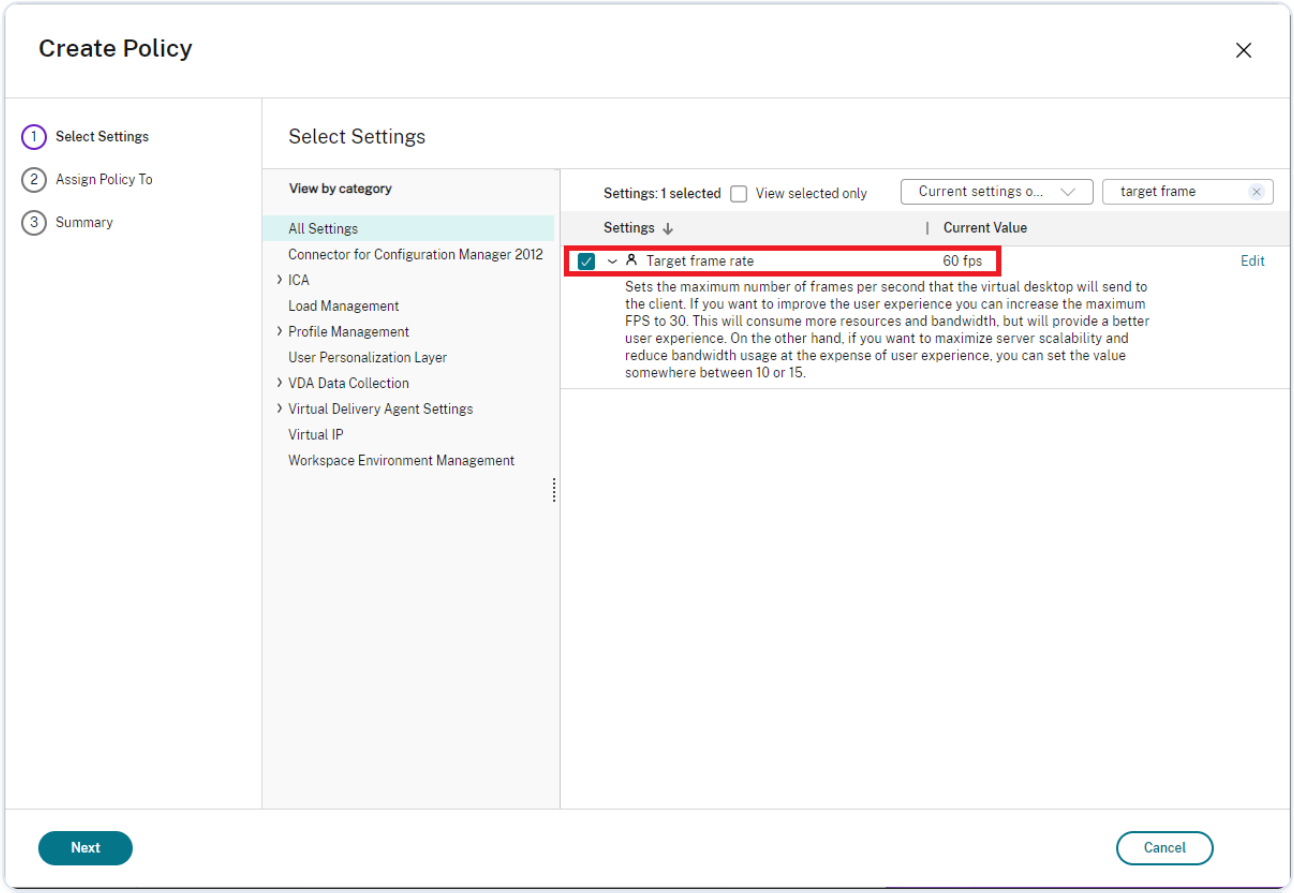


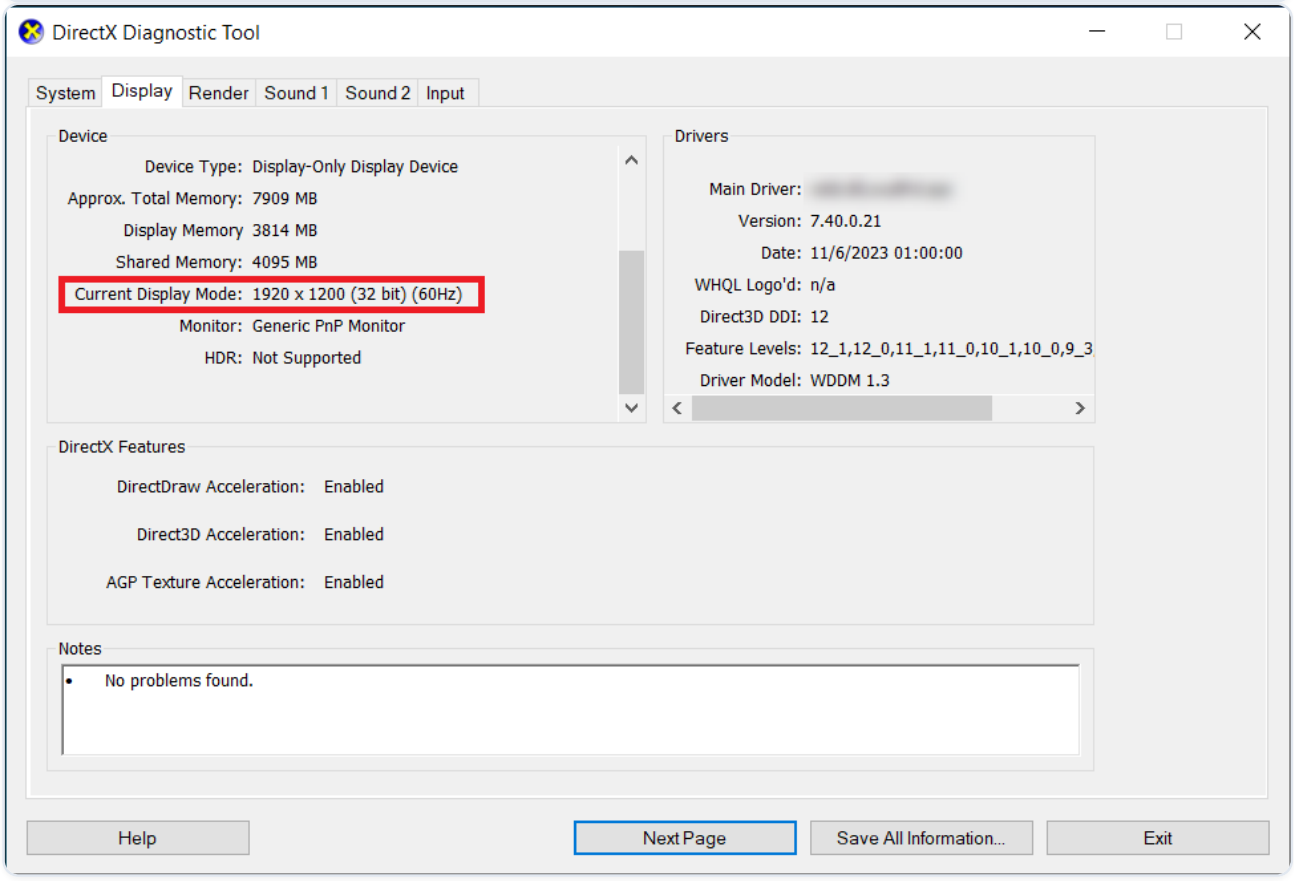
Outras considerações

- A resolução mínima de tela virtual necessária é 640 x 480.
- O DPI da tela virtual definido pela interface do usuário depende do suporte de dimensionamento do SO para a resolução de tela fornecida.
- Não use este recurso simultaneamente com o recurso de tela virtual existente no aplicativo Citrix Workspace™.
- A funcionalidade de visualização não é compatível com o Server 2016.

Taxa de atualização adaptativa

Com as novas melhorias de escalabilidade, o HDX™ ajusta a taxa de atualização dos monitores virtuais para corresponder à política de FPS de destino definida. A Taxa de Atualização Adaptativa (ARR) está disponível para VDAs de sessão única e multissessão e funciona para cenários acelerados por GPU e não-GPU.


Create Policy
1 Select Settings
2 Assign Policy To
3 Summary
Select Settings
View by category
All Settings
Connector for Configuration Manager 2012
ICA
Load Management
Profile Management
User Personalization Layer
VDA Data Collection
Virtual Delivery Agent Settings
Virtual IP
Workspace Environment Management
Settings: 1 selected
View selected only
Current settings o...
target frame
Settings
Current Value
Target frame rate
60 fps
Edit
Sets the maximum number of frames per second that the virtual desktop will send to the client. If you want to improve the user experience you can increase the maximum FPS to 30. This will consume more resources and bandwidth, but will provide a better user experience. On the other hand, if you want to maximize server scalability and reduce bandwidth usage at the expense of user experience, you can set the value somewhere between 10 or 15.
Next
Cancel


DirectX Diagnostic Tool
System
Display
Render
Sound 1
Sound 2
Input
Device
Device Type: Display-Only Display Device
Approx. Total Memory: 7909 MB
Display Memory 3814 MB
Shared Memory: 4095 MB
Current Display Mode: 1920 x 1200 (32 bit) (60Hz)
Monitor: Generic PnP Monitor
HDR: Not Supported
Drivers
Main Driver:
Version: 7.40.0.21
Date: 11/6/2023 01:00:00
WHQL Logo'd: n/a
Direct3D DDI: 12
Feature Levels: 12_1,12_0,11_1,11_0,10_1,10_0,9_3
Driver Model: WDDM 1.3
DirectX Features
DirectDraw Acceleration: Enabled
Direct3D Acceleration: Enabled
AGP Texture Acceleration: Enabled
Notes
No problems found.
Help
Next Page
Save All Information...
Exit

Observação

> A Taxa de Atualização Adaptativa está disponível apenas quando o Citrix Indirect Display ou IDD é usado (conforme o padrão do Citrix Virtual Apps and Desktops™) e não está disponível ao usar Adaptadores de Exibição fornecidos pelo Fornecedor.

Modo tolerante a perdas

O modo tolerante a perdas para gráficos foi completamente reformulado para garantir que a sessão permaneça interativa quando a perda de pacotes é detectada. Quando as condições da rede se degradam além dos limites predefinidos de largura de banda, latência e perda de pacotes, o codificador gráfico Citrix® muda automaticamente para um modo mais agressivo de entrega de pacotes para superar o efeito da perda de pacotes. Como resultado, o uso da largura de banda aumenta em uma quantidade proporcional à quantidade de perda de pacotes. Se as condições melhorarem posteriormente, o codificador gráfico Citrix retorna perfeitamente. Os limites podem ser configurados via política, sendo os padrões 300 ms de latência e 5% de perda de pacotes.

O Citrix Workspace™ app para Windows 2311 é atualmente suportado. O suporte para outras plataformas será adicionado em versões futuras do Citrix Workspace app. Assim como nas versões anteriores desse recurso, o HDX™ Adaptive Transport (EDT) deve estar habilitado para que esse recurso funcione. Além disso, se a conexão for feita via Citrix Gateway Service, o modo tolerante a perdas para gráficos também deve ser habilitado no Gateway.

Framehawk

> **Importante:**

> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais suportado. Em vez disso, use Thinwire com o transporte adaptável ativado.

> Framehawk é uma tecnologia especializada de acesso remoto de exibição para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE) sujeitas a alta perda de pacotes. O Framehawk supera os desafios de interferência espectral e propagação por múltiplos caminhos. O Framehawk oferece uma experiência de usuário fluida e interativa para usuários de aplicativos e desktops virtuais em dispositivos móveis Windows e iOS, como laptops e tablets. Para maximizar a escalabilidade do servidor e minimizar o consumo de largura de banda da rede, recomendamos usar o Framehawk apenas para o caso de uso específico descrito acima. Recomendamos o transporte

> adaptável, que incorpora muitos conceitos do Framehawk para maximizar o rendimento dos dados, para todos os outros casos de uso.

Você pode usar os modelos de política do Citrix® para implementar o Framehawk para um conjunto de usuários e cenários de acesso de uma forma que seja apropriada para sua organização. O Framehawk visa casos de uso móveis de tela única, como laptops e tablets. Use o Framehawk onde o valor comercial do desempenho interativo em tempo real justifica o custo extra em recursos do servidor e a necessidade de uma conexão de banda larga.

Como o Framehawk mantém uma experiência de usuário fluida

Pense no Framehawk como uma implementação de software do olho humano, observando o que está no buffer de quadros e discernindo os diferentes tipos de conteúdo na tela. O que é importante para o usuário? Quando áreas da tela estão mudando rapidamente, como vídeo ou gráficos em movimento, não importa para o olho humano se alguns pixels são perdidos. Essas áreas são rapidamente sobrescritas com novos dados.

Mas quando se trata de áreas estáticas da tela, o olho humano é exigente. Por exemplo, os ícones na área de notificação ou uma barra de ferramentas, ou texto depois de rolar para onde o usuário deseja começar a ler. Um usuário espera que essas áreas sejam perfeitas em pixels. Ao contrário dos protocolos que visam ser tecnicamente precisos de uma perspectiva de **uns e zeros**, o Framehawk visa ser relevante para o ser humano que está usando a tecnologia.

O Framehawk inclui um amplificador de sinal de Qualidade de Serviço de próxima geração, além de um mapa de calor baseado em tempo para uma identificação mais granular e eficiente das cargas de trabalho. Ele usa transformações autônomas e de autocorreção, além da compressão de dados, e evita a retransmissão de dados para manter a resposta ao clique, a linearidade e uma cadência consistente. Em uma conexão de rede com perdas, o Framehawk pode ocultar a perda com interpolação, e o usuário ainda percebe uma boa qualidade de imagem enquanto desfruta de uma experiência mais fluida. Além disso, os algoritmos do Framehawk distinguem inteligentemente entre diferentes tipos de perda de pacotes. Por exemplo, perda aleatória (envie mais dados para compensar) versus perda por congestionamento (não envie mais dados porque o canal já está congestionado).

O Framehawk Intent Engine no aplicativo Citrix Workspace™ distingue entre rolar para cima ou para baixo, aplicar zoom, mover para a esquerda ou para a direita, ler, digitar e outras ações comuns. O mecanismo também gerencia a comunicação de volta para o Virtual Delivery Agent (VDA) usando um dicionário compartilhado. Se o usuário estiver tentando ler, a qualidade visual do texto deve ser excelente. Se o usuário estiver rolando, deve ser rápido e suave. E tem que ser

interrompível, para que o usuário esteja sempre no controle da interação com o aplicativo ou desktop.

Ao medir a cadência na conexão de rede (**engrenagem**, análoga à tensão em uma corrente de bicicleta), a lógica do Framehawk reage mais rapidamente, proporcionando uma experiência superior em conexões de alta latência. Este sistema de engrenagem exclusivo e patenteado fornece feedback constante e atualizado sobre as condições da rede, permitindo que o Framehawk reaja imediatamente a mudanças na largura de banda, latência e perda.

Considerações de design usando Thinwire e Framehawk

O Framehawk usa uma camada de transporte de dados construída sobre o (User Datagram Protocol (UDP). O UDP é uma pequena parte de como o Framehawk supera a perda de dados, como você pode ver ao comparar o desempenho do Framehawk com outros protocolos baseados em UDP. O UDP fornece uma base importante para as técnicas centradas no ser humano que diferenciam o Framehawk.

Quanta largura de banda o Framehawk exige?

O significado de banda larga sem fio depende de vários fatores, incluindo quantos usuários estão compartilhando a conexão, a qualidade da conexão e os aplicativos em uso. Para um desempenho ideal, a Citrix sugere uma base de 4 Mbps ou 5 Mbps mais cerca de 150 Kbps por usuário simultâneo.

Nossa recomendação de largura de banda para Thinwire é geralmente uma base de 1,5 Mbps mais 150 Kbps por usuário. Para obter detalhes, consulte o blog de largura de banda do Citrix Virtual Apps and Desktops). Com 3% de perda de pacotes, você descobrirá que o Thinwire sobre TCP precisa de muito mais largura de banda do que o Framehawk para manter uma experiência de usuário positiva.

Thinwire permanece o canal principal de acesso remoto de exibição no protocolo ICA®. O Framehawk é desabilitado por padrão. A Citrix recomenda habilitá-lo seletivamente para atender aos cenários de acesso sem fio de banda larga em sua organização. Lembre-se de que o Framehawk exige consideravelmente mais recursos de servidor (CPU e memória) do que o Thinwire.

Requisitos e considerações

O Framehawk exige VDA 7.6.300 e Gerenciamento de Política de Grupo 7.6.300, no mínimo.

O endpoint deve ter, no mínimo, o Workspace app para Windows 1808, ou Citrix Receiver para Windows 4.3.100, Workspace app para iOS 1808, ou Citrix Receiver para iOS 6.0.1.

Por padrão, o Framehawk usa um intervalo de portas bidirecional do User Datagram Protocol (UDP) (3224 a 3324) para trocar dados do canal de exibição do Framehawk com o aplicativo Citrix Workspace. O intervalo pode ser personalizado em uma configuração de política chamada **Framehawk display channel port range**. Cada conexão simultânea entre o cliente e o desktop virtual requer uma porta exclusiva. Para ambientes de SO multiusuário, como servidores Citrix Virtual Apps™, defina portas suficientes para suportar o número máximo de sessões de usuário simultâneas. Para um SO de usuário único, como desktops VDI, é suficiente definir uma única porta UDP. O Framehawk tenta usar a primeira porta definida, trabalhando até a porta final especificada no intervalo. Isso se aplica tanto ao passar pelo Citrix Gateway quanto às conexões internas diretamente para o servidor StoreFront.

Para acesso remoto, um Citrix Gateway deve ser implantado. Por padrão, o Citrix Gateway usa a porta UDP 443 para comunicação criptografada entre o aplicativo Citrix Workspace do cliente e o Gateway. Essa porta deve estar aberta em quaisquer firewalls externos para permitir comunicação segura em ambas as direções. O recurso é conhecido como Datagram Transport Security (DTLS).

> **Observação:**
>
> As conexões Framehawk/DTLS não são suportadas em dispositivos FIPS.
>
> As conexões Framehawk criptografadas são suportadas, a partir do NetScaler Gateway versão 11.0.62 e NetScaler Unified Gateway versão 11.0.64.34 ou posterior.

A alta disponibilidade do NetScaler é suportada a partir do XenApp e XenDesktop 7.12.

Considere as seguintes recomendações antes de implementar o Framehawk:

- Entre em contato com o administrador de segurança para confirmar se as portas UDP definidas para o Framehawk estão abertas no firewall. O processo de instalação não configura automaticamente o firewall.
- Frequentemente, o Citrix Gateway pode ser instalado na DMZ, ladeado por firewalls nos lados externo e interno. Certifique-se de que a porta UDP 443 esteja aberta no firewall externo. Certifique-se de que as portas UDP 3224 a 3324 estejam abertas no firewall interno se o ambiente estiver usando os intervalos de portas padrão.

Configuração

> **Cuidado:**
>
> A Citrix recomenda que você habilite o Framehawk apenas para usuários que provavelmente experimentarão alta perda de pacotes. Também recomendamos que você não habilite o Framehawk como uma política universal para todos os objetos no Site.

> O Framehawk é desabilitado por padrão. Quando habilitado, o servidor tenta usar o Framehawk para gráficos e entrada do usuário. Se os pré-requisitos não forem atendidos por qualquer motivo, a conexão será estabelecida usando o modo padrão (Thinwire).

As seguintes configurações de política afetam o Framehawk:

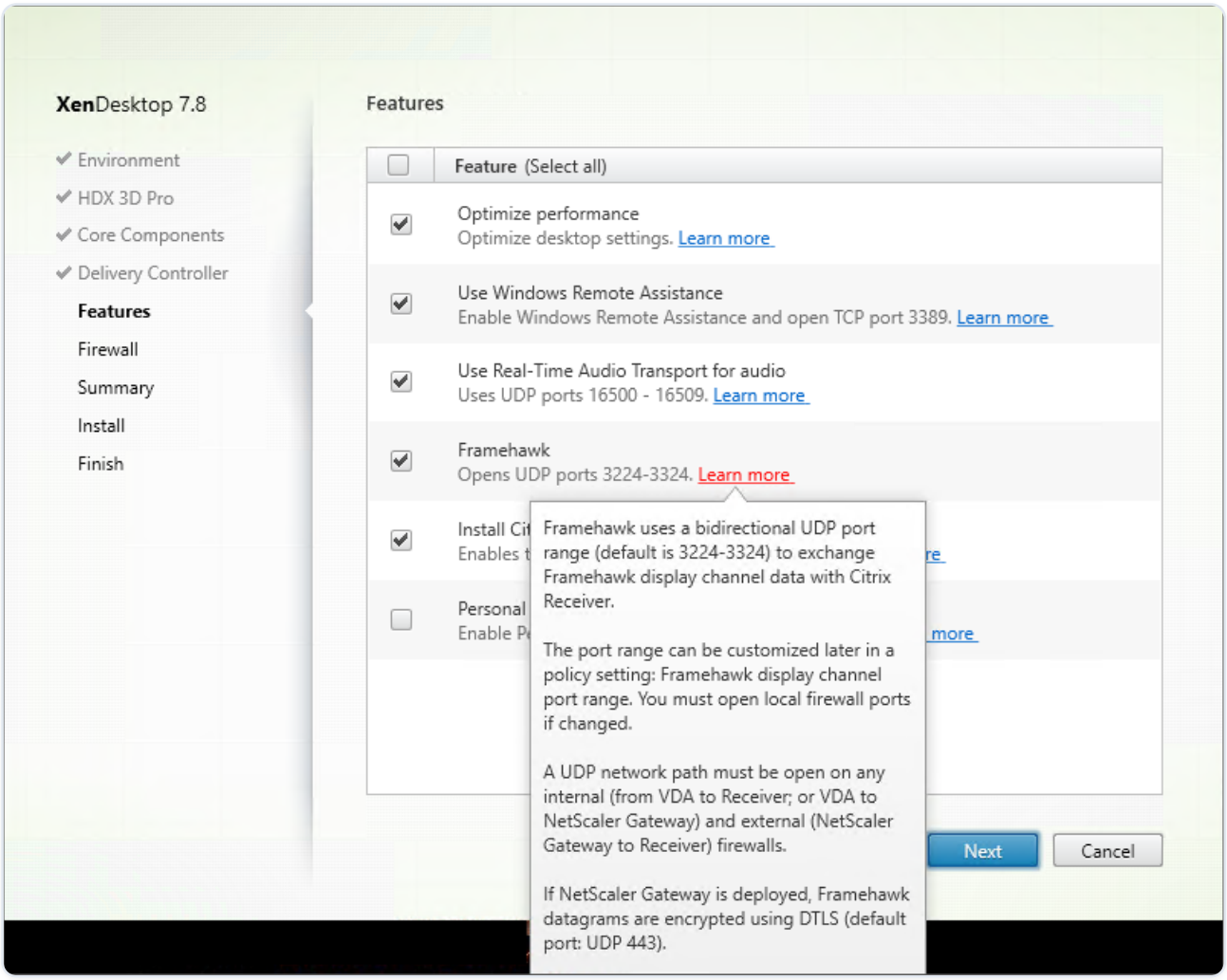
- Canal de exibição Framehawk: Habilita ou desabilita o recurso.
- Intervalo de portas do canal de exibição Framehawk: Especifica o intervalo de números de porta UDP (do menor ao maior número de porta) que o VDA usa para trocar dados do canal de exibição Framehawk com o dispositivo do usuário. O VDA tenta usar cada porta, começando pelo menor número de porta e incrementando a cada tentativa subsequente. A porta lida com o tráfego de entrada e saída.

Abrindo portas para o canal de exibição Framehawk

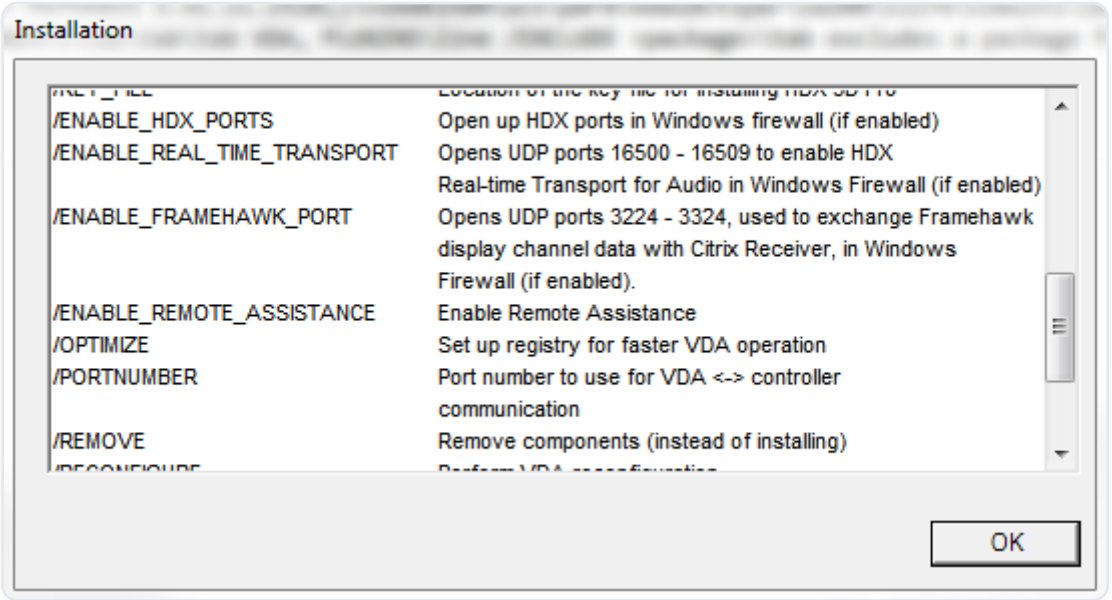
A partir do XenApp e XenDesktop 7.8, uma opção está disponível para reconfigurar o Firewall durante a etapa de **Recursos** do instalador do VDA. Esta caixa de seleção abre as portas UDP 3224 a 3324 no Firewall do Windows, se selecionada. A configuração manual do Firewall é necessária em algumas circunstâncias:

- Para quaisquer Firewalls de rede. Ou
- O intervalo de portas padrão é personalizado.

Para abrir essas portas UDP, selecione a caixa de seleção **Framehawk**:

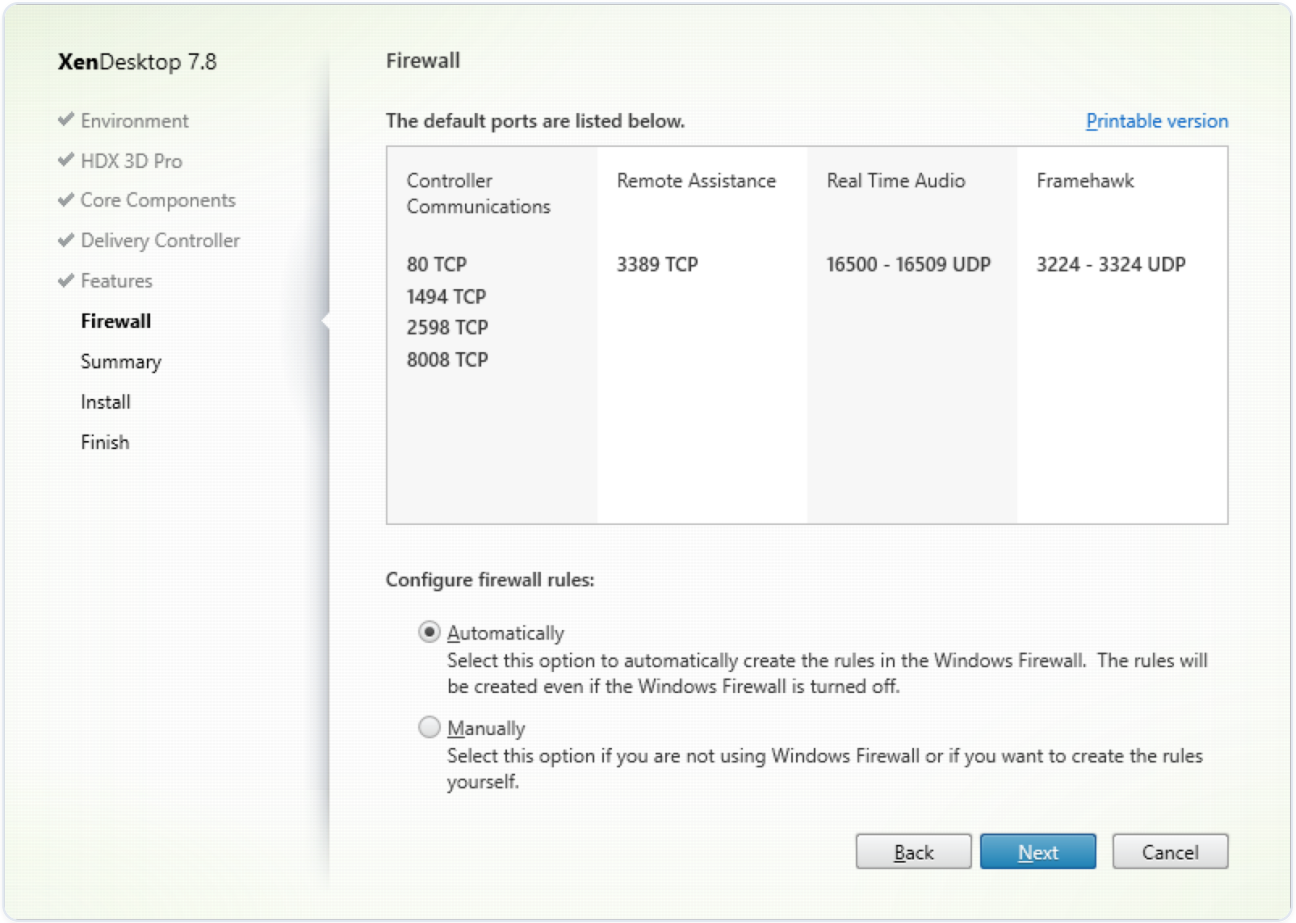


Você também pode usar a linha de comando para abrir portas UDP para Framehawk usando */* **ENABLE_FRAMEHAWK_PORT**:

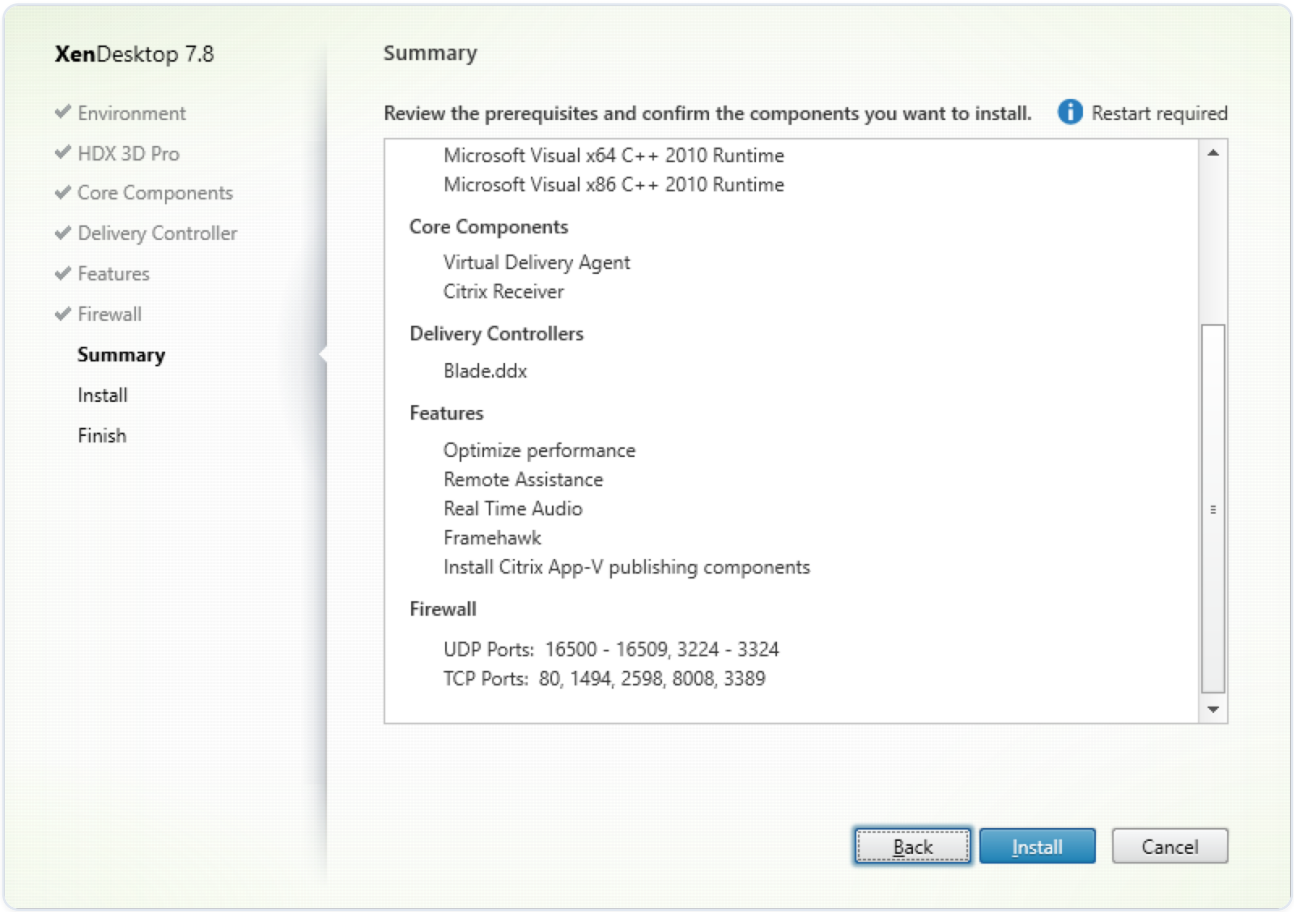


Verificando atribuições de porta UDP do Framehawk

Durante a instalação, você pode verificar as portas UDP atribuídas ao Framehawk na tela **Firewall**:



A tela de **Resumo** indica se o recurso Framehawk está habilitado:



Suporte do Citrix Gateway para Framehawk

O tráfego Framehawk criptografado é compatível com o Citrix Gateway 1808 ou posterior e NetScaler Gateway 11.0.62.10 ou posterior, e Citrix Unified Gateway 1808 e NetScaler Unified Gateway 11.0.64.34 ou posterior.

- Citrix Gateway refere-se à arquitetura de implantação onde o servidor virtual VPN do Gateway é diretamente acessível a partir do dispositivo do usuário final. Ou seja, o servidor virtual VPN tem um endereço IP público atribuído e o usuário se conecta diretamente a este endereço IP.
- Citrix Gateway com Unified Gateway refere-se à implantação onde o servidor virtual VPN do Gateway é vinculado como um destino ao servidor virtual de Comutação de Conteúdo (CS). Nesta implantação, o servidor virtual CS tem o endereço de protocolo de internet público e o servidor virtual VPN do Gateway tem um endereço de protocolo de internet fictício.

Para habilitar o suporte Framehawk no Citrix Gateway, o parâmetro DTLS no nível do servidor virtual VPN do Gateway deve ser habilitado. Depois que o parâmetro é habilitado e os componentes no Citrix Virtual Apps ou Citrix Virtual Desktops™ são atualizados corretamente, o tráfego de áudio, vídeo e interativo do Framehawk é criptografado entre o servidor virtual VPN do Gateway e o dispositivo do usuário.

Citrix Gateway, Unified Gateway e Citrix Gateway + balanceamento de carga de servidor global são compatíveis com Framehawk.

Os seguintes cenários não são compatíveis com Framehawk:

- HDX™ Insight
- Citrix Gateway no modo IPv6
- Citrix Gateway Double Hop
- Citrix Gateway com configuração de Cluster

CENÁRIO	SUPORTE FRAMEHAWK
Citrix Gateway	Sim
Citrix Gateway + balanceamento de carga de servidor global	Sim
Citrix Gateway com Unified Gateway	Sim. **Nota:** A versão 11.0.64.34 ou posterior do Unified Gateway é compatível.
HDX Insight	Não
Citrix Gateway no modo IPv6	Não
Citrix Gateway Double Hop	Não
Múltiplas Secure Ticket Authority no Citrix Gateway	Sim
Citrix Gateway e Alta Disponibilidade	Sim
Citrix Gateway e configuração de Cluster	Não

Configurando o Citrix Gateway para suporte Framehawk

Para habilitar o suporte Framehawk no Citrix Gateway, habilite o parâmetro DTLS no nível do *servidor virtual* VPN do Gateway. Depois que o parâmetro é habilitado e os componentes no Citrix Virtual Apps and Desktops™ são atualizados corretamente, o tráfego de áudio, vídeo e interativo do Framehawk é criptografado entre o servidor virtual VPN do Gateway e o dispositivo do usuário.

Essa configuração é necessária se você estiver habilitando a criptografia UDP no Citrix Gateway para acesso remoto.

Ao configurar o Citrix Gateway para suporte Framehawk:

- Certifique-se de que a porta UDP 443 esteja aberta em quaisquer firewalls externos
- Certifique-se de que a porta CGP (padrão 2598) esteja aberta em quaisquer firewalls externos
- Habilite o DTLS nas configurações do servidor virtual VPN
- Desvincule e revincule o par de certificados e chaves SSL. Esta etapa não é necessária se você estiver usando o Citrix Gateway 1808 ou posterior ou o NetScaler versão 11.0.64.34 ou posterior.

Para configurar o Citrix Gateway para suporte Framehawk:

1. Implante e configure o Citrix Gateway para se comunicar com o StoreFront™ e autenticar usuários para Citrix Virtual Apps and Desktops.
2. Na guia Configuração do Citrix Gateway, expanda Citrix Gateway e selecione **Virtual Servers**.
3. Escolha **Editar** para exibir as Configurações Básicas para o Servidor Virtual VPN; verifique o estado da configuração DTLS.
4. Escolha **Mais** para exibir mais opções de configuração:
5. Escolha **DTLS** para fornecer segurança de comunicação para protocolos de datagrama como o Framehawk. Clique em **OK**. A área de Configurações Básicas para o Servidor Virtual VPN mostra que o sinalizador DTLS está definido como **True**.
6. Reabra a tela de Vinculação de Certificado do Servidor e clique em **+** para vincular o par de chaves do certificado.
7. Escolha o par de chaves do certificado anterior, clique em **Selecionar**.
8. Salve as alterações na vinculação do certificado do servidor.
9. Após salvar, o par de chaves do certificado aparece. Clique em **Vincular**.
10. Ignore a mensagem de aviso **Nenhum cifra utilizável configurada no vserver/serviço SSL**, se ela aparecer.

Etapas para versões mais antigas do NetScaler® Gateway

Se você estiver usando uma versão do NetScaler Gateway anterior a 11.0.64.34:

1. Reabra a tela de Vinculação de Certificado do Servidor e clique em + para vincular o par de chaves do certificado.
2. Escolha o par de chaves do certificado anterior, clique em **Selecionar**.
3. Salve as alterações na vinculação do certificado do servidor.

4. Após salvar, o par de chaves do certificado aparece. Clique em **Vincular**.
5. Ignore a mensagem de aviso **Nenhum cifra utilizável configurada no vserver/serviço SSL**, se ela aparecer.

Para configurar o Unified Gateway para suporte ao Framehawk:

1. Certifique-se de que o Unified Gateway esteja instalado e configurado corretamente. Para obter informações adicionais, consulte as informações sobre Unified Gateway no site de Documentação de Produtos Citrix.
2. Habilite o parâmetro DTLS no *servidor virtual* VPN, que está vinculado ao *servidor virtual* CS como *servidor virtual* de destino.

Limitações

Se houver entradas DNS obsoletas para o servidor virtual do Citrix Gateway no dispositivo cliente, o transporte adaptável e o Framehawk podem retornar ao transporte TCP em vez do transporte UDP. Se ocorrer o retorno ao transporte TCP, limpe o cache DNS no cliente e reconecte para estabelecer a sessão usando o transporte UDP.

O Framehawk não oferece suporte a cursores de mouse de 32 bits, como os encontrados em aplicativos como o PTC Creo.

O Framehawk foi projetado para dispositivos móveis, como laptops e tablets, usando um único monitor, e retorna ao Thinwire em uma configuração de monitor duplo/múltiplo.

Suporte para outros produtos VPN

O Citrix Gateway é o único produto SSL VPN a oferecer suporte à criptografia UDP exigida pelo Framehawk. Se outro SSL VPN ou uma versão incorreta do Citrix Gateway for usado, a política do Framehawk poderá falhar ao ser aplicada. Os produtos VPN IPsec tradicionais suportam o Framehawk sem modificações.

Monitorando o Framehawk

Você pode monitorar o uso e o desempenho do Framehawk a partir do Citrix Director. A exibição Detalhes do Canal Virtual HDX contém informações úteis para solucionar problemas e monitorar o Framehawk em qualquer sessão. Para visualizar métricas relacionadas ao Framehawk, selecione **Gráficos-Framehawk**.

Se a conexão Framehawk for estabelecida, você verá **Provider = VD3D** e **Connected = True** na página de detalhes. É normal que o estado do canal virtual esteja ocioso, pois ele monitora o

canal de sinalização, que é usado apenas durante o handshake inicial. Esta página também fornece outras estatísticas úteis sobre a conexão.

Se você encontrar problemas, consulte o blog de solução de problemas do Framehawk.

Multimídia

A pilha de tecnologia HDX™ oferece suporte à entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia com renderização no lado do servidor
- Redirecionamento de multimídia com renderização no lado do cliente

Essa estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, enquanto maximiza a escalabilidade do servidor para reduzir o custo por usuário.

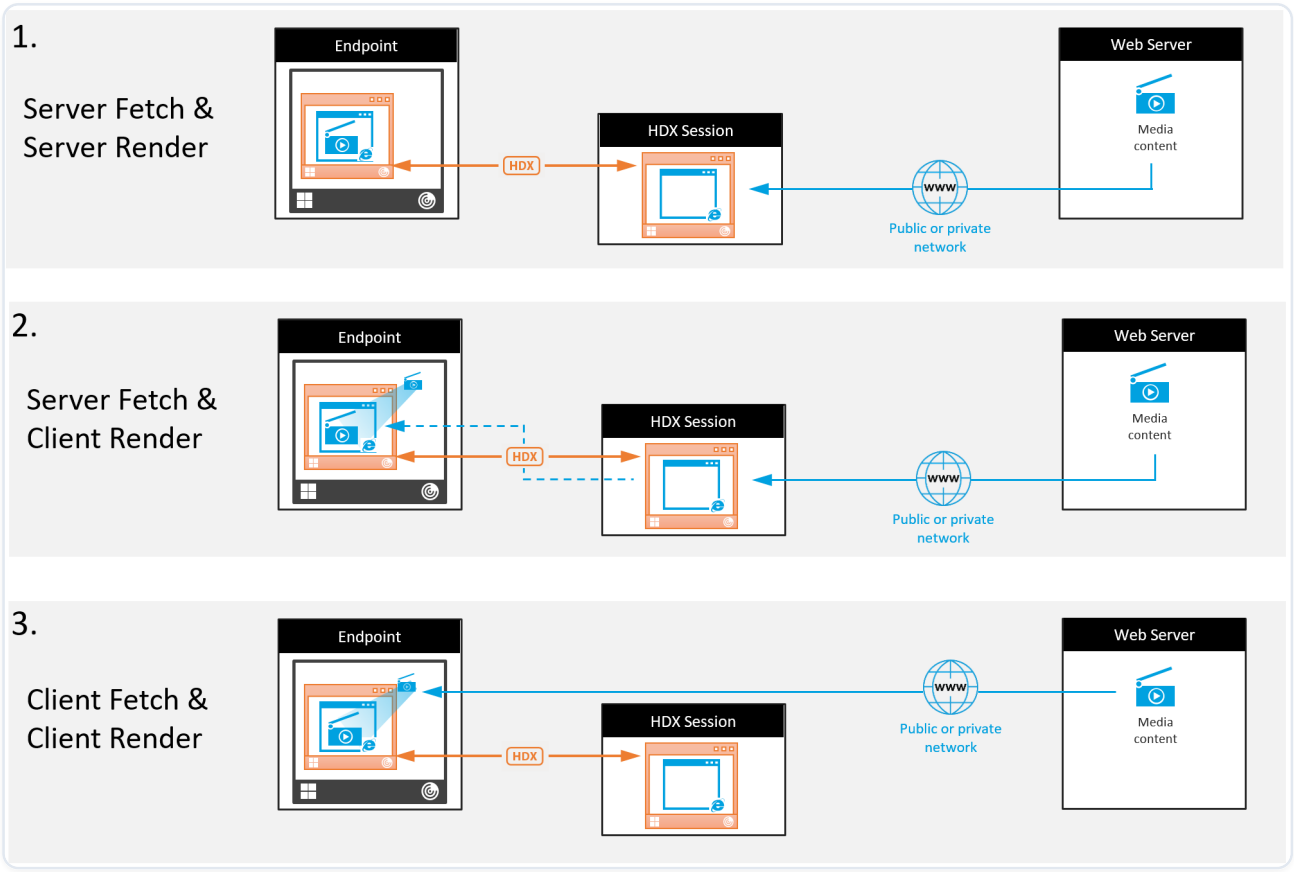
Com a entrega de multimídia renderizada no servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor Citrix Virtual Apps and Desktops pelo aplicativo. O conteúdo é então compactado e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo exige muitos recursos computacionais, a entrega de multimídia renderizada no servidor se beneficia muito da aceleração de hardware integrada. Por exemplo, o suporte para DirectX Video Acceleration (DXVA) desafoga a CPU ao realizar a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

Como a maioria dos servidores não oferece nenhuma aceleração de hardware para compactação de vídeo, a escalabilidade do servidor é negativamente impactada se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter alta escalabilidade do servidor, redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

- O redirecionamento do Windows Media desafoga o servidor para uma ampla variedade de formatos de mídia tipicamente associados ao Windows Media Player.
- O vídeo HTML5 tornou-se popular, e a Citrix® introduziu uma tecnologia de redirecionamento para esse tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento de contato, redirecionamento Host-to-client e Acesso a Aplicativos Locais, ao conteúdo multimídia.

Juntando essas tecnologias, se você não configurar o redirecionamento, o HDX fará a Renderização no Lado do Servidor. Se você configurar o redirecionamento, o HDX usará a Busca no Servidor e Renderização no Cliente ou a Busca no Cliente e Renderização no Cliente. Se esses métodos falharem, o HDX retornará à Renderização no Lado do Servidor conforme necessário e estará sujeito à Política de Prevenção de Fallback.

Cenários de exemplo



Cenário 1. (Busca no Servidor e Renderização no Servidor):

1. O servidor busca o arquivo de mídia de sua origem, decodifica e, em seguida, apresenta o conteúdo a um dispositivo de áudio ou dispositivo de exibição.
2. O servidor extrai a imagem ou som apresentados do dispositivo de exibição ou dispositivo de áudio, respectivamente.
3. O servidor opcionalmente o compacta e, em seguida, o transmite para o cliente.

Essa abordagem acarreta um alto custo de CPU, alto custo de largura de banda (se a imagem/som extraído não for compactado de forma eficiente) e tem baixa escalabilidade do servidor.

Os canais virtuais Thinwire e Áudio manipular essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para os clientes. Usando essa abordagem, a

decodificação acontece no servidor e funciona para uma variedade maior de dispositivos e formatos.

Cenário 2. (Busca pelo Servidor e Renderização pelo Cliente):

Essa abordagem depende da capacidade de interceptar o conteúdo de mídia antes que ele seja decodificado e apresentado ao dispositivo de áudio ou exibição. O conteúdo de áudio/vídeo compactado é enviado ao cliente, onde é então decodificado e apresentado localmente. A vantagem dessa abordagem é que o processamento é descarregado para os dispositivos cliente, economizando ciclos de CPU no servidor.

No entanto, também introduz alguns requisitos adicionais de hardware e software para o cliente. O cliente deve ser capaz de decodificar cada formato que possa receber.

Cenário 3. (Busca pelo Cliente e Renderização pelo Cliente):

Essa abordagem depende da capacidade de interceptar a URL do conteúdo de mídia antes que ela seja buscada da origem. A URL é enviada ao cliente, onde o conteúdo de mídia é buscado, decodificado e apresentado localmente. Essa abordagem é conceitualmente simples. Sua vantagem é que ela economiza ciclos de CPU no servidor e largura de banda, pois o servidor envia apenas comandos de controle. No entanto, o conteúdo de mídia nem sempre está acessível aos clientes.

Estrutura e plataforma:

Sistemas operacionais de sessão única (Windows, Mac OS X e Linux) fornecem estruturas multimídia que permitem o desenvolvimento mais rápido de aplicativos multimídia. Esta tabela lista algumas das estruturas multimídia mais populares. Cada estrutura divide o processamento de mídia em várias etapas e usa uma arquitetura baseada em pipeline.

ESTRUTURA	PLATAFORMA
DirectShow	Windows (98 e posterior)
Media Foundation	Windows (Vista e posterior)
Gstreamer	Linux
Quicktime	Mac OS X

Suporte a salto duplo com tecnologias de redirecionamento de mídia

Redirecionamento de áudio	Não
Redirecionamento de conteúdo do navegador	Não
Redirecionamento de webcam HDX	Sim
Redirecionamento de vídeo HTML5	Sim
Redirecionamento de mídia do Windows	Sim

Recursos de áudio

Você pode configurar e adicionar as seguintes configurações de política do Citrix a uma política que otimiza os recursos de áudio HDX. Para detalhes de uso, além de relacionamentos e dependências com outras configurações de política, consulte Configurações de política de áudio, Configurações de política de largura de banda e Configurações de política de conexões multi-stream.

Áudio adaptável

Com o áudio adaptável, você não precisa configurar manualmente as políticas de qualidade de áudio no VDA. O áudio adaptável otimiza as configurações para o seu ambiente e substitui formatos de compressão de áudio obsoletos para proporcionar uma excelente experiência do usuário.

O áudio adaptável é habilitado por padrão. Para desabilitar o áudio adaptável, consulte Configurações de política de áudio.

> **Importante:**
>
> A Citrix® recomenda a entrega de áudio usando o User Datagram Protocol (UDP) em vez de TCP quando aplicativos de áudio em tempo real são necessários. As seguintes opções de transporte de áudio estão disponíveis via UDP:
>
> - Áudio via UDP

- Transporte Adaptável HDX™ (Enlightened Data Transport)

A criptografia de áudio UDP usando DTLS está disponível apenas entre o Citrix Gateway e o aplicativo Citrix Workspace™. Portanto, às vezes pode ser preferível usar o transporte TCP. O TCP oferece suporte à criptografia TLS de ponta a ponta do VDA para o aplicativo Citrix Workspace.

Para obter mais informações sobre áudio adaptável e áudio UDP, consulte Transporte em tempo real de áudio via UDP e intervalo de portas UDP de áudio.

Modo tolerante a perdas para áudio

O modo tolerante a perdas suporta áudio. Este recurso aumenta a experiência do usuário para streaming em tempo real e melhora a qualidade do áudio via EDT quando os usuários estão se conectando através de redes com alta latência e perda de pacotes. Este recurso é desabilitado por padrão.

Observação:

Ambas as políticas de **Transporte Adaptável HDX (EDT)** e **modo tolerante a perdas para áudio** devem ser habilitadas para que este recurso funcione.

Requisitos do sistema

Certifique-se de que os seguintes produtos estejam nas versões mínimas que suportam o modo tolerante a perdas:

- Citrix Virtual Delivery Agent (VDA) 2308
- Aplicativo Citrix Workspace para Windows 2309

Além disso, os seguintes recursos devem ser habilitados:

- Política de Transporte Adaptável HDX.
- (Opcional) Para conexões remotas, Citrix Gateway Service é necessário.

Observação:

> Se as condições acima não forem atendidas, o áudio é enviado através do transporte confiável EDT.

Informações adicionais

O modo tolerante a perdas é um protocolo de transporte tolerante a perdas que permite a perda de pacotes na transmissão sem reenviar conteúdo multimídia, resultando em uma experiência mais em tempo real para os usuários.

O Enlightened Data Transport (EDT) é um protocolo de transporte proprietário da Citrix que oferece uma experiência de usuário superior em conexões de longa distância desafiadoras, mantendo a escalabilidade do servidor. O modo tolerante a perdas é um recurso do serviço Citrix Gateway que usa o modo tolerante a perdas como protocolo de transporte para manter uma conexão estável mesmo diante do congestionamento da rede. Isso garante uma experiência consistente e estável para trabalhadores remotos. Em condições normais, tanto o EDT quanto o modo tolerante a perdas fornecem resultados semelhantes. No entanto, em condições de rede com perda de pacotes, o modo tolerante a perdas oferece uma experiência de áudio melhor em comparação com o EDT. Isso o torna um recurso essencial para trabalhadores remotos que dependem de multimídia em tempo real para o seu trabalho.

Qualidade do áudio

Em geral, uma qualidade de som mais alta consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para os dispositivos do usuário. A compressão de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações de política do Citrix para configurar os níveis de compressão a serem aplicados aos arquivos de som.

Por padrão, a configuração da política de **Qualidade de áudio** é definida como Alta - áudio de alta definição quando o transporte TCP é usado. A política é definida como Média - otimizada para fala quando o transporte UDP (recomendado) é usado. A configuração de **Áudio de alta definição** fornece áudio estéreo de alta fidelidade, mas consome mais largura de banda do que outras configurações de qualidade. Não use esta qualidade de áudio para aplicativos de bate-papo por voz ou vídeo não otimizados (como softphones). O motivo é que isso pode introduzir latência no caminho do áudio, o que não é adequado para comunicações em tempo real. Recomendamos a configuração de política otimizada para fala para áudio em tempo real, independentemente do protocolo de transporte selecionado.

Quando a largura de banda é limitada, por exemplo, conexões via satélite ou discadas, reduzir a qualidade do áudio para **Baixa** consome a menor largura de banda possível. Nesta situação, crie políticas separadas para usuários em conexões de baixa largura de banda para que os usuários em conexões de alta largura de banda não sejam afetados negativamente.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Diretrizes de largura de banda para reprodução e gravação de áudio:

- Áudio adaptável (padrão)
  - Taxa de bits: adaptável variável
  - Número de canais: 2 (Estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 48000 Hz
  - Profundidade de bits: 16 bits
- Alta qualidade
  - Taxa de bits: ~100 kbps (mín. 75, máx. 175 kbps) para reprodução / ~70 kbps para captura de microfone
  - Número de Canais: 2 (Estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 44100 Hz
  - Profundidade de bits: 16 bits
- Qualidade média (recomendado para VoIP)
  - Taxa de bits: ~16 kbps (mín. 20, máx. 40 kbps) para reprodução, ~16 kbps para captura de microfone
  - Número de Canais: 1 (Mono) para reprodução e captura
  - Frequência: 16000 Hz (banda larga)
  - Profundidade de bits: 16 bits
- Qualidade baixa
  - Taxa de bits: ~ 11 kbps (mín. 10; máx. 25 kbps) para reprodução, ~11 kbps para captura de microfone
  - Número de Canais: 1 (Mono) para reprodução e captura
  - Frequência: 8000 Hz (banda estreita)

- Profundidade de bits: 16 bits

Redirecionamento de áudio do cliente

Para permitir que os usuários recebam áudio de um aplicativo em um servidor através de alto-falantes ou outros dispositivos de som no dispositivo do usuário, deixe a configuração de **Redirecionamento de áudio do cliente** como **Permitido**. Esta é a configuração padrão.

O mapeamento de áudio do cliente sobrecarrega os servidores e a rede. No entanto, proibir o redirecionamento de áudio do cliente desativa toda a funcionalidade de áudio HDX.

Para obter detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Redirecionamento de microfone do cliente

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Redirecionamento de microfone do cliente** em seu padrão (Permitido).

Por segurança, os dispositivos do usuário alertam seus usuários quando servidores em que não confiam tentam acessar microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar este alerta no aplicativo Citrix Workspace.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Plug N Play de áudio

A configuração de política Plug N Play de áudio permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração está **Habilitada** por padrão. O Plug N Play de áudio permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até depois do início da sessão do usuário.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Para obter detalhes da configuração, consulte Configurações de política de áudio.

Limite de largura de banda de redirecionamento de áudio e porcentagem de limite de largura de banda de redirecionamento de áudio

A configuração de política Limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para reprodução e gravação de áudio em uma sessão.

A configuração Porcentagem de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima para redirecionamento de áudio como uma porcentagem da largura de banda total disponível.

Por padrão, zero (sem máximo) é especificado para ambas as configurações. Se ambas as configurações forem configuradas, a que tiver o menor limite de largura de banda será usada.

Para obter detalhes da configuração, consulte Configurações de política de largura de banda. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre transporte em tempo real UDP e intervalo de porta UDP de áudio

Por padrão, o Áudio sobre Transporte em Tempo Real do Protocolo de Datagrama de Usuário (UDP) é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam Áudio sobre Transporte em Tempo Real UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar UDP/RTP para áudio para garantir a melhor experiência possível ao usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio UDP é preferível ao EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que nenhuma latência seja adicionada em conexões com alta perda de pacotes.

> **Importante:**

> Quando o Citrix Gateway não está no caminho, os dados de áudio transmitidos com UDP não são criptografados. Se o Citrix Gateway estiver configurado para acessar recursos do Citrix Virtual Apps and Desktops™, o tráfego de áudio entre o dispositivo de endpoint e o Citrix Gateway é protegido usando o protocolo DTLS.

> O intervalo de portas UDP de áudio especifica o intervalo de números de porta que o VDA do Windows usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é de 16500 a 16509.

> **Observação:**
>
> Se o Áudio sobre Transporte UDP em Tempo Real não for necessário para áudio adaptável, a Citrix recomenda configurar a política para Desativado. Isso ajuda a evitar que os clientes do aplicativo Citrix Workspace solicitem conexões UDP abertas ou acionem o aparecimento de janelas de diálogo de configuração de firewall do cliente do aplicativo Citrix Workspace indesejadas.

> Para obter detalhes de configuração sobre Áudio sobre UDP Real-time Transport, consulte Configurações de política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações de política de conexões multi-stream. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre UDP requer o VDA do Windows. Para políticas suportadas no VDA do Linux, consulte Lista de suporte de políticas.

Políticas de configuração de áudio para dispositivos de usuário

1. Carregue os modelos de política de grupo seguindo Configurando o modelo administrativo do Objeto de Política de Grupo.
2. No Editor de Política de Grupo, expanda **Modelos Administrativos > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Para **Configurações de áudio do cliente**, selecione **Não Configurado**, **Habilitado** ou **Desabilitado**.
   - **Não Configurado**. Por padrão, o Redirecionamento de Áudio é habilitado usando áudio de alta qualidade ou as configurações de áudio personalizadas configuradas anteriormente.
   - **Habilitado**. Habilita o redirecionamento de áudio usando as opções selecionadas.
   - **Desabilitado**. Desabilita o redirecionamento de áudio.
4. Se você selecionar **Habilitado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Habilitar Transporte em Tempo Real** e então defina o intervalo de portas de entrada a serem abertas no firewall local do Windows.

6. Para usar Áudio UDP com Citrix Gateway, selecione **Permitir Transporte em Tempo Real Através do gateway**. Configure o Citrix Gateway com DTLS. Para mais informações, consulte este artigo.

Como Administrador, se você não tiver controle sobre os dispositivos de endpoint para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o Áudio UDP. Por exemplo, para dispositivos pessoais ou computadores domésticos.

1. Na máquina StoreFront, abra C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica com um editor como o notepad.
2. Faça as seguintes entradas na seção .

   ; Este texto habilita o Transporte em Tempo Real

   EnableRtpAudio=true

   ; Este texto permite o Transporte em Tempo Real Através do gateway

   EnableUDPThroughGateway=true

   ; Este texto define a qualidade do áudio como Média

   AudioBandwidthLimit=1

   ; Intervalo de portas UDP

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Se você habilitar o áudio do User Datagram Protocol (UDP) editando default.ica, o áudio UDP será habilitado para todos os usuários que estiverem usando essa loja.

Evitar eco durante conferências multimídia

Usuários em conferências de áudio ou vídeo podem ouvir um eco. Ecos geralmente ocorrem quando alto-falantes e microfones estão muito próximos um do outro. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX oferece uma opção de cancelamento de eco (habilitada por padrão) que minimiza qualquer eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Certifique-se de que os dispositivos não estejam muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração de registro para desabilitar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados por meio do registro.

Softphones

Um softphone é um software que atua como uma interface de telefone. Você usa um softphone para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Ao usar um softphone, você pode discar números de telefone e realizar outras funções relacionadas ao telefone usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para a entrega de softphones.

- **Modo de controle**. O softphone hospedado controla um aparelho telefônico físico. Neste modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.
- **Suporte a softphone otimizado para HDX RealTime (recomendado)**. O mecanismo de mídia é executado no dispositivo do usuário, e o tráfego de Voz sobre Protocolo de Internet flui de ponto a ponto. Para exemplos, consulte:
  - Otimização HDX para Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone para VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings para VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin VDI do Zoom
  - Genesys PureEngage Cloud
  - Dispositivo de ditado Nuance Dragon PowerMic
- **Acesso a Aplicativos Locais**. Um recurso do Citrix Virtual Apps and Desktops que permite que um aplicativo, como um softphone, seja executado localmente no dispositivo de usuário Windows, mas apareça perfeitamente integrado ao seu desktop virtual/publicado. Este recurso descarrega todo o processamento de áudio para o dispositivo do usuário. Para obter mais informações, consulte Acesso a Aplicativos Locais e redirecionamento de URL.
- **Suporte genérico a softphone HDX RealTime.** Voz sobre Protocolo de Internet sobre ICA.

Suporte genérico a softphone

O suporte genérico a softphones permite hospedar um softphone não modificado no XenApp ou XenDesktop no data center. O tráfego de áudio passa pelo protocolo Citrix ICA (preferencialmente usando UDP/RTP) para o dispositivo do usuário executando o aplicativo Citrix Workspace.

O suporte genérico a softphone é um recurso do HDX RealTime. Essa abordagem para entrega de softphone é especialmente útil quando:

- Uma solução otimizada para entregar o softphone não está disponível e o usuário não está em um dispositivo Windows onde o Acesso a Aplicativos Locais possa ser usado.
- O mecanismo de mídia necessário para a entrega otimizada do softphone não está instalado no dispositivo do usuário ou não está disponível para a versão do sistema operacional em execução no dispositivo do usuário. Nesse cenário, o HDX RealTime Genérico fornece uma solução de fallback valiosa.

Existem duas considerações sobre a entrega de softphone usando Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é entregue ao desktop virtual/publicado.
- Como o áudio é entregue para e do headset, microfone e alto-falantes do usuário, ou conjunto de telefone USB.

Citrix Virtual Apps and Desktops incluem inúmeras tecnologias para suportar a entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida do áudio em tempo real e eficiência de largura de banda.
- Pilha de áudio de baixa latência.
- Buffer de jitter do lado do servidor para suavizar o áudio quando a latência da rede flutua.
- Marcação de pacotes (DSCP e WMM) para Qualidade de Serviço.
    - Marcação DSCP para pacotes RTP (Camada 3)
    - Marcação WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voz sobre Protocolo de Internet. O aplicativo Citrix Workspace para Windows oferece estes recursos:

- Buffer de jitter do lado do cliente - Garante áudio suave mesmo quando a latência da rede flutua.

- Cancelamento de eco - Permite maior variação na distância entre o microfone e os alto-falantes para trabalhadores que não usam fone de ouvido.
- Áudio plug-n-play - Dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.
- Roteamento de dispositivo de áudio - Os usuários podem direcionar o toque para os alto-falantes, mas o caminho de voz para o fone de ouvido.
- ICA multi-stream - Permite roteamento flexível baseado em Qualidade de Serviço pela rede.
- O ICA suporta quatro fluxos TCP e dois UDP. Um dos fluxos UDP suporta o áudio em tempo real sobre RTP.

Para um resumo dos recursos do aplicativo Citrix Workspace, consulte Matriz de Recursos do Citrix Receiver.

Recomendações de configuração do sistema

Hardware e Software do Cliente: Para uma qualidade de áudio ideal, recomendamos a versão mais recente do aplicativo Citrix Workspace e um fone de ouvido de boa qualidade que tenha cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac suportam Voz sobre Protocolo de Internet. Além disso, a Dell Wyse oferece suporte a Voz sobre Protocolo de Internet para ThinOS (WTOS).

Considerações sobre a CPU: Monitore o uso da CPU no VDA para determinar se é necessário atribuir duas CPUs virtuais a cada máquina virtual. Voz e vídeo em tempo real são intensivos em dados. A configuração de duas CPUs virtuais reduz a latência de troca de threads. Portanto, recomendamos que você configure duas vCPUs em um ambiente VDI do Citrix Virtual Desktops™.

Ter duas CPUs virtuais não significa necessariamente dobrar o número de CPUs físicas, pois as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de Confiabilidade da Sessão, também aumenta o consumo de CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo de CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor poderoso.

Áudio UDP: O áudio sobre UDP oferece excelente tolerância a congestionamento de rede e perda de pacotes. Recomendamos usá-lo em vez de TCP quando disponível.

Configuração de LAN/WAN: A configuração adequada da rede é fundamental para uma boa qualidade de áudio em tempo real. Normalmente, você deve configurar redes locais virtuais (VLANs) porque pacotes de broadcast excessivos podem introduzir jitter. Dispositivos habilitados para IPv6 podem gerar muitos pacotes de broadcast. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configure para suportar Qualidade de Serviço.

Configurações para uso de conexões WAN: Você pode usar bate-papo por voz em conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se estiver entregando softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler® SD-WAN entre o data center e o escritório remoto. Isso mantém uma alta Qualidade de Serviço. O NetScaler SD-WAN suporta ICA Multi-Stream, incluindo UDP. Além disso, para um único fluxo TCP, é possível distinguir as prioridades de vários canais virtuais ICA para garantir que os dados de áudio em tempo real de alta prioridade recebam tratamento preferencial.

Use o Director ou o HDX Monitor para validar sua configuração HDX.

Conexões de usuário remoto: O Citrix Gateway suporta DTLS para entregar tráfego UDP/RTP nativamente (sem encapsulamento em TCP). Abra os firewalls bidirecionalmente para tráfego UDP na Porta 443.

Seleção de codec e consumo de largura de banda: Entre o dispositivo do usuário e o VDA no data center, recomendamos usar a configuração de codec **Otimizado para Fala**, também conhecida como áudio de Qualidade Média. Entre a plataforma VDA e o IP-PBX, o softphone usa o codec configurado ou negociado. Por exemplo:

- G711 oferece boa qualidade de voz, mas tem um requisito de largura de banda de 80 kilobits por segundo a 100 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).
- G729 oferece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo a 40 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).

Entrega de aplicativos de softphone para o desktop virtual

Existem dois métodos pelos quais você pode entregar um softphone para o desktop virtual XenDesktop®:

- O aplicativo pode ser instalado na imagem do desktop virtual.

- O aplicativo pode ser transmitido por streaming para o desktop virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciamento porque a imagem do desktop virtual é mantida organizada. Após ser transmitido por streaming para o desktop virtual, o aplicativo é executado nesse ambiente como se tivesse sido instalado da maneira usual. Nem todos os aplicativos são compatíveis com o App-V.

Entrega de áudio para e do dispositivo do usuário

O HDX RealTime genérico suporta dois métodos de entrega de áudio para e do dispositivo do usuário:

- **Canal Virtual de Áudio Citrix**. Geralmente recomendamos o Canal Virtual de Áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB Genérico**. Suporta dispositivos de áudio com botões ou um display (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou similar à LAN de volta para o servidor Citrix Virtual Apps and Desktops.

Canal virtual de áudio Citrix

O Canal Virtual de Áudio Bidirecional Citrix (CTXCAM) permite que o áudio seja entregue de forma eficiente pela rede. O HDX RealTime Genérico pega o áudio do fone de ouvido ou microfone do usuário e o compacta. Em seguida, ele o envia via ICA para o aplicativo de softphone no desktop virtual. Da mesma forma, a saída de áudio do softphone é compactada e enviada na outra direção para o fone de ouvido ou alto-falantes do usuário. Essa compactação é independente da compactação usada pelo próprio softphone (como G.729 ou G.711). Ela é feita usando o codec Otimizado para Fala (Qualidade Média). Suas características são ideais para Voz sobre Protocolo de Internet. Ele apresenta tempo de codificação rápido e consome apenas aproximadamente 56 Kilobits por segundo de largura de banda de rede (28 Kbps em cada direção), no pico. Este codec deve ser explicitamente selecionado no console do Studio porque não é o codec de áudio padrão. O padrão é o codec de Áudio HD (Alta Qualidade). Este codec é excelente para trilhas sonoras estéreo de alta fidelidade, mas é mais lento para codificar em comparação com o codec Otimizado para Fala.

Redirecionamento USB Genérico

A tecnologia de Redirecionamento USB Genérico da Citrix (canal virtual CTXGUSB) fornece um meio genérico de acesso remoto a dispositivos USB, incluindo dispositivos compostos (áudio mais HID) e dispositivos USB isócronos. Essa abordagem é limitada a usuários conectados à LAN. A razão é que o protocolo USB tende a ser sensível à latência da rede e requer uma largura de banda considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones.

Este redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o Canal Virtual de Áudio Citrix é preferido porque é otimizado para tráfego de áudio. A principal exceção é quando você está usando um dispositivo de áudio com botões. Por exemplo, um telefone USB conectado ao dispositivo do usuário que está conectado à LAN do data center. Neste caso, o Redirecionamento USB Genérico suporta botões no aparelho telefônico ou headset que controlam recursos enviando um sinal de volta para o softphone. Não há problema com botões que funcionam localmente no dispositivo.

Ferramenta de linha de comando de diagnóstico de áudio

A ferramenta de linha de comando de diagnóstico de áudio no VDA pode ser usada para consultar dados de sessão relacionados a políticas de áudio, configuração e transporte de dados.

Uso

Abra um prompt de comando e execute `CtxAudio.exe` da pasta `C:\Program Files\Citrix\HDX\bin`.

- Executar a ferramenta como administrador exibe todas as informações de áudio das sessões ICA ativas.
- Executar a ferramenta como não administrador exibe as informações de áudio da sessão ICA do usuário atual.

Saída

A ferramenta exibe várias configurações que podem ajudar a diagnosticar problemas relacionados ao áudio em uma sessão.

SEÇÃO	DESCRIÇÃO
Informações da política	Políticas de áudio aplicadas à(s) sessão(ões) atual(is).
Informações de configurações	Configurações relacionadas ao áudio armazenadas no registro.
Informações de estado	Estado do áudio, versão, codecs e transporte aplicados à(s) sessão(ões) atual(is).
Informações dos dispositivos	Nomes dos dispositivos, suas funções e seus status usados na sessão.

Observação:

A saída varia dependendo se você executa a ferramenta em um VDA de múltiplas sessões (TS) ou em um VDA de sessão única (WSVDA).

Limitação

Você instala um dispositivo de áudio no seu cliente, habilita o redirecionamento de áudio e inicia uma sessão RDS. Os arquivos de áudio podem falhar ao reproduzir e uma mensagem de erro aparece.

Como solução alternativa, adicione a chave do registro na máquina RDS e, em seguida, reinicie a máquina. Para obter informações, consulte Limitação de áudio na lista de recursos gerenciados por meio do registro.

Redirecionamento de conteúdo do navegador

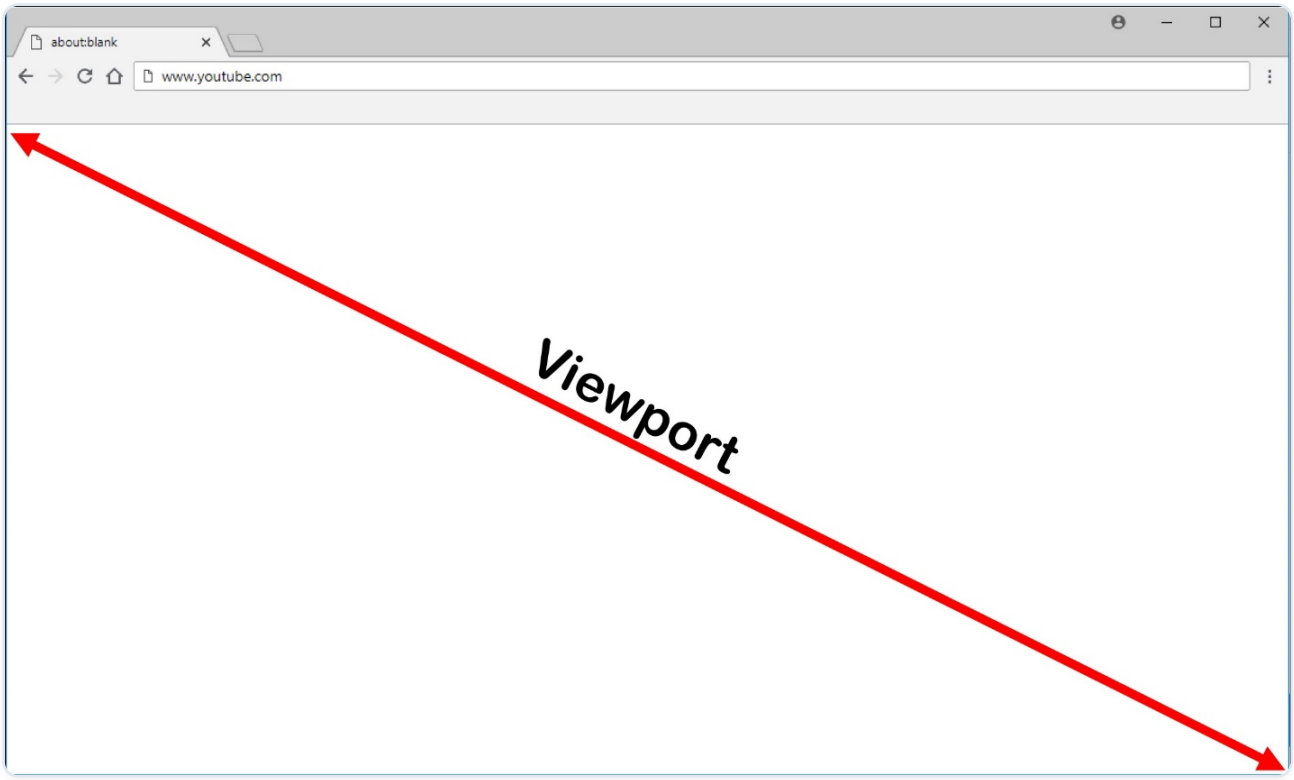
O redirecionamento de conteúdo do navegador impede a renderização de páginas da web na lista de permissões no lado do VDA. Esse recurso usa o Citrix Workspace™ app para Windows ou o Citrix Workspace app para Linux para instanciar um mecanismo de renderização correspondente no lado do cliente, que busca o conteúdo HTTP e HTTPS da URL.

Observação:

Você pode especificar que as páginas da web sejam redirecionadas para o lado do VDA (e não para o lado do cliente) usando uma lista de bloqueio.

Esse mecanismo de layout da web de sobreposição é executado no dispositivo de endpoint em vez de no VDA e usa a CPU, GPU, RAM e Rede do endpoint.

Apenas a área de visualização (viewport) do navegador é redirecionada. A área de visualização é a área retangular no seu navegador onde o conteúdo é exibido. A área de visualização não inclui itens como a Barra de Endereços, a Barra de Ferramentas de **Favoritos** ou a Barra de **Status**. Esses itens estão na interface do usuário, que ainda está sendo executada no navegador no VDA.



1. Configure uma política do Studio que especifique uma Lista de Controle de Acesso contendo as URLs na lista de permissões para redirecionamento ou a lista de bloqueio que desabilita o redirecionamento para caminhos de URL específicos. 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 bloqueio, uma extensão do navegador realiza a comparação. Para o Chrome, a extensão do navegador está disponível na Chrome Web Store, e você pode implantá-la usando Políticas de Grupo e arquivos ADMX. As extensões do Chrome são instaladas por usuário. A atualização de uma imagem dourada para adicionar ou remover uma extensão não é necessária. Para o Microsoft Edge, a extensão não está disponível diretamente. Você deve permitir extensões da Chrome Store para encontrá-la e instalá-la.
2. Se uma correspondência for encontrada na lista de permissões (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 Citrix Workspace app de que um redirecionamento é necessário e retransmite a URL. O Citrix Workspace app então instancia um mecanismo de renderização local e exibe o site.
3. O Citrix Workspace app então integra o site de volta à área de conteúdo do navegador da área de trabalho virtual de forma contínua.

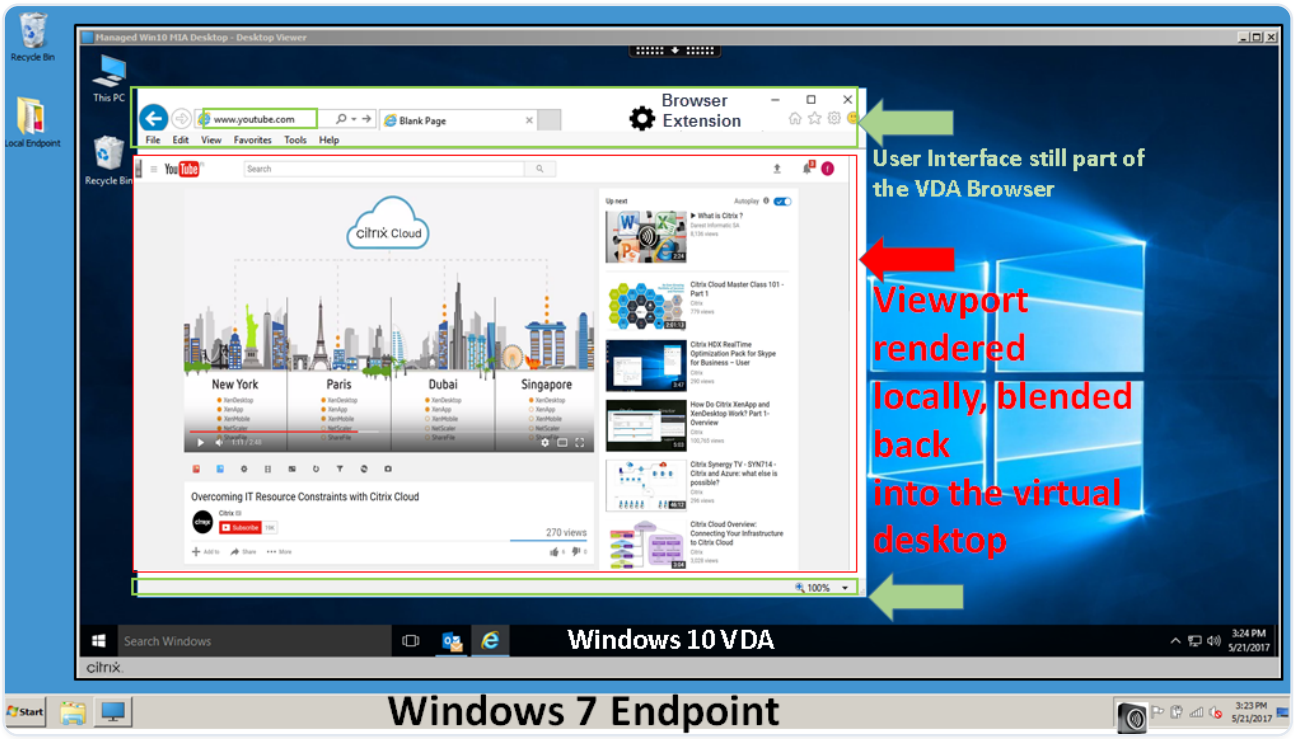
> **Observação:**

> Para obter mais informações sobre as novidades e correções para a extensão de redirecionamento de conteúdo do navegador, acesse a Chrome Web Store e pesquise por `citrix bcr` para encontrar a extensão.

> A cor do logotipo especifica o status da extensão do Chrome. É uma destas três cores:

- Verde: Ativo e conectado.
- Cinza: Não ativo/ocioso na guia atual.
- Vermelho: Quebrado/Não funcionando.

Você pode depurar o registro usando **Opções** no menu de extensões.



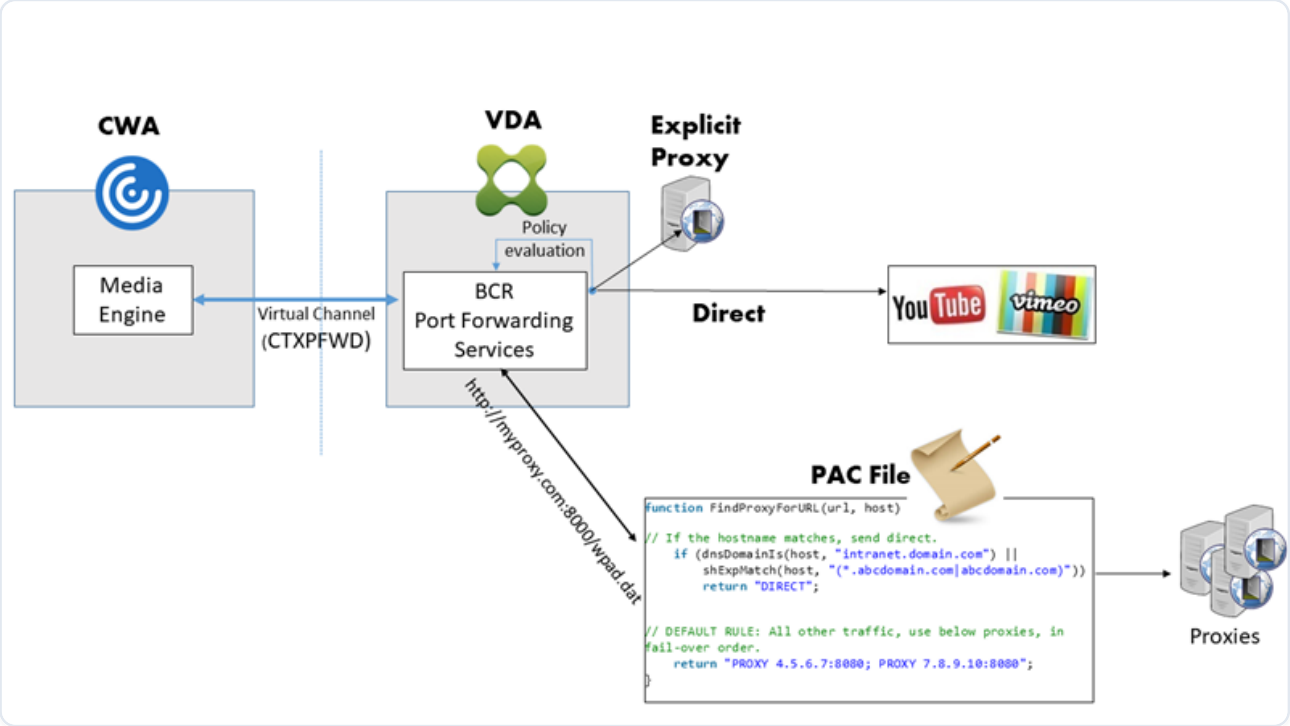
Aqui estão os cenários de como o aplicativo Citrix Workspace busca conteúdo:

- **Busca e renderização no servidor**: Não há redirecionamento porque você não adicionou o site à lista de permissões ou o redirecionamento falhou. Voltamos a renderizar a página da web no VDA e usamos o Thinwire para remover os gráficos. Use políticas para controlar o comportamento de fallback. Alto consumo de CPU, RAM e largura de banda no VDA.
- **Busca no servidor e renderização no cliente**: O aplicativo Citrix Workspace contata e busca conteúdo do servidor web através do VDA usando um canal virtual (CTXPFWD). Esta opção é útil quando o cliente não tem acesso à internet (por exemplo, thin clients). Baixo consumo de CPU e RAM no VDA, mas a largura de banda é consumida no canal virtual ICA®.

Existem três modos de operação neste cenário. O termo proxy refere-se a um dispositivo proxy que o VDA acessa para obter acesso à Internet.

Qual opção de política escolher:

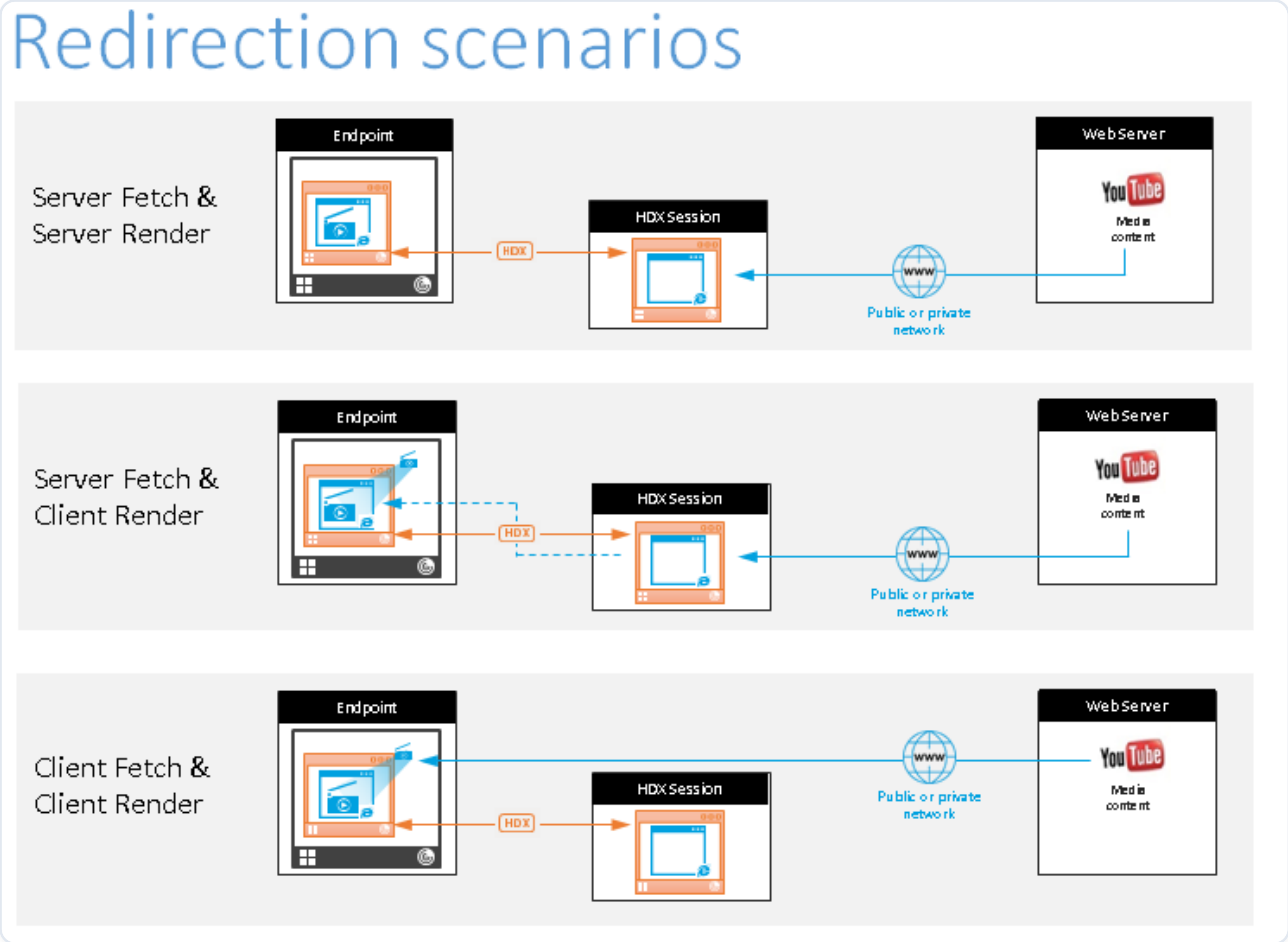
- **Proxy Explícito**: Se você tiver um único proxy explícito em seu data center.
- **Direto ou Transparente**: Se você não tiver proxies, ou se usar proxies transparentes.
- **Arquivos PAC**: Se você depender de arquivos PAC, os navegadores no VDA podem escolher automaticamente o servidor proxy apropriado para buscar uma URL especificada.



- **Busca no cliente e renderização no cliente**: Como o aplicativo Citrix Workspace contata o servidor web diretamente, ele requer acesso à internet. Este cenário descarrega todo o uso de rede, CPU e RAM de seus sites XenApp e XenDesktop®.

  Benefícios:

  - Melhor experiência do usuário final (Adaptive Bit Rate (ABR))
  - Uso reduzido de recursos do VDA (CPU/RAM/IO)
  - Consumo de largura de banda reduzido



Mecanismo de fallback:

Pode haver momentos em que o redirecionamento do cliente falhe. Por exemplo, se a máquina cliente não tiver acesso direto à internet, uma resposta de erro pode ser enviada de volta ao VDA. Nesses casos, o navegador no VDA pode então recarregar e renderizar a página no servidor.

Você pode suprimir a renderização de elementos de vídeo no servidor usando a política existente de **prevenção de fallback do Windows Media**. Defina esta política como **Reproduzir todo o conteúdo apenas no cliente** ou **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Essas configurações impedem que elementos de vídeo sejam reproduzidos no servidor se houver falhas no redirecionamento do cliente. Esta política entra em vigor somente quando você habilita o redirecionamento de conteúdo do navegador e a política de **Lista de Controle de Acesso** contém a URL que faz o fallback. A URL não pode estar na política de lista de bloqueio.

Requisitos do sistema

Citrix Aplicativos Virtuais e Desktops™

- Citrix Virtual Apps and Desktops 7 1808 ou posterior
- XenApp and XenDesktop 7.15 CU5 ou posterior

- SO do VDA: Windows 10 e 11, Windows Server 2016/2019/2022
- Navegador no VDA:
  - Versão mais recente do Google Chrome
  - Versão mais recente do Microsoft Edge
- Extensão BCR da Chrome Web Store instalada no navegador no VDA

Endpoints Windows

- Windows 10 e 11
- Citrix Workspace app 1809 para Windows ou posterior

> **Observação:**

> O redirecionamento de conteúdo do navegador não é suportado nas versões LTSR do Citrix Workspace app -1912 e 2203.1.

Endpoints Linux

- Citrix Workspace app 1808 para Linux ou posterior
- Terminais thin client devem incluir WebKitGTK+

Endpoints Mac (Pré-visualização)

- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma (até 14.2.1) com a versão mínima do Citrix Workspace app 2311

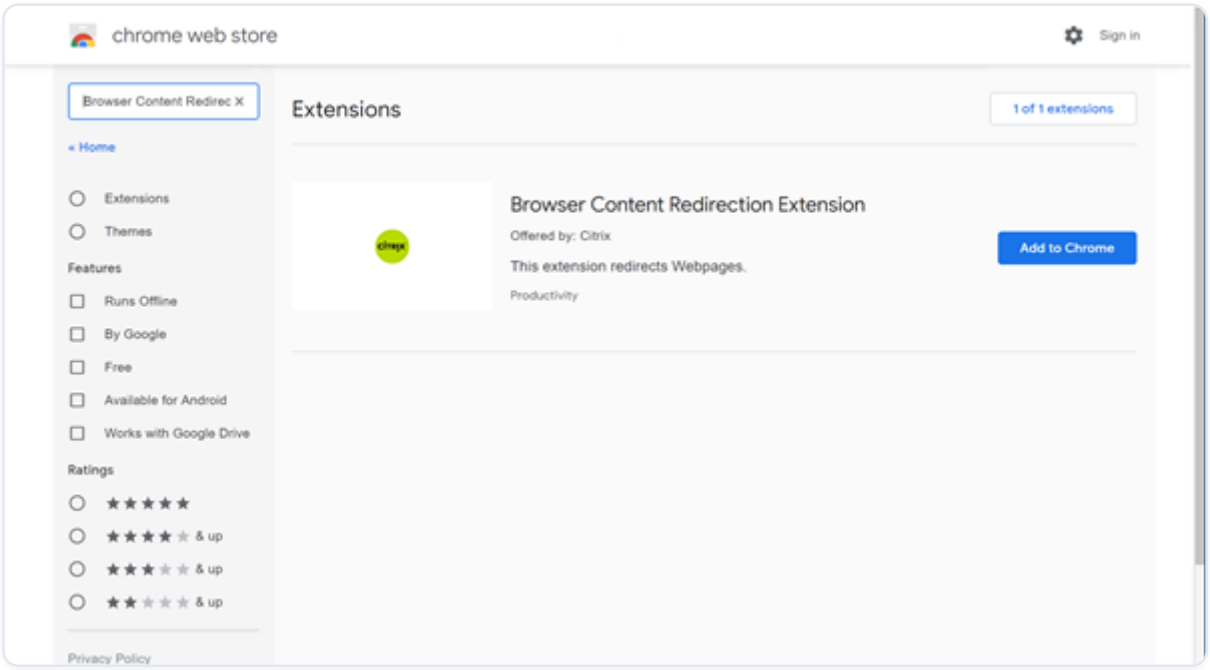
Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo Como solucionar problemas de redirecionamento de conteúdo do navegador Knowledge Center.

Extensão do Chrome para redirecionamento de conteúdo do navegador

Para usar o redirecionamento de conteúdo do navegador com o Chrome, adicione a extensão de redirecionamento de conteúdo do navegador da Chrome Web Store. Clique em **Adicionar ao Chrome** no ambiente Citrix Virtual Apps and Desktops.

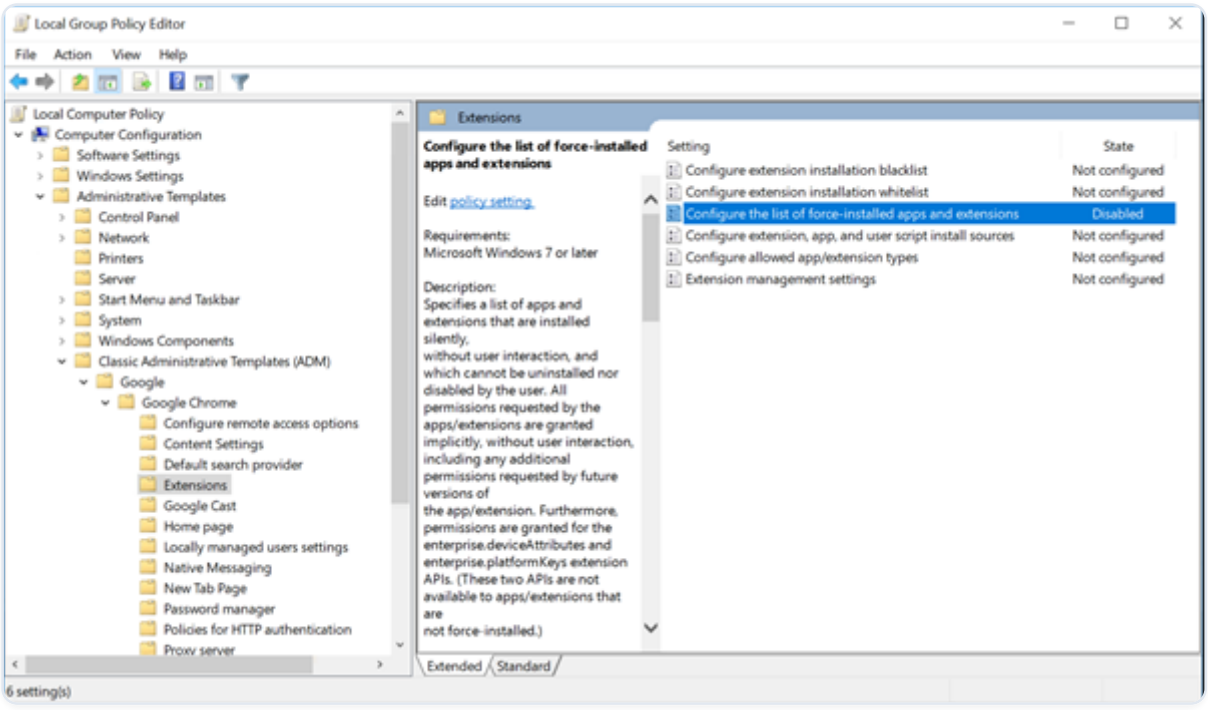
A extensão **não** é necessária na máquina cliente do usuário – apenas no VDA.



Este método funciona para usuários individuais. Para implantar a extensão para um grande grupo de usuários em sua organização, implante a extensão usando a Política de Grupo.

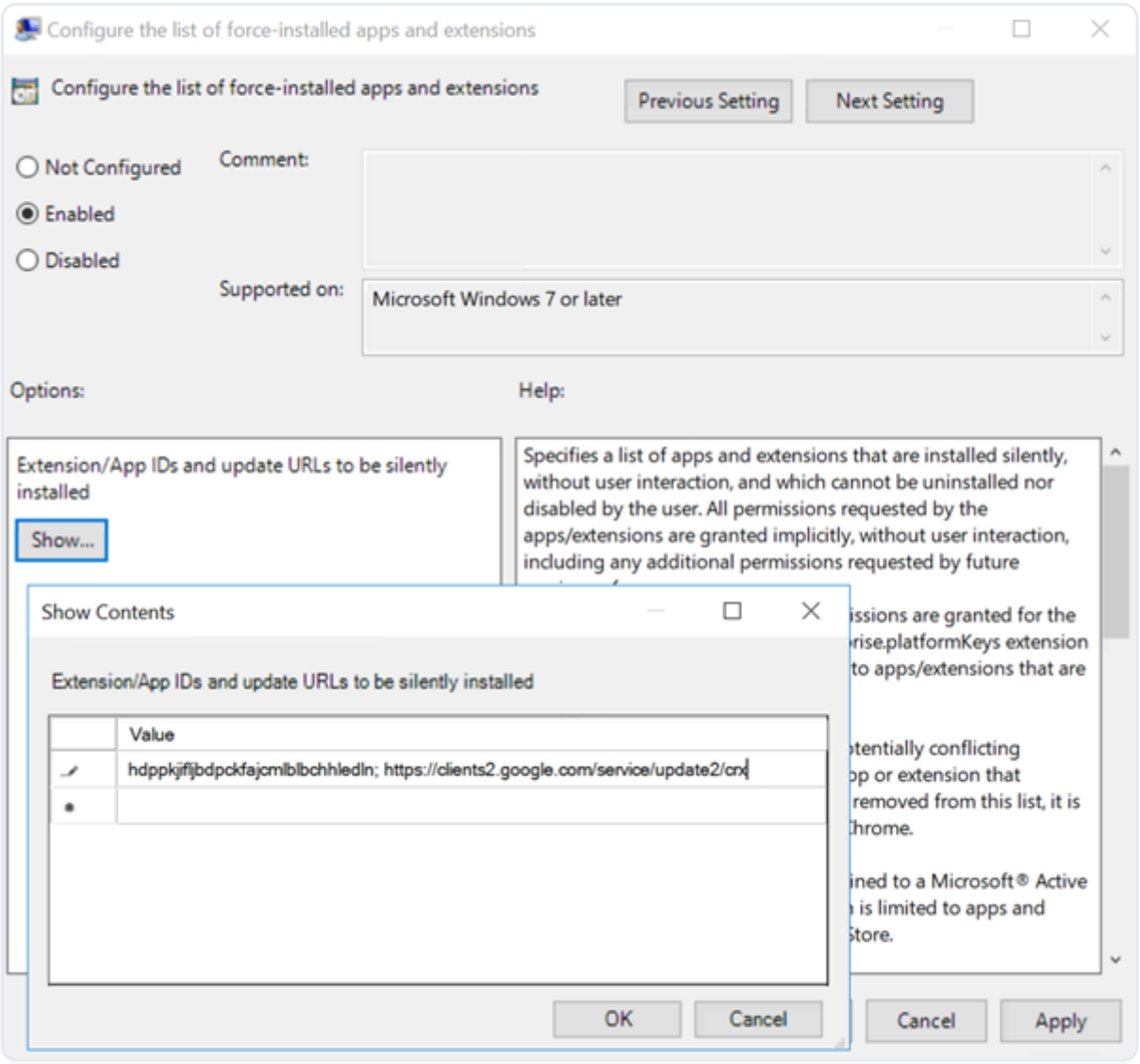
Implantar a extensão usando a Política de Grupo

1. Importe os arquivos ADMX do Google Chrome para o seu ambiente. Para obter informações sobre como baixar modelos de política e instalar e configurar os modelos no seu Editor de Política de Grupo, consulte Definir políticas do navegador Chrome em PCs gerenciados.
2. Abra seu console de Gerenciamento de Política de Grupo e vá para **Configuração do Usuário \ Modelos Administrativos\Modelos Administrativos Clássicos (ADM) \ Google\ Google Chrome \ Extensões**. Habilite a configuração **Configurar a lista de aplicativos e extensões instalados à força**.



3. Clique em **Mostrar** e digite a seguinte string correspondente 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, após uma atualização de **gpupdate**, o usuário recebe automaticamente a extensão. Se você iniciar o navegador Chrome na sessão do usuário, a extensão já estará aplicada e ele não poderá removê-la.

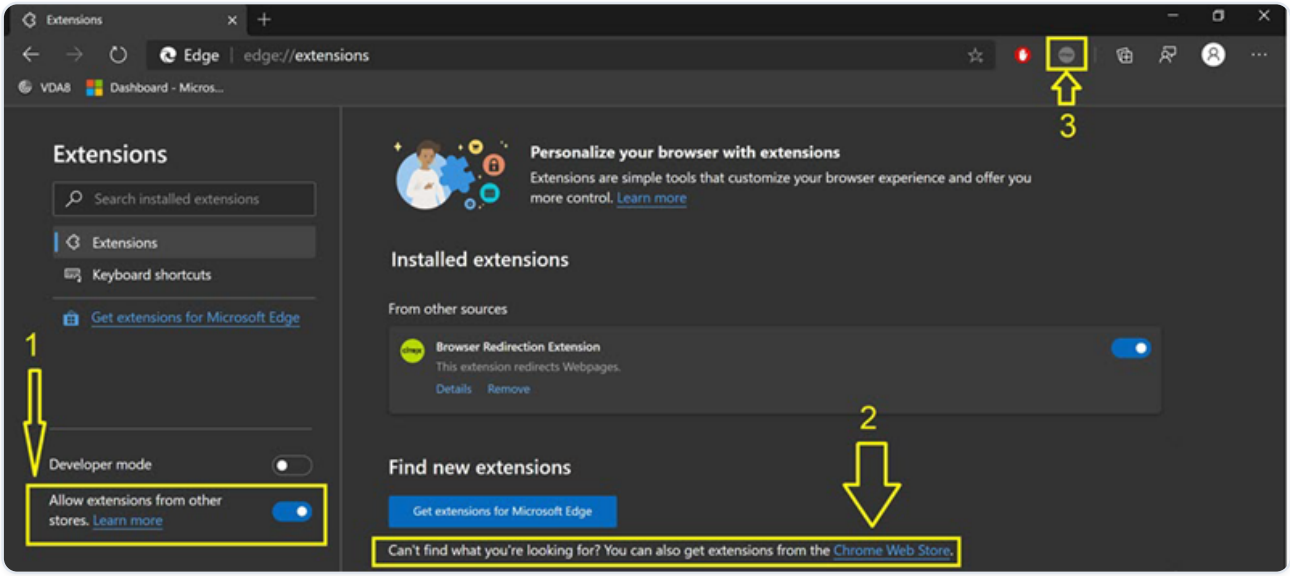
   Quaisquer atualizações da extensão são instaladas automaticamente nas máquinas dos usuários por meio do URL de atualização que você especificou na configuração.

   Se a configuração **Configurar a lista de aplicativos e extensões instalados à força** estiver definida como **Desativada**, a extensão é automaticamente removida do Chrome para todos os usuários.

Extensão de redirecionamento de conteúdo do navegador Edge Chromium

Para instalar a extensão de redirecionamento de conteúdo do navegador no Edge, certifique-se de ter a versão **83.0.478.37** ou superior do navegador Edge instalada.

1. Clique na opção **Extensões**. Escolha **Gerenciar extensão**. Ative **Permitir extensões de outras lojas**.
2. Clique no link da **Chrome Web Store** e a extensão aparecerá na barra superior direita. Para 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 (escala) definido para qualquer 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 desabilitar a aceleração de GPU do redirecionamento de conteúdo do navegador para o Chrome, criando a chave de registro na máquina do usuário. Para obter informações, consulte Redirecionamento de conteúdo do navegador e DPI na lista de recursos gerenciados por meio do registro.

Logon único com Autenticação Integrada do Windows

O redirecionamento de conteúdo do navegador aprimora a sobreposição para usar o esquema **Negotiate** para autenticação em servidores web configurados com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio do VDA.

Por padrão, o redirecionamento de conteúdo do navegador usa um esquema de autenticação básico que exige que os usuários se autenticar com suas credenciais do VDA cada vez que acessam o servidor web. Para logon único, você pode habilitar a configuração de política **Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador** ou criar uma chave de registro no VDA.

Antes de habilitar o logon único, conclua o seguinte:

- Configure a infraestrutura Kerberos para emitir tickets para nomes de entidade de serviço (SPNs) construídos a partir do nome do host. Por exemplo, `HTTP/serverhostname.com`.
- Para busca no servidor: Ao usar o redirecionamento de conteúdo do navegador no modo de busca no servidor, certifique-se de que o DNS esteja configurado corretamente no VDA.
- Para busca no cliente: Ao usar o redirecionamento de conteúdo do navegador no modo de busca no cliente, certifique-se de que o DNS esteja configurado corretamente no dispositivo cliente e que você permita conexões TCP da sobreposição para o endereço IP do servidor web.

Para configurar o logon único usando a política de redirecionamento de conteúdo do navegador, consulte a configuração Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador.

Alternativamente, você pode habilitar o logon único em um servidor web adicionando uma chave de registro no VDA. Para obter informações, consulte Logon único com Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador na lista de recursos gerenciados através do registro.

Cabeçalho de solicitação User-agent

O cabeçalho user-agent ajuda a identificar as solicitações HTTP enviadas pelo redirecionamento de conteúdo do navegador. Essa configuração pode ser útil ao configurar regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas pelo redirecionamento de conteúdo do navegador, você pode criar uma regra que contenha o cabeçalho user-agent para ignorar certos requisitos.

Apenas dispositivos Windows suportam o cabeçalho de solicitação user-agent.

Por padrão, a string do cabeçalho de solicitação user-agent está desabilitada. Para habilitar o cabeçalho user-agent para conteúdo renderizado no cliente, use o editor de Registro. Para obter informações, consulte Cabeçalho de solicitação User-agent na lista de recursos gerenciados através do registro.

Compatibilidade do cliente de redirecionamento de conteúdo do navegador

Você pode usar o WMI para verificar se seu cliente é compatível com o redirecionamento de conteúdo do navegador. Qualquer método para acessar o WMI funciona. O seguinte é um exemplo usando PowerShell.

1. Abra o PowerShell.

2. Execute `Get-WmiObject -Class CTXBCRStatus`.
3. Verifique o parâmetro `BCR_Capable`.
    - Se `True`, o cliente é compatível com o redirecionamento de conteúdo do navegador.
    - Se `False`, o cliente não é compatível com o redirecionamento de conteúdo do navegador.

Informações adicionais

- Se `CtxBrowserSvc` não estiver disponível, nenhum resultado será exibido ao executar o comando.
- Se `CtxBrowserSvc` nunca tiver sido executado, os resultados retornarão um erro de classe inválida.

Limitações do redirecionamento de conteúdo do navegador

O redirecionamento de conteúdo do navegador não oferece suporte aos seguintes casos de uso:

- Aplicativos web que exigem janelas pop-up não são suportados.
- Aplicativos web que exigem persistência de cookie de sessão também não são suportados. Aplicativos dependentes do serviço de autenticação do Google (por exemplo, Google Meet) podem ser bloqueados.
- O plug-in de extensão não é publicado oficialmente na loja do Microsoft Edge. No entanto, você pode usar a loja do Chrome para instalar as extensões.
- A política de redirecionamento de vídeo HTML5 deve ser desabilitada quando o Redirecionamento de Conteúdo do Navegador estiver em uso.
- O Redirecionamento de Conteúdo do Navegador não é suportado em estrutura ARMhf (ARM hard float).
- Às vezes, os usuários também podem ser desconectados de suas sessões devido a redes não confiáveis, latência de rede altamente variável ou limitações de alcance de dispositivos sem fio. Atualmente, o BCR não possui mecanismos de fallback ou relatórios suficientes para esses cenários.
- Não é possível baixar arquivos ou imprimir no navegador de sobreposição do BCR.
- O modo de navegação anônima ou privada não é suportado com o redirecionamento de conteúdo do navegador.

Videoconferência HDX™ e compressão de vídeo de webcam

Aviso:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Webcams podem ser usadas por aplicativos em execução na sessão virtual usando a compressão de vídeo de webcam HDX ou o redirecionamento USB genérico plug-n-play HDX. Use **Citrix Workspace™ app > Preferências > Dispositivos** para alternar entre os modos. A Citrix recomenda que você sempre use a compressão de vídeo de webcam HDX, se possível. O redirecionamento USB genérico HDX é recomendado apenas quando há problemas de compatibilidade de aplicativos com a compressão de vídeo HDX ou quando você precisa de funcionalidades nativas avançadas da webcam. Para um melhor desempenho, a Citrix recomenda que o Virtual Delivery Agent tenha pelo menos duas CPUs virtuais.

Para impedir que os usuários alternem da compressão de vídeo de webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em **Configurações de política ICA® > Configurações de política de dispositivos USB**. Os usuários do Citrix Workspace app podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**.

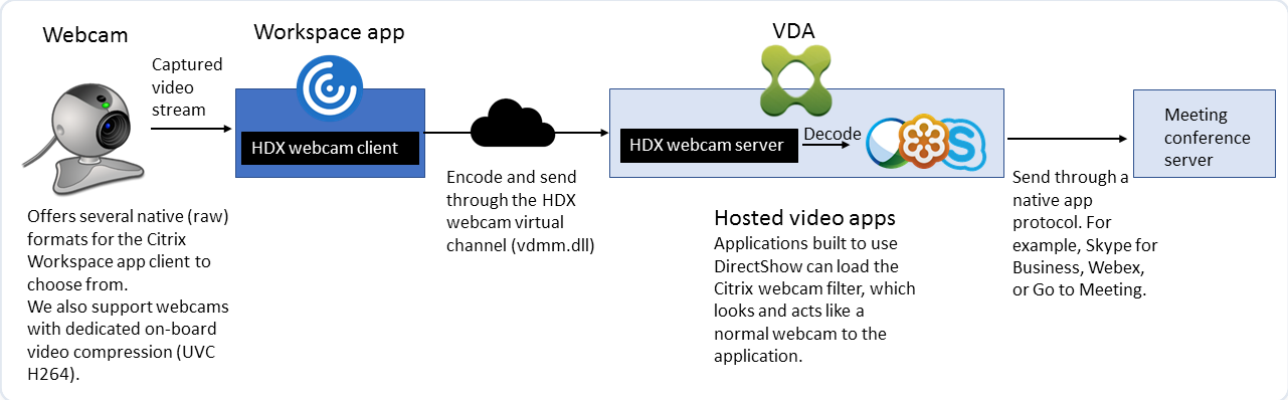
Compressão de vídeo de webcam HDX

A compressão de vídeo de webcam HDX também é chamada de modo de webcam **Otimizado**. Este tipo de compressão de vídeo de webcam envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compressão de webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Este recurso é habilitado por padrão.

Para desabilitar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina a chave de registro como 0 no VDA. Para obter informações, consulte Compressão de vídeo de webcam na lista de recursos gerenciados através do registro.

Se você desabilitar a funcionalidade padrão para streaming de recursos de vídeo, a compressão de vídeo de webcam HDX usa a tecnologia de framework multimídia que faz parte do sistema operacional cliente para interceptar vídeo de dispositivos de captura, transcodificá-lo e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do SO.

O cliente lida com a comunicação com a webcam. O cliente então envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua integração oferece a mesma experiência em sua área de trabalho. O aplicativo Workspace compacta o vídeo para economizar largura de banda e proporcionar melhor resiliência em cenários de WAN.



A política de **Conferência multimídia** deve ser habilitada para a compressão de vídeo de webcam HDX. Esta política é habilitada por padrão.

Se uma webcam suporta codificação de hardware, a compressão de vídeo HDX usa a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compressão de software, edite a chave de registro no cliente. Para obter informações, consulte Compressão de software de webcam na lista de recursos gerenciados através do registro.

Requisitos de compressão de vídeo de webcam HDX

A compressão de vídeo de webcam HDX suporta as seguintes versões do Citrix Workspace app:

PLATAFORMA	PROCESSADOR
Aplicativo Citrix Workspace para Windows	O aplicativo Citrix Workspace para Windows suporta compactação de vídeo de webcam para aplicativos de 32 bits e 64 bits no XenApp e XenDesktop 7.17 e posterior. Em versões anteriores, o aplicativo Citrix Workspace para

PLATAFORMA	PROCESSADOR
	Windows suporta apenas aplicativos de 32 bits.
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 posterior. 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 aplicativos de 32 bits e 64 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.

Aplicativos de vídeo baseados em Media Foundation suportam compactação de vídeo de webcam HDX no Windows 10 ou superior e Windows Server 2019 ou superior. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.
- Webcam compatível com DirectShow (use as configurações padrão da webcam). Webcams com capacidade de codificação de hardware reduzem o uso da CPU do lado do cliente.
- Para compactação de vídeo de webcam HDX, instale os drivers da webcam no cliente, obtidos do fabricante da câmera, se possível. A instalação dos drivers do dispositivo não é necessária no servidor.

Diferentes webcams oferecem diferentes taxas de quadros e têm diferentes níveis de brilho e contraste. Ajustar o contraste da webcam pode reduzir significativamente o tráfego de upstream. A Citrix usa as seguintes webcams para validação inicial de recursos:

- Modelos Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro

- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar a taxa de quadros de vídeo preferida, edite a chave do registro no cliente. Para obter informações, consulte Taxa de quadros de compactação de vídeo da webcam na lista de recursos gerenciados por meio do registro.

Streaming de webcam de alta definição

O aplicativo de videoconferência no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo. Quando a webcam e o aplicativo de videoconferência suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos todas as resoluções de webcam.

Este recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver para Windows, versão mínima 4.10.

Você pode usar uma chave do registro para desabilitar 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 do tipo de mídia falhar, o HDX reverterá para a resolução VGA padrão (640 x 480 pixels). Você pode usar chaves do registro no cliente para configurar a resolução padrão. Certifique-se de que a câmera suporte a resolução especificada. Para obter informações, consulte Resolução de webcam de alta definição na lista de recursos gerenciados por meio do registro.

A compactação de vídeo da webcam HDX usa significativamente menos largura de banda em comparação com o redirecionamento USB genérico plug-n-play e funciona bem em conexões WAN. Para ajustar a largura de banda, defina a chave do registro no cliente. Para obter informações, consulte Largura de banda da webcam de alta definição na lista de recursos gerenciados por meio do registro.

Insira um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usarão 350000 bps por padrão.

Redirecionamento USB genérico plug-n-play HDX

O redirecionamento USB genérico plug-n-play HDX (isócrono) também é chamado de modo de webcam **Genérico**. O benefício do redirecionamento USB genérico plug-n-play HDX é que você

não precisa instalar drivers em seu thin client/endpoint. A pilha USB é virtualizada de forma que qualquer coisa que você conecte ao cliente local é enviada para a VM remota. A área de trabalho remota age como se você a tivesse conectado nativamente. A área de trabalho do Windows lida com toda a interação com o hardware e executa a lógica plug-n-play para encontrar os drivers corretos. A maioria das webcams funciona se os drivers existirem no servidor e puderem funcionar via ICA. O modo de webcam genérico usa significativamente mais largura de banda (muitos Megabits por segundo) porque você está enviando vídeo não compactado com o protocolo USB pela rede.

Redirecionamento multimídia HTML5

O redirecionamento multimídia HTML5 estende os recursos de redirecionamento multimídia do HDX™ MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento na distribuição online de conteúdo multimídia, especialmente para dispositivos móveis, a indústria de navegadores desenvolveu maneiras mais eficientes de apresentar áudio e vídeo.

O Flash tem sido o padrão, mas requer um plug-in, não funciona em todos os dispositivos e tem maior consumo de bateria em dispositivos móveis. Empresas como YouTube, Netflix e versões mais recentes de navegadores da Mozilla, Google e Microsoft estão migrando para o HTML5, tornando-o o novo padrão.

Multimídia baseada em HTML5 tem muitas vantagens sobre plug-ins proprietários, incluindo:

- Padrões independentes de empresas (W3C)
- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança levantados por plug-ins

Downloads progressivos HTTP

O download progressivo HTTP é um método de pseudo-streaming baseado em HTTP que suporta HTML5. Em um download progressivo, o navegador reproduz um único arquivo (codificado em uma única qualidade) enquanto ele está sendo baixado de um servidor web HTTP. O vídeo é armazenado na unidade à medida que é recebido e é reproduzido da unidade. Se você assistir ao vídeo novamente, o navegador pode carregar o vídeo do cache.

Para um exemplo de download progressivo, consulte a página de teste de redirecionamento de vídeo HTML5. Para inspecionar os elementos de vídeo na página da web e encontrar as fontes (formato de contêiner mp4) nas tags de vídeo HTML5, use as ferramentas de desenvolvedor em seu navegador:

Comparando HTML5 e Flash

RECURSO	HTML5	FLASH
Requer um reprodutor proprietário	Não	Sim
Executa em dispositivos móveis	Sim	Alguns
Velocidade de execução em diferentes plataformas	Alta	Lento
Compatível com iOS	Sim	Não
Uso de recursos	Menos	Mais
Carrega mais rápido	Sim	Não

Requisitos

Oferecemos suporte apenas ao redirecionamento para downloads progressivos no formato mp4. Não oferecemos suporte a WebM e tecnologias de streaming de taxa de bits adaptável como DASH/HLS.

Oferecemos suporte ao seguinte e usamos políticas para controlá-los. Para obter mais informações, consulte Configurações de política de multimídia.

- Renderização no lado do servidor
- Busca no servidor, renderização no cliente
- Busca e renderização no lado do cliente

Versões mínimas do aplicativo Citrix Workspace™ e do Citrix Receiver™:

- Aplicativo Citrix Workspace 1808 para Windows
- Citrix Receiver para Windows 4.5
- Citrix Workspace app 1808 para Linux
- Citrix Receiver para Linux 13.5

VERSÃO MÍNIMA DO NAVEGADOR VDA	VERSÃO/COMPILAÇÃO/SP DO SO WINDOWS
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Adicione manualmente os certificados ao armazenamento de certificados do Firefox ou configure o Firefox para procurar certificados em um armazenamento de certificados confiável do Windows. Para obter mais informações, consulte `https://wiki.mozilla.org/CA:AddRootToFirefox`	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Componentes da solução de redirecionamento de vídeo HTML5

- **HdxVideo.js** - Hook JavaScript que intercepta comandos de vídeo no site. HdxVideo.js se comunica com o WebSocketService usando WebSockets Seguros (SSL/TLS).
- **Certificados SSL do 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 and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) Local: **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 and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) Localização: **Certificates (Local Computer) > Personal > Certificates**.
- **WebSocketService.exe** - Executa no sistema local e realiza a terminação SSL e o mapeamento da sessão do usuário. WebSocket Seguro TLS escutando em 127.0.0.1 porta 9001.
- **WebSocketAgent.exe** - Executa na sessão do usuário e renderiza o vídeo conforme instruído pelos comandos do WebSocketService.

Como faço para habilitar o redirecionamento de vídeo HTML5?

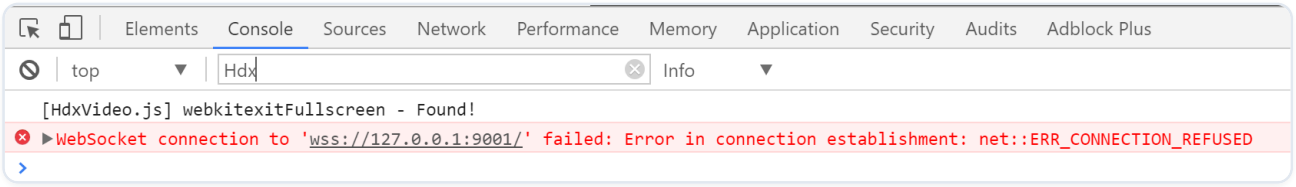
Nesta versão, este recurso está disponível apenas para páginas web controladas. Requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de taxa de bits adaptativa (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não são suportados.

Para obter mais informações, consulte *Configurações de política multimídia*.

Dicas de Solução de Problemas

Podem ocorrer erros quando a página web tenta executar HdxVideo.js. Se o JavaScript falhar ao carregar, o mecanismo de redirecionamento HTML5 falha. Certifique-se de que não há erros relacionados a HdxVideo.js inspecionando o console nas janelas da ferramenta de desenvolvedor do seu navegador. Por exemplo:



Otimização para Microsoft Teams (Novo)

A Citrix® oferece suporte a duas maneiras de otimizar áudio e vídeo do Microsoft Teams em um ambiente VDI: Otimização Citrix HDX™ e a Nova solução VDI para Teams da Microsoft. O Teams Clássico atingiu o fim da vida útil, portanto, as abordagens de otimização descritas nesta página se aplicam ao cliente atual do Microsoft Teams.

> **Observação:**

> A Microsoft anunciou a descontinuação da Otimização Citrix HDX baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

> - October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.

- April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

Recomenda-se que os clientes migrem para a Nova solução VDI para Teams. Essa alteração afeta apenas os endpoints Windows. Os endpoints macOS, Linux, ChromeOS e HTML5 não são impactados. Para mais detalhes, consulte Blog da Microsoft.

Abordagens de otimização

- **Otimização Citrix HDX (MTOP)**: Uma solução combinada Citrix e Microsoft que usa um canal virtual de propriedade da Citrix (CTXMTOP). O descarregamento de mídia é tratado por `HdxRtcEngine` no aplicativo Citrix Workspace™. Esta solução é tradicionalmente referida como MTOP.
- **Nova solução VDI para Teams**: Uma otimização mais recente que é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2). Está disponível em endpoints Windows e Mac. Para detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.

Principais distinções

OTIMIZAÇÃO CITRIX HDX	NOVA SOLUÇÃO VDI PARA TEAMS
A otimização é uma solução combinada da Citrix e da Microsoft e usa um canal virtual de propriedade da Citrix (CTXMTOP).	A solução de otimização é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2).
O descarregamento de mídia é tratado por `HdxRtcEngine` que reside no aplicativo Citrix Workspace.	O descarregamento de mídia é tratado pelo mecanismo de mídia SlimCore em endpoints Windows e Mac.
Nenhum componente adicional é necessário no endpoint, exceto a instalação do aplicativo Citrix Workspace.	Um componente adicional - o **Teams VDI Plugin** - precisa ser implantado no endpoint por vários meios. Este plug-in gerencia o download e as atualizações do mecanismo de mídia SlimCore.
Disponível nas plataformas de endpoint - Windows, macOS, Linux e ChromeOS.	Disponível nas plataformas de endpoint - Windows e Mac.

OTIMIZAÇÃO CITRIX HDX	NOVA SOLUÇÃO VDI PARA TEAMS
Novos recursos são gerenciados em conjunto entre a Citrix e a Microsoft.	Novos recursos são gerenciados pela Microsoft. Os usuários têm acesso a alguns novos recursos indisponíveis com a Otimização Citrix HDX.
Suportado tanto pela Citrix quanto pela Microsoft, dependendo do componente envolvido. Os clientes podem abrir um caso com a Citrix ou com a Microsoft e são redirecionados para a equipe apropriada conforme necessário.	De propriedade e suportado pela Microsoft. A Citrix suporta os componentes Citrix envolvidos, como o aplicativo Citrix Workspace, a lista de permissões de canais virtuais e os mecanismos de implantação de plug-ins.

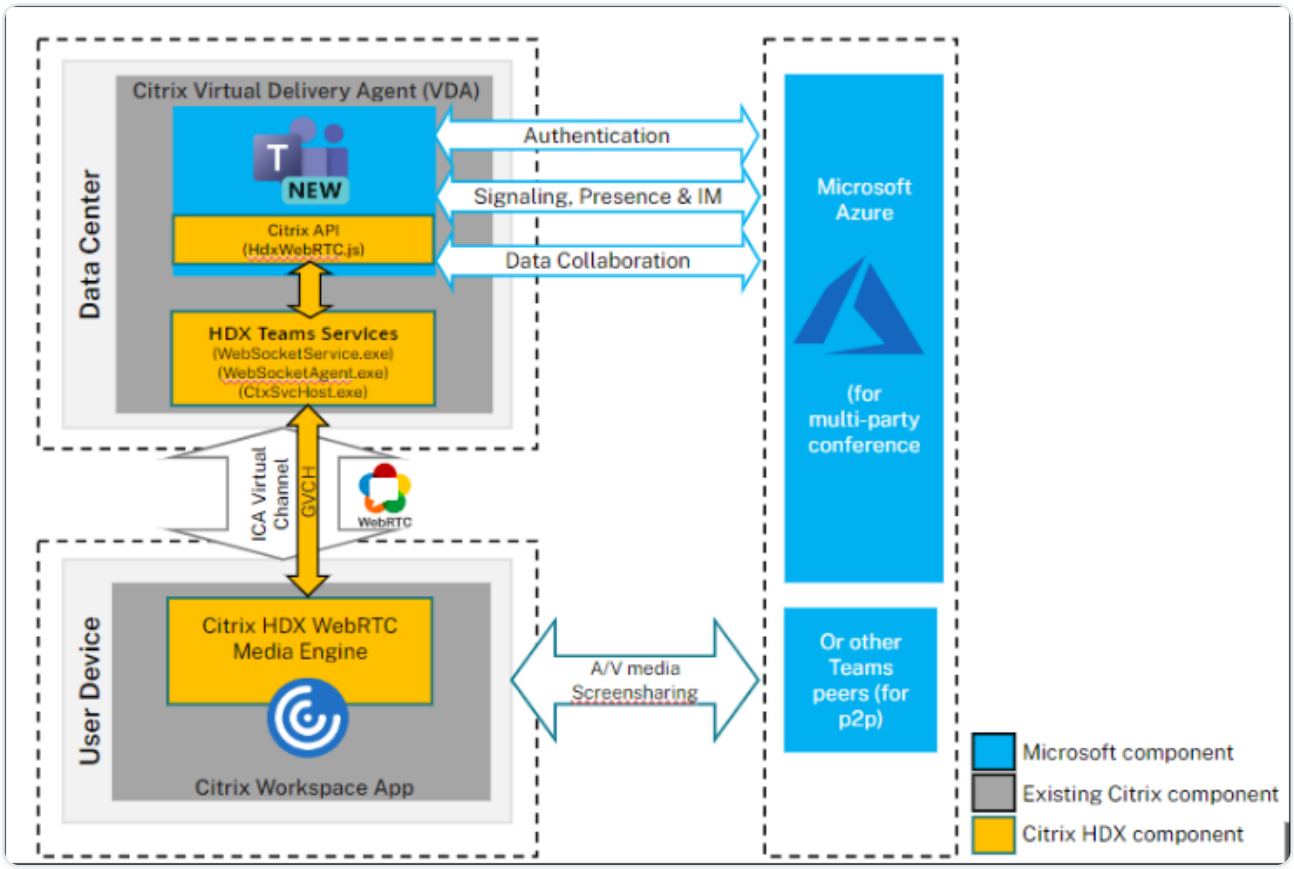
Interoperabilidade e roaming

A Otimização Citrix HDX e a nova solução VDI para Teams podem coexistir em paralelo, mas o cliente Teams usa apenas uma delas por vez.

- A otimização é selecionada quando o aplicativo Teams é iniciado, na seguinte ordem: nova solução VDI para Teams, depois Otimização Citrix HDX (WebRTC), e então redirecionamento padrão de áudio/vídeo.
- Se a nova solução VDI para Teams falhar, o Teams retorna diretamente para o redirecionamento padrão de áudio/vídeo, em vez de para o WebRTC. É necessário reiniciar o aplicativo Teams para executar novamente a seleção e escolher a otimização adequada.
- O roaming entre endpoints é contínuo e não requer a reinicialização do aplicativo Teams, inclusive quando um usuário alterna entre um endpoint que suporta a nova solução VDI para Teams e um que não suporta.

Otimização do Citrix HDX™

No Citrix HDX (Otimização WebRTC), o mecanismo de mídia (HdxRtcEngine) no endpoint responsável por lidar com a mídia descarregada é incorporado no aplicativo Citrix Workspace™ e a instalação do aplicativo Citrix Workspace instala automaticamente o mecanismo também.



Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para suportar o novo cliente Teams. Observe que nas versões mínimas, algumas correções de bugs críticas ou os recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as últimas correções e recursos.

Sistemas operacionais VDI

Para informações detalhadas, consulte as recomendações fornecidas na documentação Microsoft.

Observação:

- O Windows Server 2016 não é suportado. A Citrix recomenda que você planeje suas atualizações de acordo.
- Como as versões são atualizadas frequentemente, as versões mencionadas aqui podem se tornar obsoletas. Portanto, consulte as páginas de ciclo de vida do produto de Citrix Workspace app e Citrix Virtual Apps and Desktops para garantir que você esteja usando versões suportadas dos diferentes componentes.

- Se você estiver usando o Citrix Virtual Apps and Desktops™ 1912 LTSR, a Citrix recomenda planejar uma atualização, pois ele chegará ao fim de vida em dezembro de 2024.

Virtual Delivery Agent (VDA)

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
1912 LTSR CU8+; 2203 LTSR (qualquer CU); 2212 CR	2203 LTSR CU5+ (ou) 2402 LTSR e quaisquer versões CR acima

Aplicativo Citrix Workspace

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
Windows 2203 LTSR (CU mais recente); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405

Implantação

1. Instale o novo cliente Teams no VDI. Para obter informações detalhadas, consulte Implantar o novo Teams para VDI.
2. Configure a seguinte chave de registro no VDA para otimizar o novo Teams.
   - **Local**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **Chave (REG_Multi_SZ)**: `ProcessWhitelist`
   - **Valor**: `msedgewebview2.exe`

   Observação:

   A partir do Citrix Virtual Apps and Desktops 2402 LTSR (ou) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, você não precisa configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela é permitida por padrão.
3. Certifique-se de que a política Redirecionamento do Microsoft Teams esteja habilitada. Esta política é ativada por padrão.

4. Nenhuma configuração adicional é necessária no lado do cliente. Siga as instruções do assistente para instalar o aplicativo Citrix Workspace.

App Layering

O novo Microsoft Teams mudou seu método de instalação e agora é instalado em C:\Program Files\WindowsApps. Para oferecer suporte a essa mudança, você deve executar o App Layering versão 2403.2 ou posterior. Você pode baixar um disco de atualização na página Downloads do App Layering que inclui essa correção.

Para obter informações detalhadas, consulte a documentação do App Layering.

Citrix Profile Management

Consulte a documentação do Citrix Profile Management para obter informações sobre como habilitar o roaming para o novo Microsoft Teams. A orientação de versão mínima atual para o Citrix Profile Management é 2402 LTSR (ou) 2203 LTSR CU5+.

Considerações de rede

Os requisitos de rede para o novo Teams não diferem do Teams Clássico. Portanto, consulte a seção Requisito de Rede na documentação do Teams Clássico.

Matriz de recursos e suporte de versão

Como as versões são atualizadas frequentemente, algumas versões mais antigas mencionadas aqui podem chegar ao fim da vida útil. Portanto, consulte as páginas de ciclo de vida do produto de Citrix Workspace App e Citrix Virtual Apps and Desktops para garantir que você esteja usando versões compatíveis dos diferentes componentes.

> **Observação:**
>
> - As versões mencionadas aqui são as versões mínimas a partir das quais o recurso específico é suportado (ou) a versão mínima na qual o novo Teams é suportado, o que for maior.
> - Citrix Virtual Apps and Desktops 1912 LTSR CU8+ mencionado na seção de versões mínimas não está sendo mencionado na tabela abaixo, pois atingirá seu fim de vida em dezembro de 2024. No entanto, ainda é uma versão suportada até lá.
> - Recursos que têm as versões mínimas do Citrix Virtual Apps and Desktops como `N/A` apenas implicam que o recurso não envolveu nenhuma alteração do lado do VDA.

RECURSO	VDA (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA CHROMEOS (VERSÃO MÍNIMA)
Áudio / Vídeo (p2p e conferência)	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Compartilhamento de tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
i. Borda Vermelha do Indicador de Tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
ii. Limitar a captura ao Desktop Viewer	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
iii. Vários monitores	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
DTMF	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301

RECURSO	VDA (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA CHROMEOS (VERSÃO MÍNIMA)
Suporte a Servidor Proxy	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2305
Compartilhamento de apps	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2209	Não
Legendas ao Vivo	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
e911 Dinâmico	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Conceder Controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
Solicitar Controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Múltiplas Janelas	2203 LTSR (qualquer	2203 LTSR CU mais	2302	2207	2303

RECURSO	VDA (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA CHROMEOS (VERSÃO MÍNIMA)
	CU), 2212 CR	recente, 2302 CR			
Transcrições de Reunião	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Desfoque de fundo	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR última CU, 2302 CR	2302	2212	2303
Compartilhamento de tela (com Proteção de Aplicativo)	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	Não
Simulcast	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
Campainha Secundária	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
Compartilhar Áudio do Sistema	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	Não

Solução de problemas e outras considerações

Para o New Teams, consulte CTX253754 , Solucionar problemas do Microsoft Teams, Para as atualizações mais recentes sobre qualquer coisa relacionada ao New Teams, consulte CTX585013.

Limitações conhecidas

Limitações no aplicativo Citrix Workspace

- Suporte HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo poderá ser capturado.
- Limitações de compartilhamento de áudio do sistema
  - O áudio não pode ser compartilhado usando este recurso ao compartilhar a tela com aplicativos ou guias redirecionados RAVE e BCR.
  - Este recurso é suportado apenas em desktops publicados

Limitações no VDA

- O Novo Teams como um aplicativo publicado (seamless) não é suportado
  - Corrigido no CVAD 2402 LTSR, 2203 LTSR CU5 e superior
- Quando você configura a opção High DPI do aplicativo Citrix Workspace para Sim, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.
- O Microsoft Teams 2.1 suporta o redirecionamento de apenas uma webcam por vez. No entanto, ele não suporta o redirecionamento de múltiplas webcams ou o redirecionamento de webcam plug and play (PnP) em VDAs de sessão única.

Limitações no aplicativo Citrix Workspace e no VDA

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente – não no VDA.

Para mais detalhes sobre as limitações da Microsoft, consulte Recursos não suportados em VDI.

Nova solução VDI para Teams

Observação:

A nova solução VDI para Teams está atualmente geralmente disponível para endpoints Windows e Mac no Citrix®. Esta solução requer uma versão mínima do Microsoft Teams. Consulte Requisitos do sistema.

Na nova solução VDI para Teams, a Microsoft usa o SDK do Canal Virtual Citrix para criar canais virtuais personalizados. No endpoint, a mídia é descarregada para o mecanismo de mídia da Microsoft (SlimCore) em vez de `HdxRtcEngine`. Os canais virtuais personalizados transportam a comunicação entre o Teams no VDA e o mecanismo de mídia no endpoint.

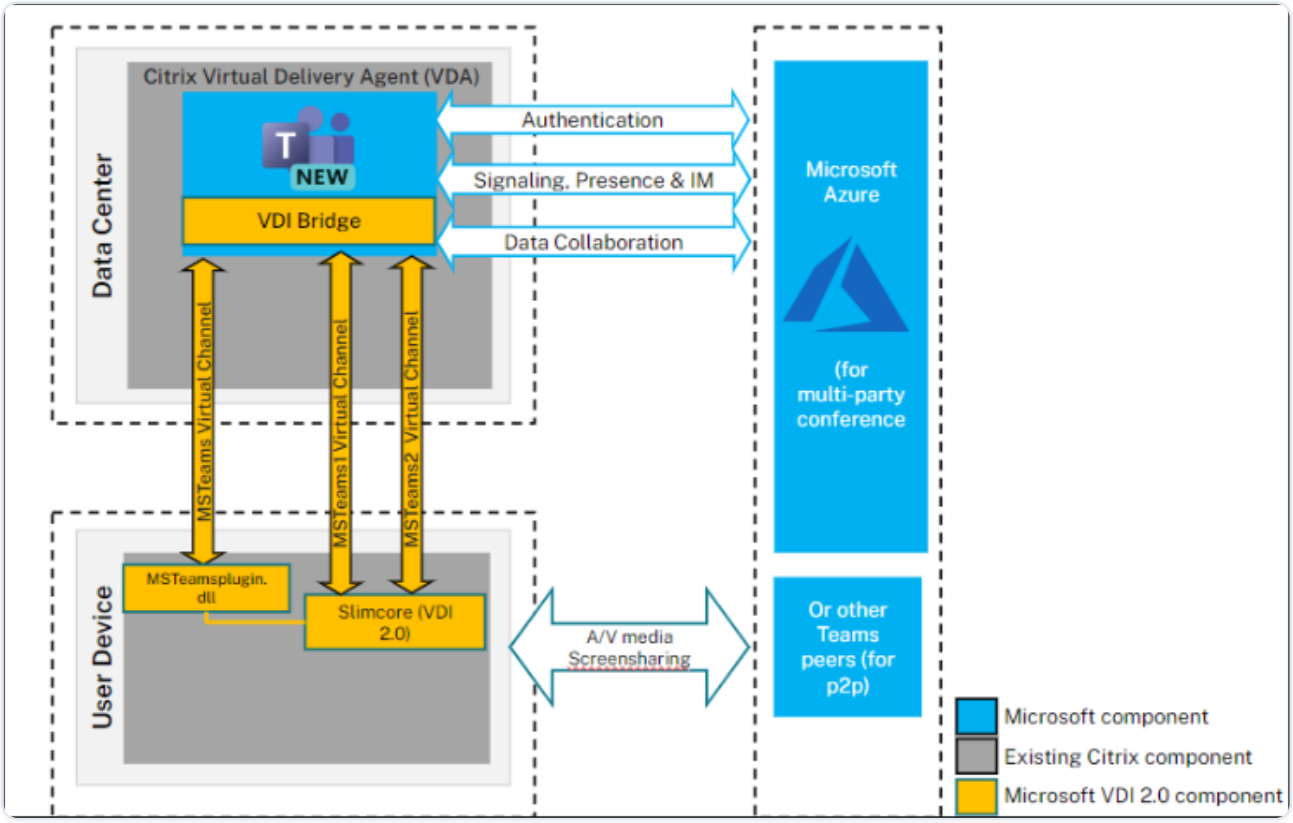
Observação:

A Microsoft anunciou a descontinuação da otimização Citrix HDX™ baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

- October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.
- April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

Recomenda-se que os clientes migrem para a nova solução VDI para Teams. Essa mudança afeta apenas os endpoints Windows. Endpoints macOS, Linux, ChromeOS e HTML5 não são impactados. Para mais detalhes, consulte Blog da Microsoft.

Esta solução é de propriedade e gerenciada pela Microsoft. A Citrix oferece suporte aos componentes Citrix envolvidos: aplicativo Citrix Workspace™, a lista de permissões de canais virtuais e os mecanismos de implantação de plug-ins descritos nesta página. Para a arquitetura de propriedade da Microsoft e detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.



Requisitos do sistema

Esta seção lista as versões mínimas e recomendadas necessárias para suportar a nova solução VDI para Teams. Em versões mínimas, algumas correções de bugs críticas ou os recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para a melhor experiência.

Virtual Delivery Agent (VDA)

Observação:

Se você estiver na versão 2203 LTSR CU2 ou inferior, ou 2303 CR ou inferior, consulte CTX682593 para entender as limitações nessas versões e planejar sua atualização.

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR e qualquer CR posterior

Aplicativo Citrix Workspace para Windows

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2203 LTSR (CU mais recente); 2302 CR	2402 LTSR; 2405 CR ou posterior

Aplicativo Citrix Workspace para Mac

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2508.10	2607 ou posterior

Os endpoints Mac exigem macOS 14, 15 ou 26. O macOS 26 exige o aplicativo Citrix Workspace 2511 ou posterior. No aplicativo Citrix Workspace para Mac 2508.10, o plug-in deve ser instalado manualmente. A opção de instalar o plug-in por meio do aplicativo Citrix Workspace, do Gerenciamento de Aplicativos Cliente ou do gerenciador de plug-ins de canal virtual está disponível a partir do aplicativo Citrix Workspace para Mac 2603.

Para a versão mínima do Microsoft Teams, requisitos de SO do endpoint e requisitos de hardware, consulte a documentação Microsoft.

Componentes

- Novo Teams `vdiBridge`: o módulo de canal virtual do lado do servidor, empacotado com o Teams.
- Canal virtual personalizado (VC): o VC personalizado de propriedade do Microsoft Teams.
- Plug-in: a DLL do VC do lado do cliente. Responsável pelo download e limpeza do mecanismo de mídia.
- Mecanismo de mídia (SlimCore): o mecanismo de mídia específico do sistema operacional, entregue pela Microsoft como um pacote MSIX.

Implantação

1. Certifique-se de ter a versão do Microsoft Teams listada em Pré-requisitos.
2. Configure a política **Lista de permissão de canais virtuais** para permitir os canais virtuais do Microsoft Teams. Esses canais permitem que o cliente Teams se conecte ao plug-in do lado do cliente. Para obter mais informações, consulte Segurança do canal virtual.

   A solução precisa de três canais virtuais personalizados. Use curingas para permitir o executável `ms-teams.exe` e os canais virtuais personalizados:

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

Observação:

- O VDA 2603 e versões posteriores permitem esses três canais virtuais por padrão. Nenhuma configuração de política do Studio é necessária nessas versões.
- Os curingas para a política de lista de permissão de canais virtuais estão disponíveis no CVAD 2203 LTSR CU2 e posterior, ou no Citrix Virtual Apps and Desktops™ 2206 CR e posterior.
- As máquinas VDA devem ser reiniciadas para que a política entre em vigor.
- O caminho de instalação do MSTeams muda porque é um aplicativo MSIX, então curingas são necessários. Permita as linhas exatas mostradas acima.

3. Esta solução é controlada por uma política do lado do Microsoft Teams, não por uma política da Citrix. Ela é habilitada por padrão. Para habilitá-la ou desabilitá-la para grupos de usuários específicos, consulte a documentação da Microsoft.
4. Implante o plug-in do Teams em seus endpoints. Consulte Opções para instalar o plug-in do Teams.
5. Para preparação e registro do mecanismo de mídia, e as políticas de grupo que podem bloquear a instalação do MSIX, consulte a documentação da Microsoft.

Opções para instalar o plug-in do Teams

Independentemente do método de instalação, o plug-in é colocado no local do aplicativo Citrix Workspace no endpoint:

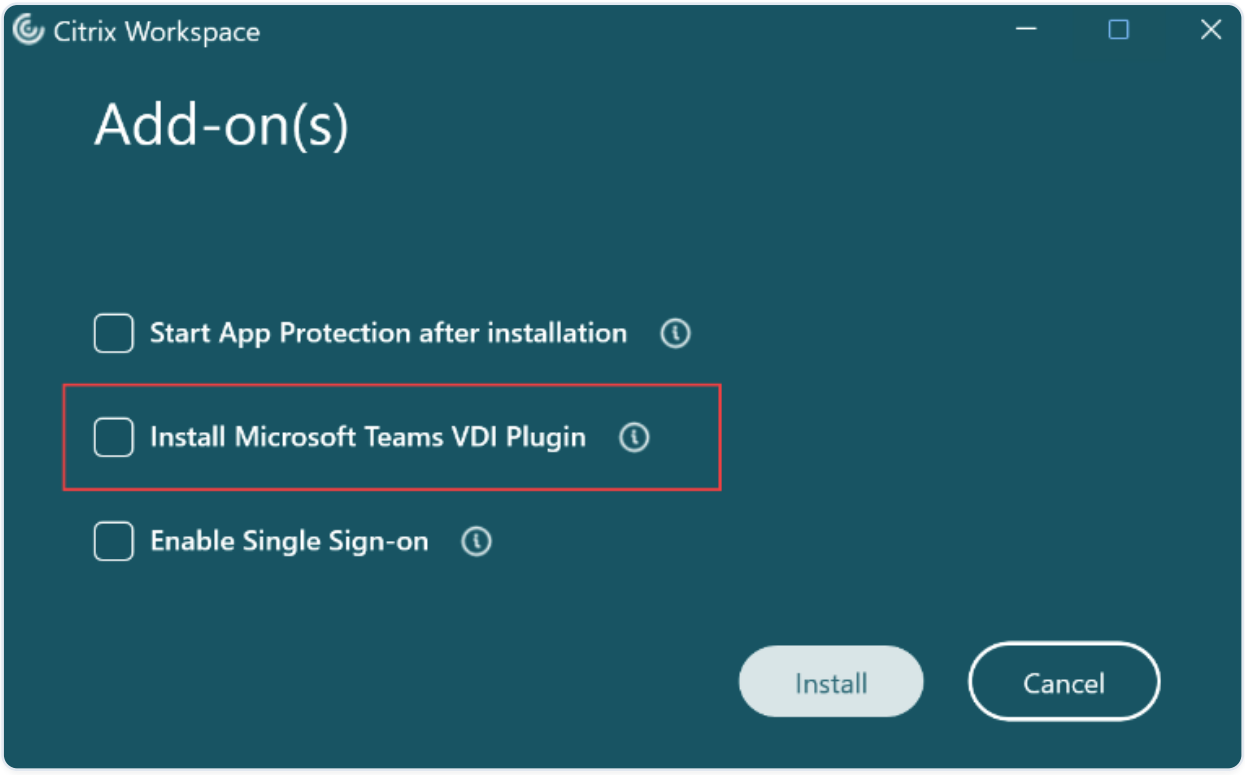
- Windows (`MsTeamsPluginCitrix.dll`): 64 bits `C:\Program Files (x86)\Citrix\ICA Client`; 32 bits `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

Observação:

- No Windows, instale o aplicativo Citrix Workspace no modo de administrador para que os canais virtuais sejam abertos corretamente. A instalação por usuário do aplicativo Citrix Workspace não é suportada.
- O plug-in VDI do Microsoft Teams não é suportado quando o aplicativo Citrix Workspace é instalado da Microsoft Store.
- A instalação do plug-in para se nenhum aplicativo Citrix Workspace for encontrado no endpoint.
- No Windows, o plug-in e o aplicativo Citrix Workspace devem ter a mesma arquitetura. Um aplicativo Citrix Workspace de 32 bits não pode carregar um plug-in de 64 bits.
- Os plug-ins podem ser atualizados ou reparados, mas não podem ser revertidos, e somente enquanto não houver uma sessão ativa.

Opção 1: Através da instalação do aplicativo Citrix Workspace

- **Windows:** Durante uma nova instalação ou atualização manual, selecione **Instalar Plug-in VDI do Microsoft Teams** na página **Complemento(s)**. A partir do aplicativo Citrix Workspace para Windows 2508, esta opção é selecionada por padrão. Desmarque-a para pular a instalação. As atualizações lembram sua seleção anterior.



Você também pode instalar pela linha de comando com a opção `/InstallMSTeamsPlugin`. Por exemplo, `CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` instala o plug-in, e `/InstallMSTeamsPlugin=N` o impede.

Para uma nova instalação, o mínimo é o aplicativo Citrix Workspace para Windows 2402 LTSR. Para atualizações no local, o mínimo é o aplicativo Citrix Workspace para Windows 2405 CR. Para obter os detalhes mais recentes, consulte Instalar plug-ins de terceiros.

- **Mac:** A opção de instalar o plug-in durante a instalação do aplicativo Citrix Workspace está disponível a partir do aplicativo Citrix Workspace para Mac 2603 e requer ação do usuário. O aplicativo Citrix Workspace para Mac 2607 instala o plug-in automaticamente por padrão. No aplicativo Citrix Workspace para Mac 2508.10, instale o plug-in manualmente. Consulte Opção 2: Baixar o plug-in diretamente.

Opção 2: Baixar o plug-in diretamente

- **Windows:** Baixe o MSI e implante-o com ferramentas como SCCM ou Intune sobre qualquer versão suportada do aplicativo Citrix Workspace:
  - Aplicativo Citrix Workspace de 32 bits: aka.ms/plugin
  - Aplicativo Citrix Workspace de 64 bits: aka.ms/plugin_x64
  - Aplicativo Citrix Workspace baseado em Arm: aka.ms/plugin_arm64
- **Mac:** Baixe o plug-in de aka.ms/macplugin e implante-o com ferramentas como JAMF.

Opção 3: Gerenciamento de Aplicativos Cliente (anteriormente serviço de Configuração Global de Aplicativos)

O Gerenciamento de Aplicativos Cliente (anteriormente serviço de Configuração Global de Aplicativos, ou GACS) gerencia as configurações de aplicativos para endpoints gerenciados e não gerenciados, e pode implantar o plug-in do Teams em seus endpoints. No Mac, isso requer o aplicativo Citrix Workspace para Mac 2603 ou posterior. Consulte Gerenciamento de plug-in VDI do Microsoft Teams.

Opção 4: Gerenciador de plug-in de canal virtual

O gerenciador de plug-in de canal virtual implanta plug-ins em endpoints de cliente para aplicativos que precisam de componentes de endpoint, incluindo a nova solução VDI para Teams. Ele detecta o aplicativo em execução no VDA e solicita ao usuário que instale o plug-in no endpoint. Os administradores podem usá-lo em cenários BYOD. No Mac, isso requer o aplicativo Citrix Workspace para Mac 2603 ou posterior. Consulte Gerenciador de plug-in de canal virtual.

Cenários de atualização de plug-in

A Citrix gerencia as atualizações do plug-in do Teams de forma transparente quando o plug-in é instalado através das Opções 1, 3 ou 4. Se o plug-in for instalado manualmente (Opção 2), a Citrix não manipular as atualizações.

- Certifique-se de que a atualização automática do aplicativo Citrix Workspace esteja ativada para atualizações automáticas de plug-in.
- Garanta um mínimo de Citrix Workspace app para Windows 2405. O Citrix Workspace app para Windows 2508 ou posterior instala o plug-in automaticamente quando o Citrix Workspace app é atualizado automaticamente.
- A Citrix não manipular a desinstalação do plug-in. Desinstale o plug-in separadamente quando necessário.

> **Observação:**
>
> A Citrix gerencia as atualizações do plug-in do Teams, não do mecanismo de mídia. A Microsoft entrega e atualiza o mecanismo de mídia.

Teams como um aplicativo publicado da Citrix

O Teams publicado como um aplicativo Citrix Virtual Apps pode ser otimizado com esta solução quando todos os componentes necessários atenderem às versões mínimas. Para as versões necessárias e limitações conhecidas, consulte a documentação Microsoft.

Interoperabilidade e roaming

Consulte Otimização para Microsoft Teams para saber como a nova solução VDI para Teams e a Otimização Citrix HDX interagem e como o roaming se comporta.

Considerações de rede

Consulte Considerações de rede na documentação da Microsoft.

Suporte a recursos

O conjunto de recursos e a implementação são de propriedade da Microsoft. Consulte a lista de recursos na documentação da Microsoft.

Solução de problemas

O cliente do Microsoft Teams relata o status de otimização e, quando a otimização falha, um código de erro. Esses indicadores de status e códigos de erro são definidos pela Microsoft. Para a lista completa e solução de problemas de ponta a ponta, consulte Solução de problemas da nova solução VDI para Teams na documentação da Microsoft.

O Citrix Monitor oferece visibilidade do estado de otimização desta solução. Nos detalhes de uma sessão, a exibição Topologia da Sessão mostra se o aplicativo está otimizado e sinaliza quaisquer componentes ausentes, como o gerenciador de plug-ins, o plug-in e sua versão, o estado do canal virtual e o status da lista de permissões do canal virtual. Para obter mais informações, consulte Visibilidade da otimização de comunicações em tempo real.

Alguns códigos de erro da Microsoft apontam para a configuração do lado do Citrix. Verificações comuns do Citrix:

- Se o cliente do Teams relatar que os canais virtuais personalizados estão bloqueados (erro da Microsoft 2003), confirme se a lista de permissões do canal virtual inclui MSTEAMS, MSTEAM1 e MSTEAM2.
- Se o cliente do Teams relatar que nenhum plug-in foi detectado (erro da Microsoft 2000), confirme se o plug-in está instalado e carregado. No Process Explorer, selecione `wfica32.exe`, mostre o painel inferior e verifique a guia DLL para `MsTeamsPluginCitrix.dll`.
- Se o cliente do Teams relatar uma versão não suportada do aplicativo Citrix Workspace (erro da Microsoft 2004), atualize para uma versão suportada. Consulte Requisitos do sistema.

Limitações conhecidas

Os recursos e a implementação são de propriedade da Microsoft. Consulte Problemas conhecidos na documentação da Microsoft.

Otimização para Microsoft Teams (Clássico)

> **Nota:**
>
> O novo Microsoft Teams 2.1 agora está geralmente disponível para VDA. Esta versão do Microsoft Teams é compatível com a Otimização do Citrix Microsoft Teams usando WebRTC (VDI 1.0).

> A partir do Citrix Virtual Apps and Desktops 2402, você não precisa configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela é permitida por padrão.

> Os aplicativos publicados agora são compatíveis com o novo Microsoft Teams.

> A Citrix oferece otimização para Microsoft Teams baseado em desktop usando Citrix Virtual Apps and Desktops™ e o aplicativo Citrix Workspace™. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

Nossa otimização para Microsoft Teams inclui serviços HDX™ do lado do VDA e uma API para interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O endpoint decodifica e fornece o multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem nativamente no aplicativo hospedado do Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um canal virtual de comando e controle. Isso significa que a mídia não é trocada entre o aplicativo Citrix Workspace e o VDA.

Apenas client-fetch/client-render está disponível.

Esta demonstração em vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam a versão mais recente disponível do Microsoft Teams e que ela seja mantida atualizada. As versões do aplicativo de desktop do Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas. As versões não suportadas do aplicativo de desktop do Microsoft Teams exibem uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Microsoft Teams (Desktop e Mac).

Recomendamos que você siga as diretrizes de instalação do Microsoft Teams para toda a máquina. Evite usar o instalador .exe que instala o Microsoft Teams em `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` na linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Ao definir este parâmetro, o Instalador do Microsoft Teams para toda a máquina aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem então desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro `ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` apenas em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não se atualiza automaticamente sempre que há uma nova versão. Recomendamos este modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou desktops de um Windows Server ou catálogos aleatórios/agrupados do Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação VDI).

Suponha que você tenha um ambiente VDI persistente dedicado do Windows 10. Você deseja que o aplicativo Microsoft Teams seja atualizado automaticamente e prefere que o Microsoft Teams seja instalado por usuário em `Appdata/Local`. Nesse caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> A Citrix recomenda instalar o VDA antes de instalar o Microsoft Teams na imagem dourada. Essa ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA, desinstale e reinstale o Microsoft Teams.

Para Acesso Remoto a PC

A Citrix recomenda que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior após a instalação do VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 e posteriores incluem lógica aumentada executada no momento do lançamento do Microsoft Teams e no momento do login para detecção do VDA. Essas versões também incluem identificação do tipo de sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem falhar ao detectar e desabilitar certos recursos ou elementos da interface do usuário. Por exemplo, Salas de Apoio, janelas pop-out para reuniões e bate-papos, ou reações de reunião.

> **Importante:**
>
> Ao alternar de uma sessão local para uma sessão HDX e se o Microsoft Teams for mantido aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar corretamente com o HDX. Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Ao trabalhar no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do Acesso Remoto ao PC (HDX ou local). Isso ocorre porque o Microsoft Teams só pode avaliar o modo VDI no momento do lançamento do aplicativo, e não enquanto já está em execução em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-out, Salas de Apoio ou reações de reunião.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, você deve criar uma chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` na linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em Multimídia.

Recomendações de Gerenciamento de Perfil

Recomendamos usar o instalador para toda a máquina para ambientes Windows Server e VDI agrupado do Windows 10.

Quando o sinalizador **ALLUSER=1** é passado para o MSI a partir da linha de comando (o instalador para toda a máquina), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**

> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> Um logon de usuário subsequente aciona a instalação final em **AppData**.

Instalador para toda a máquina

A seguir, um exemplo de pastas, atalhos da área de trabalho e registros criados pela instalação de um instalador do Microsoft Teams para toda a máquina em qualquer VM do Windows Server de 64 bits:

Pasta:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho da Área de Trabalho:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registro:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`

- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> O local do registro varia de acordo com os Sistemas Operacionais subjacentes e a arquitetura (bitness).

Recomendações

- Recomendamos desativar a inicialização automática excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do seu dia de trabalho) aumentem o uso da CPU da VM.
- Se a área de trabalho virtual não tiver uma GPU/vGPU, recomendamos definir **Desabilitar aceleração de hardware da GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada em `%Appdata%\Microsoft\Teams` em `desktop-config.json`. Você pode usar um script de logon para editar esse arquivo e definir o valor como `true`.
- Se estiver usando o Citrix Workspace Environment Management™ (WEM), ative a **Proteção contra Picos de CPU** para gerenciar o consumo do processador para o Microsoft Teams.

Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação difere. Todos os arquivos são colocados em AppData.

Pasta:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho na área de trabalho:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

Registro:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Melhores Práticas

As recomendações de melhores práticas são baseadas nos cenários de caso de uso. Usar o Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para a sincronização eficiente dos dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as informações específicas do usuário apropriadas são armazenadas em cache durante a sessão do usuário. Por exemplo, as informações específicas do usuário incluem dados do usuário, perfil e configurações. Sincronize os dados nestas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

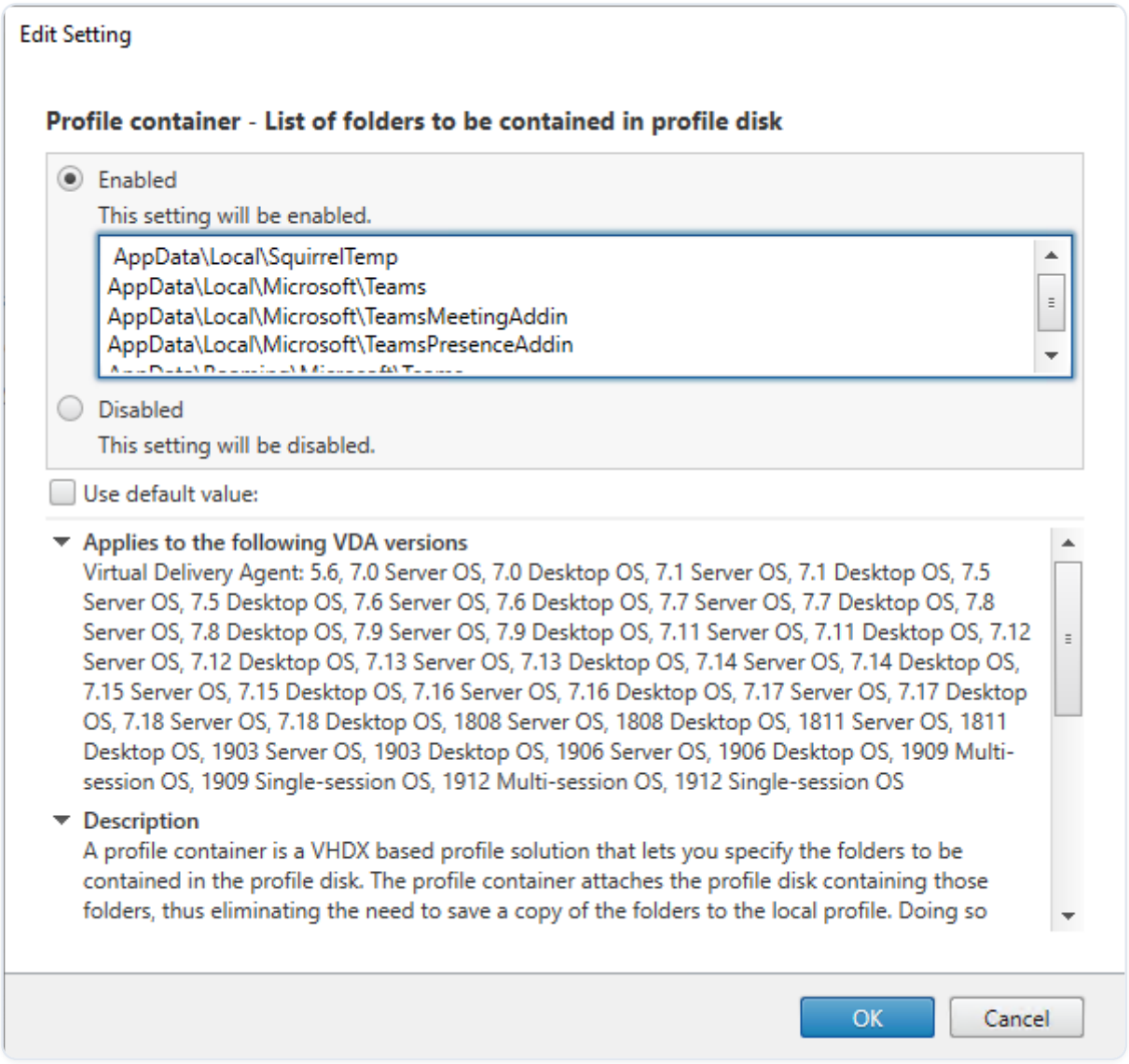
Lista de exclusão de conteúdo em cache do Microsoft Teams para configuração não persistente

Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams conforme descrito na documentação Microsoft. Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais sua configuração não persistente.

Caso de uso: cenário de sessão única

Nesse cenário, o usuário final usa o Microsoft Teams em um local por vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop, e o Microsoft Teams é implantado no desktop virtual como um aplicativo. Recomendamos habilitar o contêiner de perfil do Citrix e redirecionar os diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador do Microsoft Teams para toda a máquina (**ALLUSER=1**) na imagem dourada.
2. Habilite o Citrix Profile Management e configure o armazenamento de perfil de usuário com as permissões adequadas.
3. Habilite a seguinte configuração de política do Profile Management: **Sistema de arquivos > Sincronização > Contêiner de perfil – Lista de pastas a serem contidas no disco de perfil**.



Liste todos os diretórios por usuário nesta configuração. Você também pode configurar essas definições usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

Requisitos do sistema

Versão mínima recomendada - Delivery Controller (DDCs) 1906.2

Se você estiver usando uma versão anterior, consulte Habilitar otimização do Microsoft Teams:

Sistemas operacionais suportados:

- Windows Server 2022, 2019, 2016, 2012R2 Standard e edições de data center, e com a opção Server Core

Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais suportados:

- Windows 11
- Windows 10 de 64 bits, versões 1607 e posteriores. Aplicativos hospedados em VM são suportados no aplicativo Citrix Workspace para Windows 2109.1 e posteriores
- Windows Server 2022, 2019, 2016 e 2012 R2 (Edições Standard e Datacenter)

Requisitos:

- BCR_x64.msi - o MSI que inclui o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não o exclua.

Versão recomendada – Citrix Workspace app para Windows CR mais recente e Versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 e 64 bits, incluindo edições Embedded) (O suporte para Windows 7 foi interrompido na Versão 2006) (O suporte para Windows 8.1 foi interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas de processador (CPU) suportadas: x86 e x64 (ARM não é suportado).
- Requisito de endpoint: CPU dual-core de aproximadamente 2,2–2,4 GHz que pode suportar resolução HD de 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs dual ou quad-core com velocidades base mais baixas (~1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Thin Clients HP verificados: t630/t640, t730/t740, mt44/mt45.
- Thin Clients Dell verificados: 5070, 5470 Mobile TC e AIO.
- Thin Clients 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de endpoints verificados, consulte Thin Clients.
- O aplicativo Citrix Workspace requer pelo menos 600 MB de espaço em disco livre e 1 GB de RAM.
- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se ele não estiver presente no sistema.

Os administradores podem ativar/desativar o Microsoft Teams iniciando no modo otimizado, alterando a política de otimização do Microsoft Teams. Os usuários que iniciam no modo otimizado no aplicativo Citrix Workspace não podem desativar o Microsoft Teams.

Versão mínima - aplicativo Citrix Workspace 2006 para Linux

Para obter mais informações, consulte Otimização para Microsoft Teams na documentação do aplicativo Citrix Workspace 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
- `libnsl`
- Ubuntu 20.04 ou posterior

Aprimoramento de autenticação:

- Biblioteca Libsecret
- biblioteca libunwind-12. Para obter mais informações, consulte Adicionando a dependência da biblioteca libunwind-12 para llvm-12.

Hardware:

- CPU dual-core de no mínimo 1,8 GHz que suporte resolução HD de 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com velocidade base de 1,8 GHz e alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de endpoints verificados, consulte Thin Clients.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode 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. Após a conclusão da atualização, reinicie a Sessão. (É necessária permissão de root).

Versão mínima - aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais suportados:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e posterior.
- macOS Monterey.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Nota:**

> O aplicativo Citrix Viewer requer acesso às preferências de Segurança e Privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram esta preferência em **menu Apple > Preferências do Sistema > Segurança e Privacidade > guia Privacidade > Gravação de tela** e selecionam **Citrix Viewer**.

> A otimização do Microsoft Teams funciona por padrão com o aplicativo Citrix Workspace 2012 e posterior e macOS 10.15.

Se você quiser desabilitar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versão mínima - Versão mais recente do aplicativo Citrix Workspace para ChromeOS executando na versão mais recente do ChromeOS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core 2.4 GHz.

Recursos suportados:

- Áudio
- Vídeo

- Otimização de compartilhamento de tela (entrada e saída) - desabilitada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de Servidor Único

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) podem ser suportados em um único host físico. Isso é comumente referido como Escalabilidade de Servidor Único (SSS) do Citrix Virtual Apps and Desktops. No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade de usuário. A ideia é descobrir quantos usuários ou VMs podem ser executados em uma única peça de hardware executando um hypervisor principal.

> **Nota:**
>
> Esta seção inclui orientações para estimar o SSS. As orientações são de alto nível e podem não ser necessariamente específicas para sua situação ou ambiente exclusivo. A única maneira de realmente entender o SSS do Citrix Virtual Apps and Desktops é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda usar estas orientações e estas regras simples apenas para estimar rapidamente o SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar hardware ou tomar qualquer decisão financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2,60 GHz (Turbo máximo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- Armazenamento SSD local RAID 0 (11 discos) 6 TB

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

Terminologia

- Carga de trabalho de trabalhador do conhecimento: Inclui Acrobat Reader, Freemind/Java, Visualizador de fotos, Edge e aplicativos do MS Office, como Excel, Outlook, PowerPoint e Word.
- Linha de base: Testes de escalabilidade de servidor executados com carga de trabalho de trabalhador do conhecimento (sem Microsoft Teams).
- Carga de trabalho do Microsoft Teams: Carga de trabalho típica de trabalhador do conhecimento + Microsoft Teams.

Como o Microsoft Teams é testado sob estresse

- O Microsoft Teams é otimizado com HDX. Assim, todo o processamento multimídia é descarregado para o endpoint ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou encerrados antes do início da carga de trabalho.
- Abrir o Microsoft Teams (Inicialização a frio).
- Medir o tempo que o Microsoft Teams leva para carregar e focar na janela principal do Microsoft Teams.
- Alternar para a janela de chat usando atalhos de teclado.
- Alternar para a janela do calendário usando atalhos de teclado.
- Enviar a mensagem de chat para um usuário específico usando atalhos de teclado.
- Alternar para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- Impacto de 40% na escalabilidade com a Carga de Trabalho do Microsoft Teams (81 usuários), em comparação com a Linha de Base (137 usuários).
- Aumentar a capacidade do servidor em ~40% (em CPU) restaura o número de usuários como na carga de trabalho de Linha de Base.
- 20% de memória extra necessária com a Carga de Trabalho do Microsoft Teams, em comparação com a Linha de Base.
- Aumentar o tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% nas gravações de IOPS, aumento de ~100% nas leituras de IOPS. O Microsoft Teams pode ter um impacto significativo em um ambiente com armazenamento mais lento.

Matriz de recursos e suporte de versão

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA MAC (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA LINUX (VERSÃO MÍNIMA)	APLICATIVO CITRIX WORKSPACE PARA CHROME OS (VERSÃO MÍNIMA)
Áudio/Vídeo (P2P e conferência)	versão atual menos 90 dias	1906	1907	2009	2004	2105.5
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	2012	2006	2105.5
i. Borda vermelha do indicador de tela	Versão atual menos 90 dias	1906	2002	2012	2006	Não
ii. Limitar a captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	2012	2006	Não
iii. Vários monitores	Versão atual menos 90 dias	1912 CU6+	2106 (1)	2106	2106	Não
DTMF	Versão atual	N/A	2102	2101	2101	2111.1

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP 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 (VERSÃO MÍNIMA)
	menos 90 dias					
Suporte a Servidor Proxy	Versão atual menos 90 dias	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Compartilhamento de apps	Versão atual menos 90 dias	2109	2109.1	2203.1	2209	Não
Legendas ao Vivo	Versão atual menos 90 dias	N/A (4)	2109.1	2109	2109	2303
e911 Dinâmico	Versão atual menos 90 dias	N/A	2112.1	2112	2112	2112
Conceder Controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	Não	Não
Solicitar Controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	2203	2303

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP 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 (VERSÃO MÍNIMA)
MultiWindow	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Transcrições de Reunião	Versão atual menos 90 dias	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Desfoque de Plano de Fundo	Versão atual menos 90 dias	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer apenas no modo de tela cheia. SHIFT+F2 não é suportado.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, as Legendas ao Vivo só funcionarão se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 Linux ou 2112 para Windows. Isso ocorre porque as Legendas ao Vivo se comportam de forma diferente se o Microsoft Teams estiver no modo de interface do usuário de Janela Única ou no modo MultiJanela.
5. O MultiWindow foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

Nota:

- Todos os recursos listados em **Citrix Workspace app para Windows 1912 CU6 (ou posterior)** são aplicáveis ao Citrix Workspace app para Windows 2203.1 LTSR CU1.
- A Microsoft descontinuou o suporte para o modo de Janela Única no Microsoft Teams. Para cumprir, você deve atualizar seu VDA para 1912 CU6+ LTSR e o aplicativo Citrix Workspace 2203 CU2+ ou superior, que suporta o modo MultiJanela.

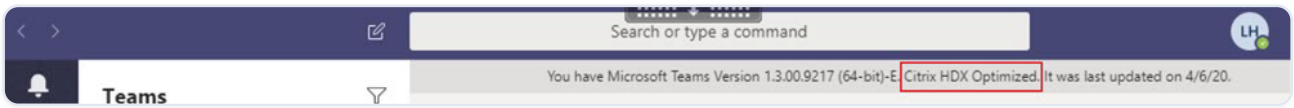
Habilitar otimização do Microsoft Teams

Para habilitar a otimização para o Microsoft Teams, use a política Gerenciar descrita na política Redirecionamento do Microsoft Teams. Esta política está **ATIVADA** por padrão. Além de esta política estar habilitada, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima exigida. Se você habilitou a política e a versão do aplicativo Citrix Workspace é compatível,
HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport é definido como **1** automaticamente no VDA. O Microsoft Teams lê a chave para carregar no modo VDI.

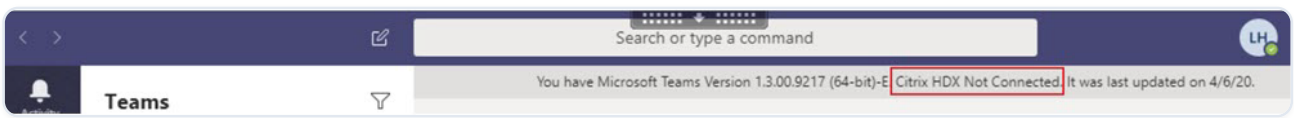
Nota:

Se você estiver usando VDAs versão 1906.2 ou posterior ou com versões de controlador mais antigas (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda pode ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

Se você clicar em **Sobre > Versão**, a legenda **Citrix HDX Optimized** será exibida:

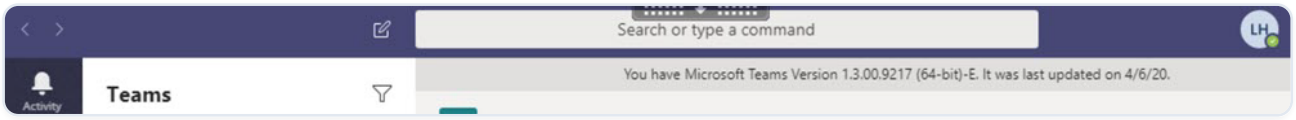


Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro nas partes posteriores da pilha. O erro provavelmente está nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, o Microsoft Teams falhou ao carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito do mouse no ícone da área de notificação e

reiniciando. Certifique-se de que a política Gerenciar não esteja definida como **Proibida** e que a versão do aplicativo Citrix Workspace seja compatível.



Importante: reconexões de sessão

- Pode ser necessário reiniciar o Microsoft Teams para obter uma sessão otimizada por HDX quando sua conectividade mudar. Por exemplo, se você estiver migrando de um endpoint não compatível (aplicativo Workspace para iOS, Android ou versões antigas de Windows/Linux/Mac) para um compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou vice-versa.
- Uma reinicialização do Microsoft Teams também é necessária se você instalou o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações VDI persistentes. Nesses casos, o Microsoft Teams pode ser atualizado automaticamente enquanto a sessão HDX está no estado desconectado. Assim, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado de forma otimizada.
- Ao migrar de uma sessão local para uma sessão HDX, você deve reiniciar o Microsoft Teams para otimizar com HDX. Esta ação é necessária em um cenário de Acesso Remoto a PC.

Requisitos de rede

O Microsoft Teams depende de servidores Media Processor no Microsoft 365 para reuniões ou chamadas multipartidárias. Além disso, o Microsoft Teams depende dos Microsoft 365 Transport Relays para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Portanto, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Consulte Princípios de conectividade de rede do Microsoft 365 para obter diretrizes detalhadas sobre o planejamento de rede.

Recomendamos avaliar seu ambiente para identificar quaisquer riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem. Use a Ferramenta de Avaliação de Rede do Skype for Business para testar se sua rede está pronta para o Microsoft Teams. Para obter informações de suporte, consulte Suporte.

Resumo das principais recomendações de rede para tráfego de Protocolo de Tempo Real (RTP)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir do escritório da filial.
- Planeje e forneça largura de banda suficiente no escritório da filial.
- Verifique a conectividade e a qualidade da rede em cada escritório da filial.
- Se você precisar usar qualquer um dos seguintes na filial, certifique-se de que o tráfego RTP/UDP (tratado por HdxRtcEngine.exe no aplicativo Citrix Workspace) não seja impedido.
    - Ignorar servidores proxy
    - Interceptação SSL de rede
    - Dispositivos de inspeção profunda de pacotes
    - Hairpins de VPN (use tunelamento dividido, se possível)

> **Importante: Configuração de tunelamento dividido de VPN**

> O tráfego HdxRtcEngine.exe deve ser desviado do túnel VPN e permitido usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira como isso é realizado depende do produto VPN e da plataforma da máquina usada, mas a maioria das soluções VPN permite uma configuração simples de política para aplicar essa lógica. Para obter mais informações sobre a orientação de túnel dividido específica da plataforma VPN, consulte este artigo da Microsoft.

> O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o Protocolo de Transporte Seguro em Tempo Real (SRTP) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para este recurso, chaves simétricas (negociadas com DTLS) são usadas para criptografar mídia e mensagens de controle usando a cifra de criptografia AES.

As seguintes métricas são recomendadas para uma experiência de usuário positiva:

MÉTRICA	PONTO DE EXTREMIDADE PARA MICROSOFT 365
Latência (sentido único)	< 50 ms
Latência (RTT)	< 100 ms
Perda de Pacotes	<1% durante qualquer intervalo de 15s
Jitter de interchegada de pacotes	<30ms durante qualquer intervalo de 15s

Para obter mais informações, consulte Prepare a rede da sua organização para o Microsoft Teams.

Para requisitos de largura de banda, a otimização para Microsoft Teams pode usar uma ampla variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam esses codecs durante o processo de estabelecimento da chamada usando o Protocolo de Descrição de Sessão (SDP) Oferta/Resposta. As recomendações mínimas da Citrix por usuário são:

TIPO	LARGURA DE BANDA	CODEC
Áudio (em cada sentido)	Cerca de 90 kbps	G.722
Áudio (em cada sentido)	Cerca de 60 kbps	Opus*
Vídeo (em cada sentido)	Aproximadamente 700 kbps	H264 360p a 30 quadros por segundo 16:9
Compartilhamento de tela	Aproximadamente 300 kbps	H264 1080p a 15 quadros por segundo

* O Opus suporta codificação de taxa de bits constante e variável de 6 kbps até 510 kbps.

Opus e H264 são os codecs preferenciais para chamadas ponto a ponto e de conferência.

> **Importante:**

> Sobre desempenho, a codificação é mais cara que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix

> Workspace para Linux e Windows. Consulte Estimador de desempenho do codificador e Otimização para Microsoft Teams.

Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

  Se você configurar um servidor proxy explícito no VDA e rotear as conexões para localhost através de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Ignorar servidores proxy para endereços locais** em **Opções da Internet > Conexões > Configurações de LAN > Servidores Proxy** e ignorar `127.0.0.1:9002`.

  Se você usar um arquivo PAC, seu script de configuração de proxy do VDA do arquivo PAC deve retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

  Se a filial estiver configurada para acessar a internet através de um proxy, estas versões suportam servidores proxy:

  - Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
  - Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler as configurações de proxy. Esses dispositivos enviam tráfego diretamente para os servidores TURN do Microsoft 365.

> **Importante:**

- Verifique se o dispositivo cliente pode se conectar ao servidor DNS para fazer resoluções DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor de retransmissão do Microsoft Teams:
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

Se as solicitações DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e as chamadas em conferência com o estabelecimento de mídia falharão.

- A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não do cliente).

Estabelecimento de chamadas e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão direta de rede Secure Real-time Transport Protocol (SRTP) sobre User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia retorna para TCP/TLS 443.

O mecanismo de mídia HDX oferece suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal Using Relays around NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Esse suporte significa que o endpoint deve ser capaz de realizar resoluções DNS.

Considere um cenário em que não há um caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está participando de uma chamada ou reunião multipartidária. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP de sub-rede do Microsoft 365 e quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver

bloqueado). Para obter mais informações, consulte o diagrama de arquitetura em Configuração de chamada e URLs e intervalos de endereços IP do Office 365 ID 11.

ID	CATEGORIA	ENDEREÇOS	PORTAS DE DESTINO
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (alternativa)

Esses intervalos incluem tanto os Transport Relays quanto os processadores de mídia, com um Azure Load Balancer como front-end. Os Transport Relays do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são endpoints ICE. Além disso, os Transport Relays do Microsoft Teams não encerram mídia, TLS ou realizam qualquer transcodificação. Eles podem fazer a ponte de TCP (se HdxRtcEngine.exe usar TCP) para UDP ao encaminhar tráfego para outros pares ou processadores de mídia.

O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com o Transport Relay do Microsoft Teams mais próximo na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e as portas UDP 3478–3481 (portas UDP diferentes por carga de trabalho, embora a multiplexação possa ocorrer) ou TCP/TLS 443 para alternativas. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado em vez do TCP, aconselhamos que você projete suas redes para acomodar o tráfego UDP no escritório remoto.

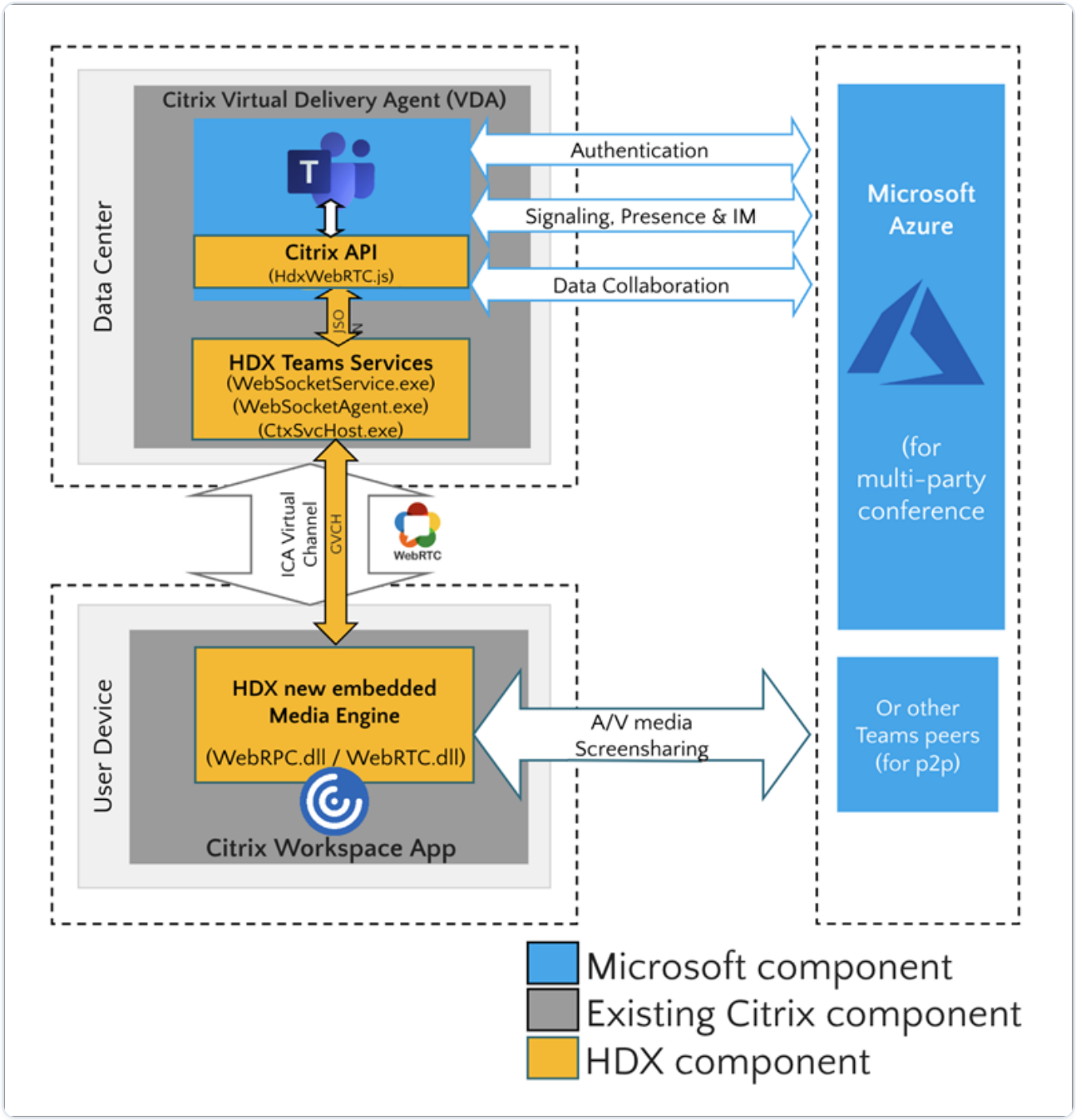
Se o Microsoft Teams for carregado no modo otimizado e HdxRtcEngine.exe estiver em execução no endpoint, falhas de ICE podem causar uma falha na configuração da chamada ou áudio/vídeo apenas unidirecional. Quando uma chamada não pode ser concluída ou os fluxos de mídia não são full duplex, verifique primeiro o **rastreamento do Wireshark** no endpoint. Para obter mais informações sobre o processo de coleta de candidatos ICE, consulte "Coleta de logs" na seção Suporte.

> **Nota:**
>
> Se os endpoints não tiverem acesso à internet, os usuários ainda poderão fazer uma chamada ponto a ponto se ambos estiverem na mesma LAN. As reuniões falham. Nesse caso, há um tempo limite de 30 segundos antes que a configuração da chamada comece.

Configuração da chamada

Use este diagrama de arquitetura como referência visual para a sequência do fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.

Arquitetura



1. Iniciar o Microsoft Teams.
2. O Microsoft Teams autentica-se no O365. As políticas de locatário são enviadas para o cliente do Microsoft Teams, e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.

3. O Microsoft Teams detecta que está sendo executado em um VDA e faz chamadas de API para a API JavaScript da Citrix.
4. O JavaScript da Citrix no Microsoft Teams abre uma conexão WebSocket segura para o WebSocketService.exe em execução no VDA, que gera o WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico chamando o Serviço de Redirecionamento do Microsoft Teams HDX da Citrix (CtxSvcHost.exe).
6. O wfica32.exe (mecanismo HDX) do aplicativo Citrix Workspace gera um novo processo chamado HdxRtcEngine.exe, que é o novo mecanismo WebRTC usado para otimização do Microsoft Teams.
7. O mecanismo de mídia da Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem começar a processar solicitações multimídia.

   -----Chamadas do usuário------

8. **Par A** clica no botão **chamar**. O Teams.exe se comunica com os serviços do Microsoft Teams no Microsoft 365, estabelecendo um caminho de sinalização de ponta a ponta com o **Par B**. O Microsoft Teams solicita ao HdxRtcEngine uma série de parâmetros de chamada suportados (codecs, resoluções e assim por diante, o que é conhecido como uma oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são então retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e, de lá, para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização, e as verificações de conectividade ICE (travessia de NAT e Firewall usando solicitações de ligação STUN) são concluídas. Em seguida, a mídia Secure Real-time Transport Protocol (SRTP) flui diretamente entre HdxRtcEngine.exe e o outro par (ou servidores de conferência do Microsoft 365, se for uma reunião).

Sistema Telefônico da Microsoft

O Phone System é a tecnologia da Microsoft que permite o controle de chamadas e PBX na nuvem do Microsoft 365 com o Microsoft Teams. A otimização para Microsoft Teams suporta o Phone System, usando Planos de Chamada do Microsoft 365 ou Roteamento Direto. Com o Roteamento Direto, você pode conectar seu próprio controlador de borda de sessão compatível diretamente ao Microsoft Phone System sem nenhum software local adicional. Filas de chamadas, transferência, encaminhamento, espera, mudo e retomada de uma chamada são suportados.

DTMF

O recurso de multifrequência de tom duplo (DTMF) é suportado com estas versões do aplicativo Citrix Workspace (e posteriores):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para ChromeOS versão 2111.1

Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace suporta chamadas de emergência dinâmicas. Quando usado em Planos de Chamada da Microsoft, Operator Connect e Roteamento Direto, ele permite que você faça o seguinte:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace que é executado no endpoint, em vez do cliente Microsoft Teams que é executado no VDA.

A lei de Ray Baum exige que a localização despachável do chamador do 911 seja transmitida para o Ponto de Atendimento de Segurança Pública (PSAP) apropriado. A Otimização do Microsoft Teams com HDX está em conformidade com a lei de Ray Baum quando usada com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Linux versão 2112 e posterior
- Aplicativo Citrix Workspace para Mac versão 2112 e posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2112 e posterior

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de rede ou de localização de emergência:

- Configurações de rede
- Serviço de Informações de Localização (LIS)

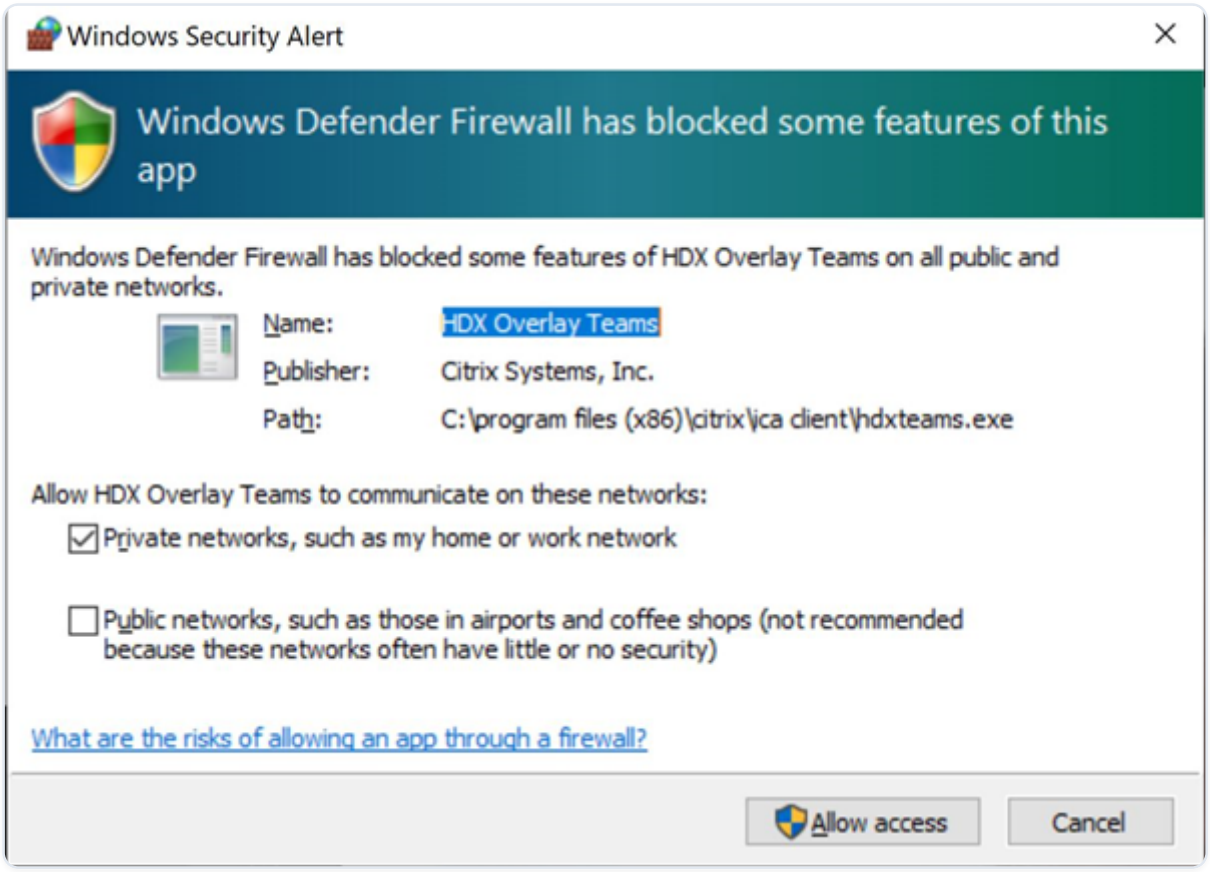
Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de localização despachável que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

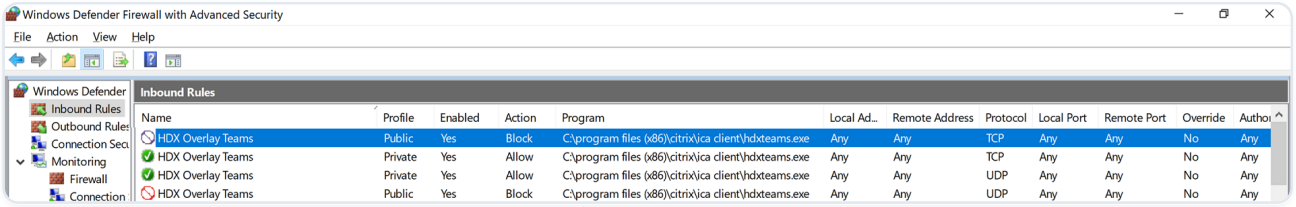
- ID do Chassi / ID da Porta usando o Protocolo de Descoberta da Camada de Link (LLDP) para conexões Ethernet/Switch. Ethernet/Switch (LLDP) é suportado em:
  - Versões do Windows 8.1 e 10
  - macOS, que requer software de habilitação LLDP. Para baixar o software de habilitação LLDP, vá para `www.microsoft.com` e procure por software de habilitação LLDP.
  - Linux, que requer que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do Thin Client.
- BBSID WLAN e {IPv4-IPv6; Sub-rede; Endereço MAC} do endpoint onde o aplicativo Citrix Workspace está instalado.
  - Locais baseados em sub-rede e WiFi são suportados no aplicativo Workspace para Windows, Linux e Mac.
- Latitude e Longitude, se a permissão do usuário for concedida no nível do sistema operacional onde o aplicativo Citrix Workspace está instalado (a permissão é definida como HDX RTC Engine)
  - Compatível com todas as plataformas do aplicativo Workspace. No entanto, para o Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do sistema operacional do Thin Client (>sudo apt-get install libgps23 gpsd lldpd).

Considerações sobre firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso nas configurações do **firewall do Windows**. O aviso pede aos usuários que permitam a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Windows Defender Firewall > Segurança Avançada**. Você pode aplicar regras mais restritivas se desejar.



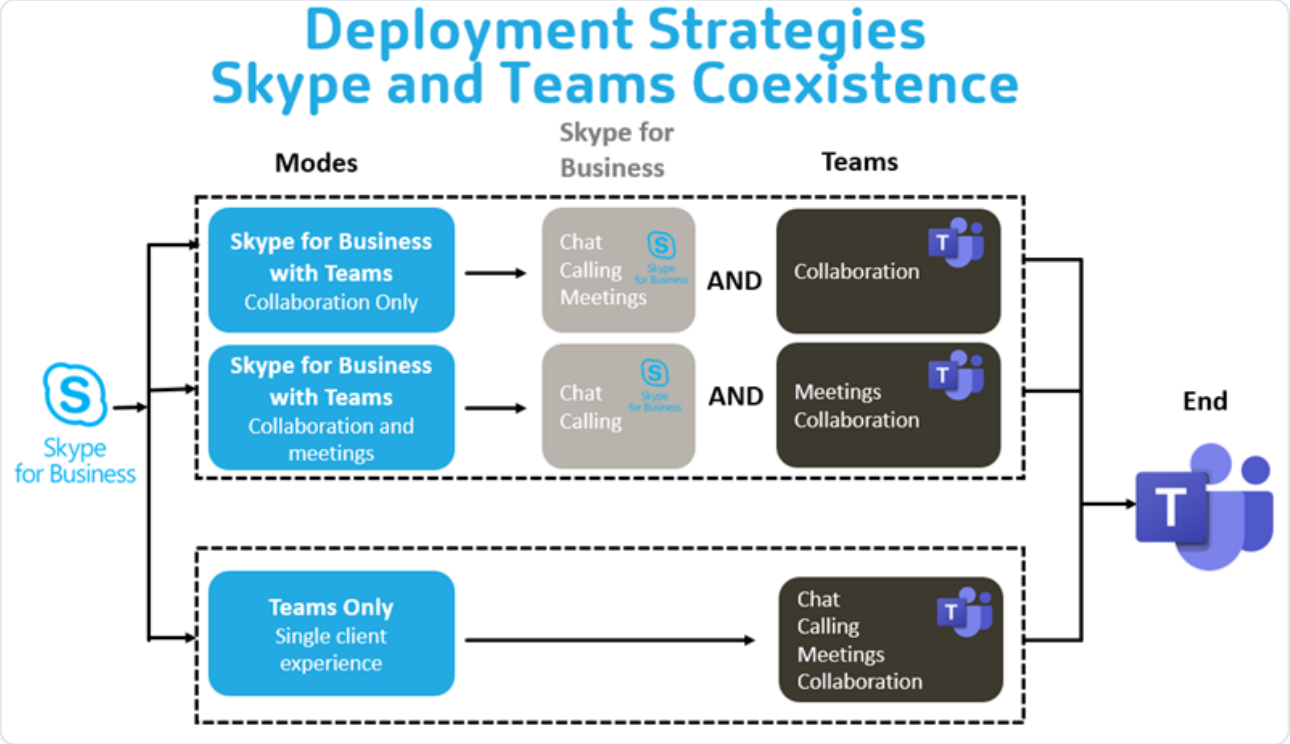
Coexistência do Microsoft Teams e do Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado como duas soluções separadas com recursos sobrepostos. Para obter mais informações, consulte Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para mecanismos multimídia do Microsoft Teams, então, respeitam a configuração definida em seu ambiente. Os exemplos incluem modos de ilha e Skype for Business com colaboração do Microsoft Teams. Além disso, Skype for Business com colaboração e reuniões do Microsoft Teams.

O acesso a periféricos pode ser concedido a apenas um aplicativo por vez. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem

durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



Citrix SD-WAN™: conectividade de rede otimizada para o Microsoft Teams

A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio e vídeo do Microsoft Teams de usuários do Citrix Workspace app em filiais para um data center antes de ir para a internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço web do Microsoft 365 baseado em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

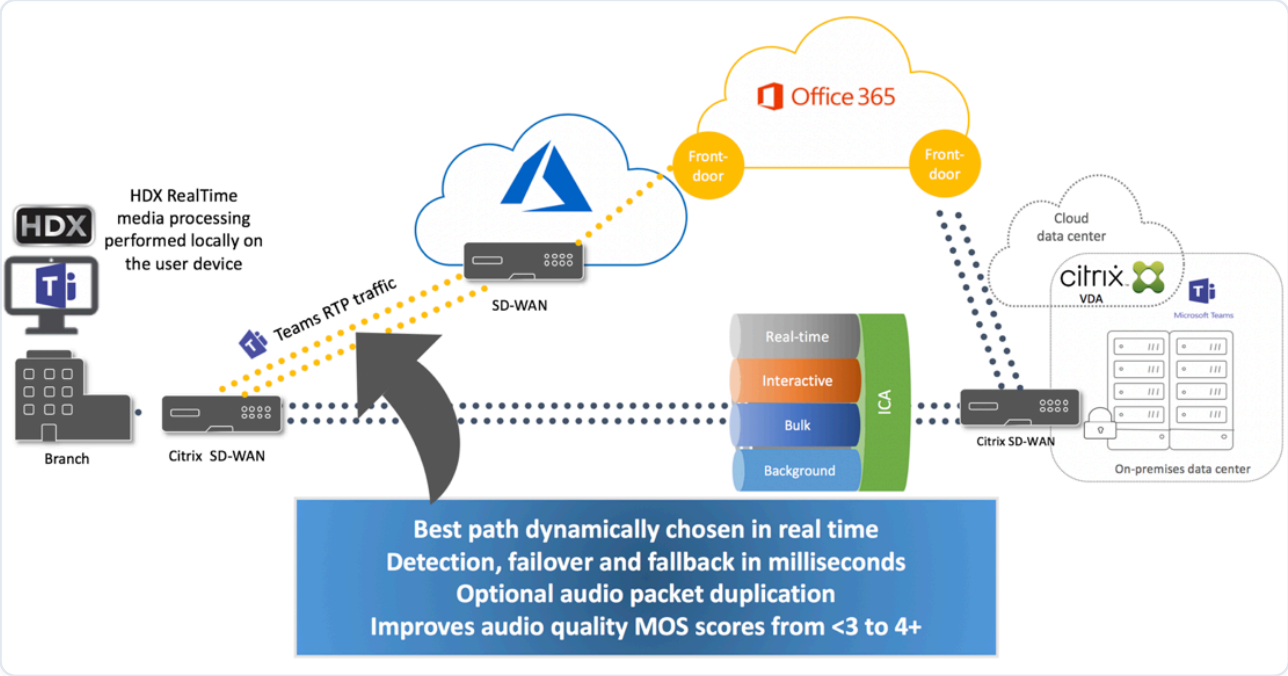
As conexões de internet banda larga empresarial em muitas áreas sofrem com perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio e vídeo do Microsoft Teams quando a integridade da rede é variável ou degradada.

- Se você usa o Microsoft Azure, um appliance virtual Citrix SD-WAN (VPX) implantado na VNET do Azure oferece otimizações avançadas de conectividade. Essas otimizações incluem failover de link contínuo e corrida de pacotes de áudio.

- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud™ Direct. Este serviço oferece entrega confiável e segura para todo o tráfego destinado à internet.

Se a qualidade da conexão de internet da filial não for uma preocupação, pode ser suficiente minimizar a latência. Direcione o tráfego do Microsoft Teams diretamente do appliance de filial do Citrix SD-WAN para o front door mais próximo do Microsoft 365 para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo em várias janelas

Você pode usar várias janelas de reunião ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Janelas Pop-Out do Microsoft Teams para Bate-papos e Reuniões no site do Microsoft 365.

Nota:

Este recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Ele requer VDA 2112 ou superior e foi retroportado para 1912 CU6+ LTSR.

Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 oferece suporte a desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas, ajudando a conversa a permanecer focada na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas P2P ou de conferência.

> **Nota:**
>
> Este recurso é integrado à interface do usuário/botões do Microsoft Teams. O suporte a MultiWindow é um pré-requisito que exige uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte Reuniões e bate-papo em várias janelas.
>
> Os controles da interface do usuário do Microsoft Teams para desfoque e efeitos de fundo exigem as seguintes versões mínimas:

- Aplicativo Citrix Workspace para Windows 2207
- Aplicativo Citrix Workspace para Mac 2301
- Aplicativo Citrix Workspace para Linux 2307
- Aplicativo Citrix Workspace para ChromeOS 2303

Limitações:

- O cliente deve estar conectado à internet ao substituir a imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição de imagem de fundo definida pelo administrador e pelo usuário não é suportada na interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser configuradas usando as configurações no cliente, se a imagem também estiver armazenada no cliente.

Definindo uma imagem de fundo personalizada

As seguintes chaves de registro são necessárias apenas se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso, ou se um administrador deseja substituir comportamentos padrão. Por exemplo, desativar o desfoque de fundo porque o endpoint não é potente o suficiente.

No Windows

Para definir uma imagem de fundo personalizada, administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou endpoint:

Local: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição de imagem de fundo)

Um valor definido como 1 desfoca o plano de fundo. O usuário final ou o administrador pode definir esse valor.

O valor definido como 2 também exige que a chave **VideoBackgroundImage** esteja presente. Somente o administrador pode definir este valor. A seguinte chave é necessária apenas se você deseja substituir a imagem de fundo e não para desfoque:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: my_image_name.jpeg

A imagem de fundo do vídeo deve estar presente no diretório `C:\Program Files (x86)\Citrix\ICA Client`.

Essa configuração de registro também pode ser usada para habilitar o desfoque de fundo ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de UI do Microsoft Teams. Em outras palavras, se seu ambiente ou VDA não suportar várias janelas, você ainda pode aplicar a solução alternativa de registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações na chave do registro só entram em vigor quando a sessão HDX se conecta.

No Mac

Local da imagem baixada pelo usuário: */Users/username/Downloads/any_image.png*

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

`defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"`

No Linux

Local da imagem baixada pelo usuário: */home/username/Downloads/any_image.jpg*

Crie o arquivo */var/.config/citrix/hdx_rtc_engine/config.json* e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

No HTML5

1. navegar até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. Salve as alterações.

Considerações sobre o consumo de CPU do cliente

Embora o recurso de desfoque seja econômico em termos de CPU, você pode esperar um aumento no consumo. Por exemplo, em um thin client com um chip Intel® Pentium® Silver de 4 núcleos, 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

Visualização de galeria e oradores ativos no Microsoft Teams

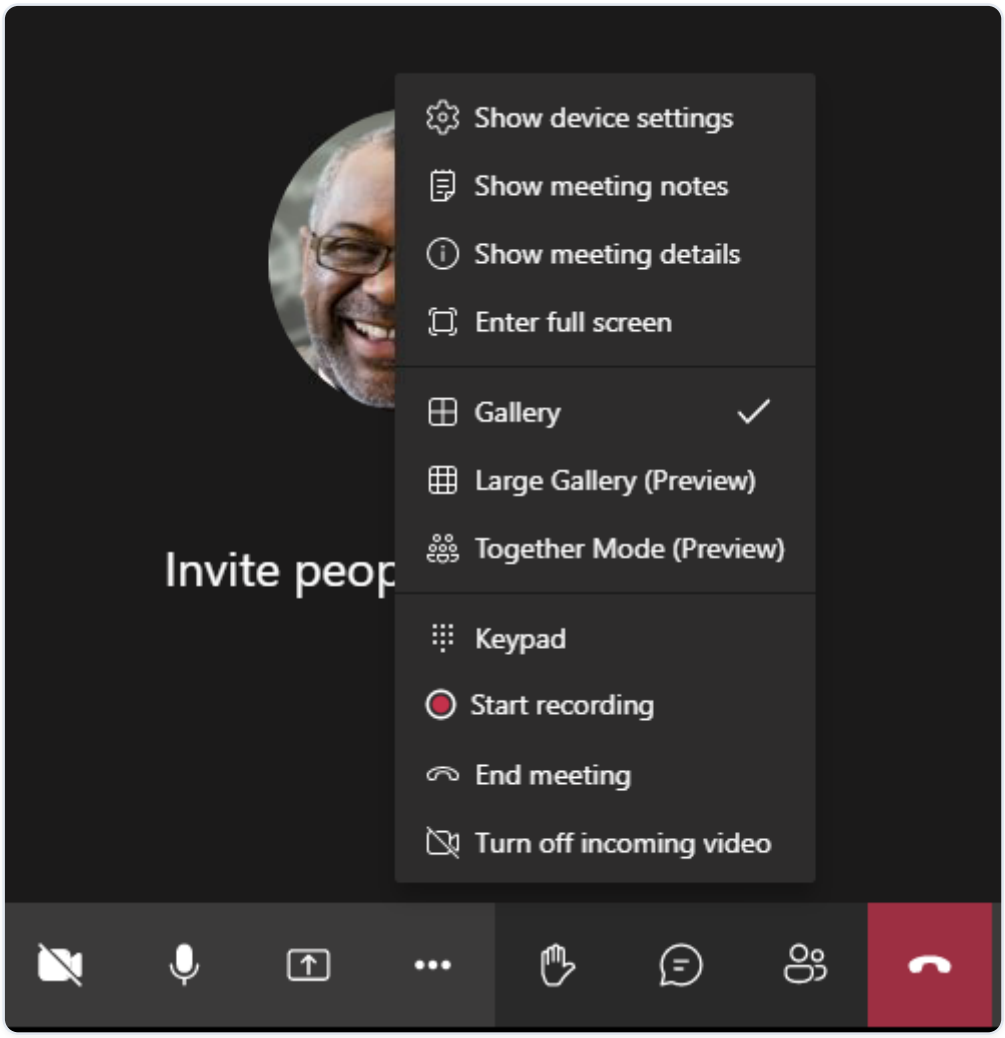
O Microsoft Teams oferece suporte aos layouts **Galeria**, **Galeria grande** e **Modo Juntos**.

O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecida como **Galeria**). Neste caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham um vídeo, apenas os quatro últimos oradores mais ativos aparecem na tela.

O Microsoft Teams também oferece a visualização de galeria grande com uma grade de até 7x7. Como resultado, o servidor de conferência do Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Este feed único, estilo matriz, também pode incluir vídeos de auto-visualização dos usuários.

Por fim, o Microsoft Teams oferece suporte ao **Modo Juntos**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para posicionar digitalmente os participantes em um plano de fundo compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada de conferência selecionando os layouts **Galeria**, **Galeria grande** ou **Modo Juntos** no menu de reticências.



Suporte para restrições de proporção de vídeo (aplicativo Citrix Workspace para Windows 2102, aplicativo Citrix Workspace para Linux 2106, aplicativo Citrix Workspace para MAC 2106 e posterior):

- A opção **Preencher para enquadrar** está disponível na Visualização de Galeria/Galeria Grande. Esta opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts de Galeria e Galeria Grande:

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
Layout / Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro oradores mais ativos aparecem na tela e outros	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
	participantes não aparecem na grade.	
Técnica de mixagem	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central mixa e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Essa ação introduz alguma latência adicional.
Orador ativo	O novo orador ativo substitui o orador menos ativo na grade.	Exibe todos os participantes independentemente de estarem ativos ou inativos.
Codificação no endpoint	Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no endpoint	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no endpoint pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo para áudio e vídeo. Essa configuração reduz o consumo de CPU no endpoint.
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é de 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando	720p para o layout composto ou mixagem. Não há necessidade de um fluxo de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
	vídeo, a resolução por feed de vídeo pode ser maior.	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. Este fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com condição de rede ruim afeta a qualidade para todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência oferece diferentes qualidades com base nas condições de rede dos participantes individuais.
Pré-visualização	Exibe você em uma pequena miniatura em tempo real.	Exibe você em miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout de vídeo principal com algum atraso adicional.

Compartilhamento de tela no Microsoft Teams

O Microsoft Teams depende do compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho compartilhada com codecs de vídeo como H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do Citrix Workspace app 2109 ou superior para Windows, Linux, Mac, e Citrix Workspace app 2303 para ChromeOS, os usuários podem compartilhar suas telas e câmera de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera será pausado. Em

vez disso, o feed de vídeo de compartilhamento de tela é exibido. O colega deve então retomar manualmente o compartilhamento da câmera.

Observação para o PowerPoint Live

Esta limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros participantes ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para revisar outros slides. Neste cenário, os slides são renderizados no VDA. Para acessar um conjunto de slides do PowerPoint Live, clique no botão 'Share tray' e selecione um dos slides sugeridos do PowerPoint, ou clique em 'Browse' e encontre um arquivo do PowerPoint em seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Qualquer aplicativo local que se sobreponha ao Desktop Viewer não é capturado.

Nota

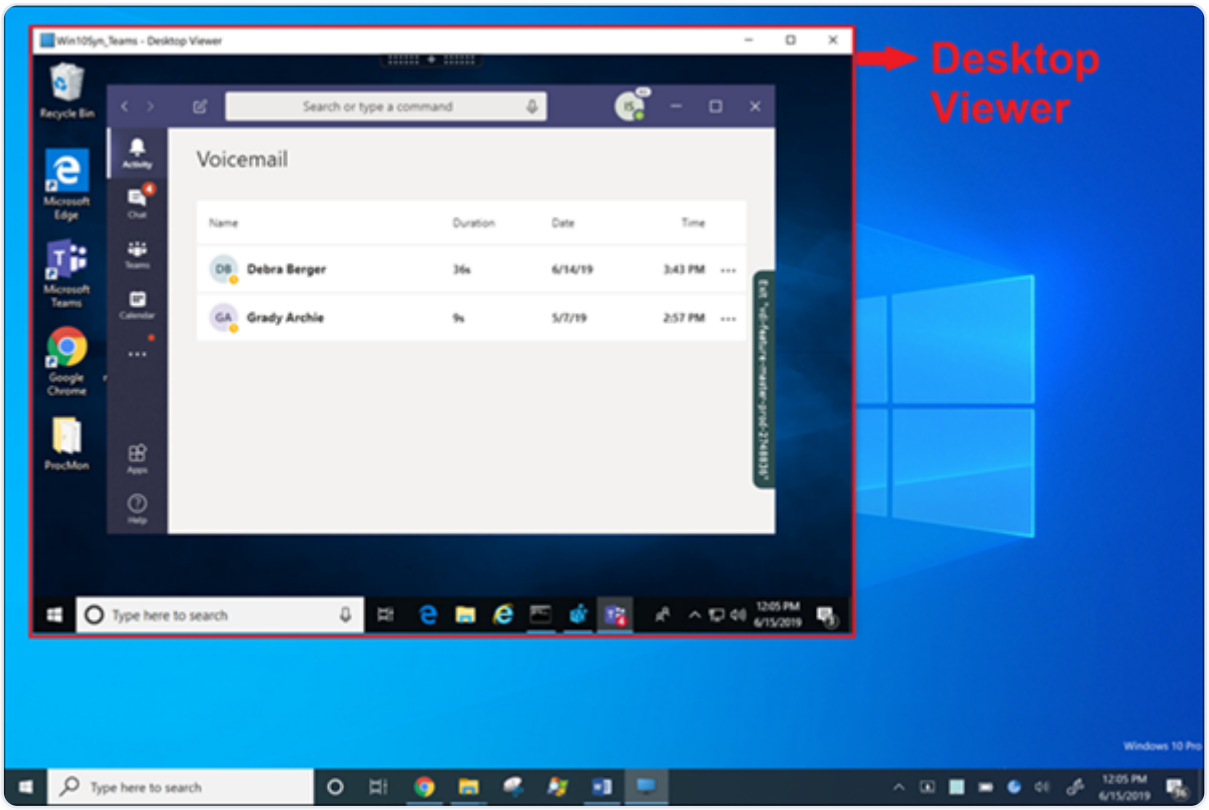
Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

Limitação conhecida:

- Se o Desktop Viewer estiver desabilitado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desabilitado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela em vários monitores.
- Em versões do aplicativo Workspace anteriores a 2106, apenas o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor principal para que os outros participantes da chamada possam vê-lo.
- O compartilhamento de tela em vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout de monitor virtual (partição lógica de um

único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.

- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento é possível apenas se o aplicativo local for sobreposto ao Desktop Viewer. Esse comportamento foi removido nas versões 2009.6 ou superior, e 1912 CU5 ou superior.
- Durante o compartilhamento de tela, se você mudar do modo janela para tela cheia, o compartilhamento de tela para. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.
- Não é possível fixar os Controles de Compartilhamento em um local específico no Microsoft Teams Otimizado.
- Ao compartilhar um aplicativo minimizado, a barra de título do aplicativo também pode ser compartilhada.



Compartilhamento de tela de aplicativo contínuo:

Se você estiver publicando o Microsoft Teams como um aplicativo autônomo e contínuo, o compartilhamento de tela capturará a área de trabalho local do seu endpoint físico. É necessária a versão mínima 1909 do aplicativo Citrix Workspace.

Compartilhamento de apps

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

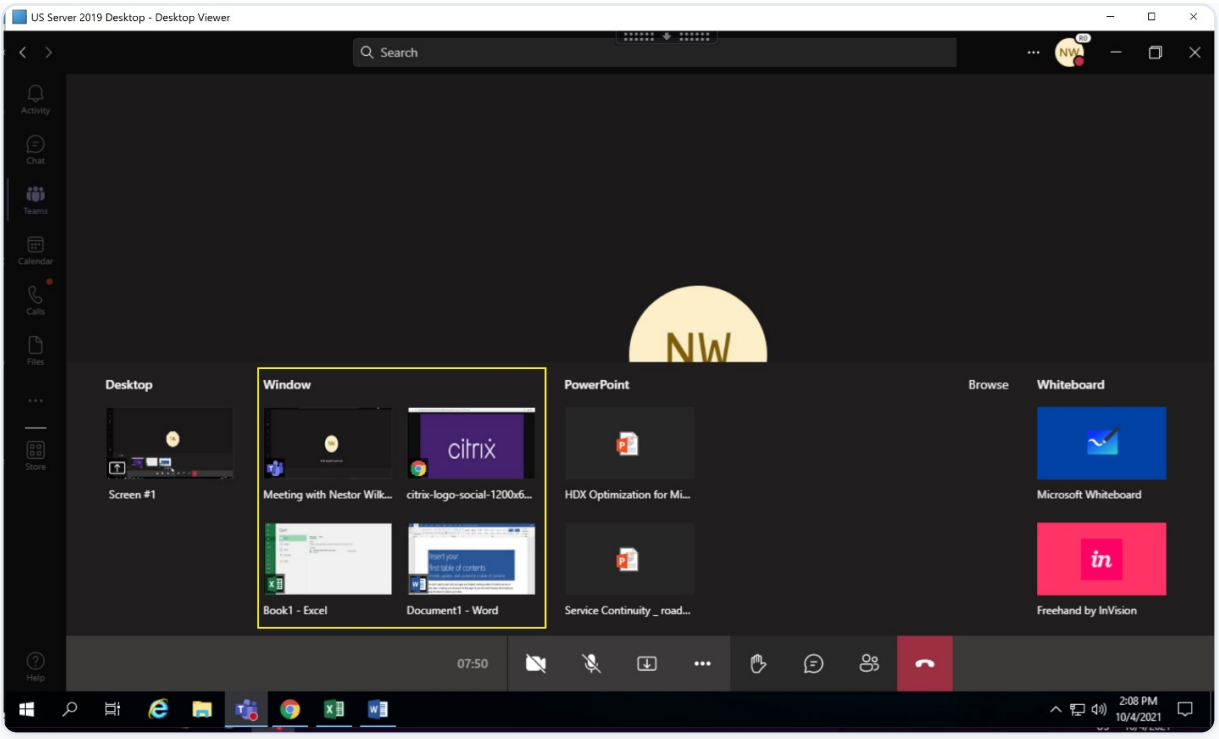
A partir do aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Você também pode compartilhar aplicativos internos personalizados, como Java, usando o Microsoft Teams otimizado. Para compartilhar um aplicativo específico:

1. navegar para o aplicativo Microsoft Teams dentro da sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo selecionado e os participantes da chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desabilitar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`: Nome: `UseWsProvider` Tipo: `DWORD` Valor: 0

> **Nota:**
>
> - Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
> - O compartilhamento de tela depende da captura da janela pelo lado do VDA. O conteúdo é então retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para o participante ou servidor de conferência.



Limitações conhecidas com o compartilhamento de tela de aplicativos específicos:

- O ponteiro do mouse não fica visível ao compartilhar a tela de um aplicativo.
- Se você minimizar um aplicativo enquanto o estiver compartilhando, apenas o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até que você maximize o aplicativo.
- Aplicativos LAA mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de desktop no Microsoft Teams otimizado no VDA. No entanto, ao selecionar o aplicativo da lista, o resultado pode não ser o esperado.

Compatibilidade com a proteção de aplicativos O compartilhamento de tela de um aplicativo específico é compatível com o recurso de proteção de aplicativos no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico se tiver iniciado o aplicativo ou a área de trabalho de um grupo de entrega que tenha a proteção de aplicativos ativada.

Ao clicar em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Desktop**. Você só pode selecionar a opção **Janela** para compartilhar qualquer aplicativo aberto.

> **Nota:**

> Ao iniciar aplicativos ou áreas de trabalho de um grupo de entrega com proteção de aplicativo ativada, você não consegue ver o vídeo ou o compartilhamento de tela de entrada se estiver usando o aplicativo Citrix Workspace para Windows 2202 ou anterior.

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 ou posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 ou posterior
- Aplicativo Citrix Workspace para Linux versão 2203 ou posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2303 ou posterior

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de ter o controle, você pode fazer seleções, edições ou outras atividades de teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela estiver sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar sua solicitação.

Enquanto você tiver o controle, poderá fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar tanto um teclado quanto um mouse. Quando terminar, clique em **Solicitar controle**.

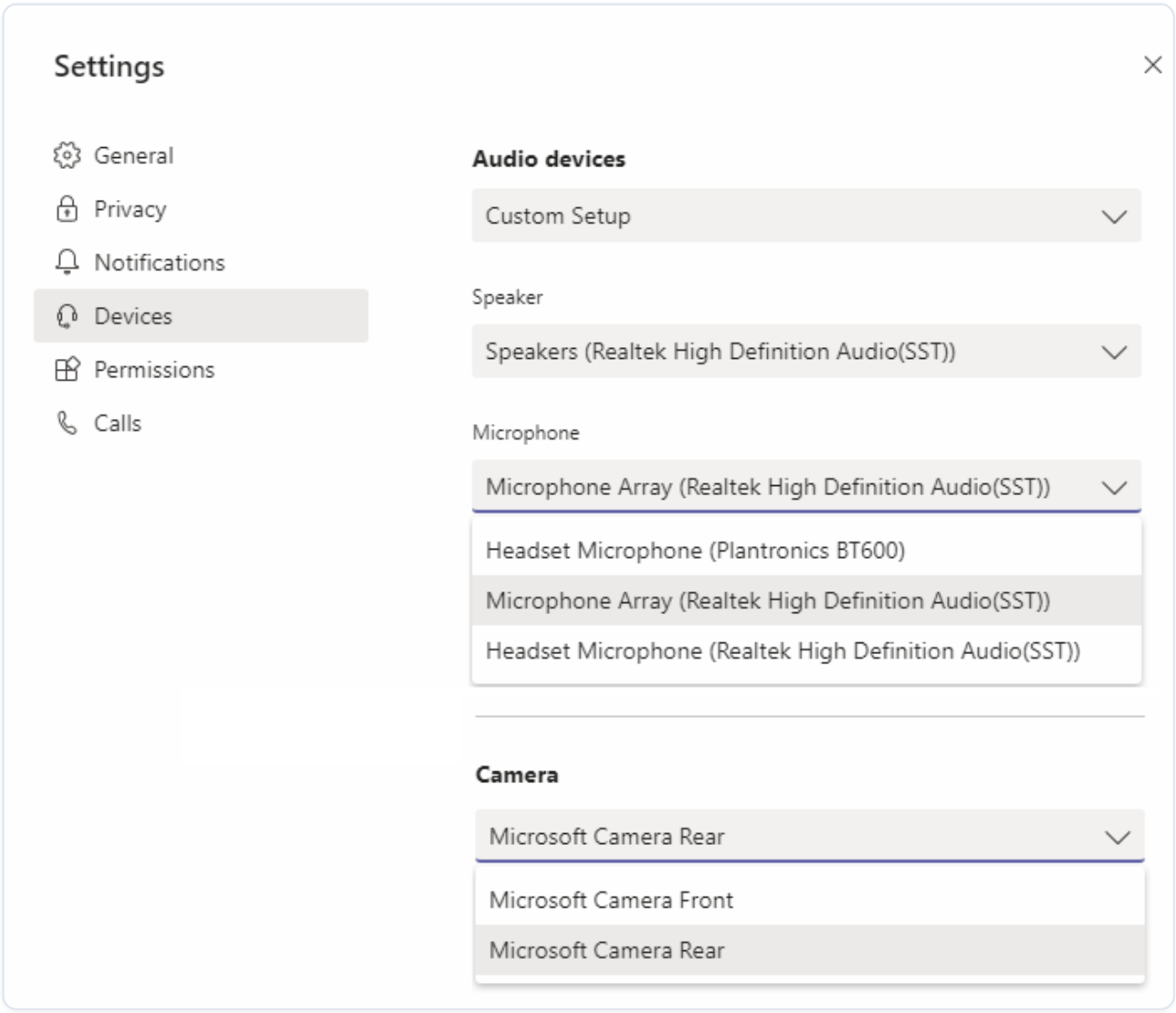
> **Limitações:**

> - Os controles de Conceder e Solicitar não estão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como Compartilhamento de aplicativo). A área de trabalho ou monitor completo deve ser compartilhado.
> - O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização para Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fones de ouvido, microfones, câmeras, alto-falantes e assim por diante). Então, os

periféricos são listados corretamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele depende do mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão do mesmo endpoint.

Recomendações:

- Fones de ouvido certificados para Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde o microfone e os alto-falantes estão em

dispositivos separados, pode haver eco. Um exemplo é uma webcam com microfone integrado e um monitor com alto-falantes. Ao usar alto-falantes externos, posicione-os o mais longe possível do microfone. Além disso, posicione-os longe de qualquer superfície que possa refratar o som para o microfone. Para obter mais informações, acesse `www.microsoft.com` e procure por fones de ouvido certificados para Microsoft Teams.

- Câmeras certificadas para Microsoft Teams, embora os periféricos certificados para Skype for Business sejam compatíveis com o Microsoft Teams. Para obter mais informações, acesse <www.microsoft.com> e procure por câmeras certificadas para Microsoft Teams e periféricos certificados para Skype for Business.
- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento da CPU com webcams que realizam codificação H.264 integrada - UVC 1.1 e 1.5.

Nota:

O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio de 24 bits ou com frequências acima de 96 kHz.

HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou anterior) suporta apenas estes formatos específicos de dispositivo de áudio (canais, profundidade de bits e taxa de amostragem):

- Dispositivos de Reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
- Dispositivos de Gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz

Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.

Os logs do **Webrpc** em **HdxTeams.exe** mostram este tipo de informação:

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

> `Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

> Como solução alternativa, desative o dispositivo específico ou:

> 1. Abra o **Painel de Controle de Som** (mmsys.cpl).
> 2. Selecione o dispositivo de reprodução ou gravação.
> 3. Vá para **Propriedades > Avançado** e altere as configurações para um modo compatível.

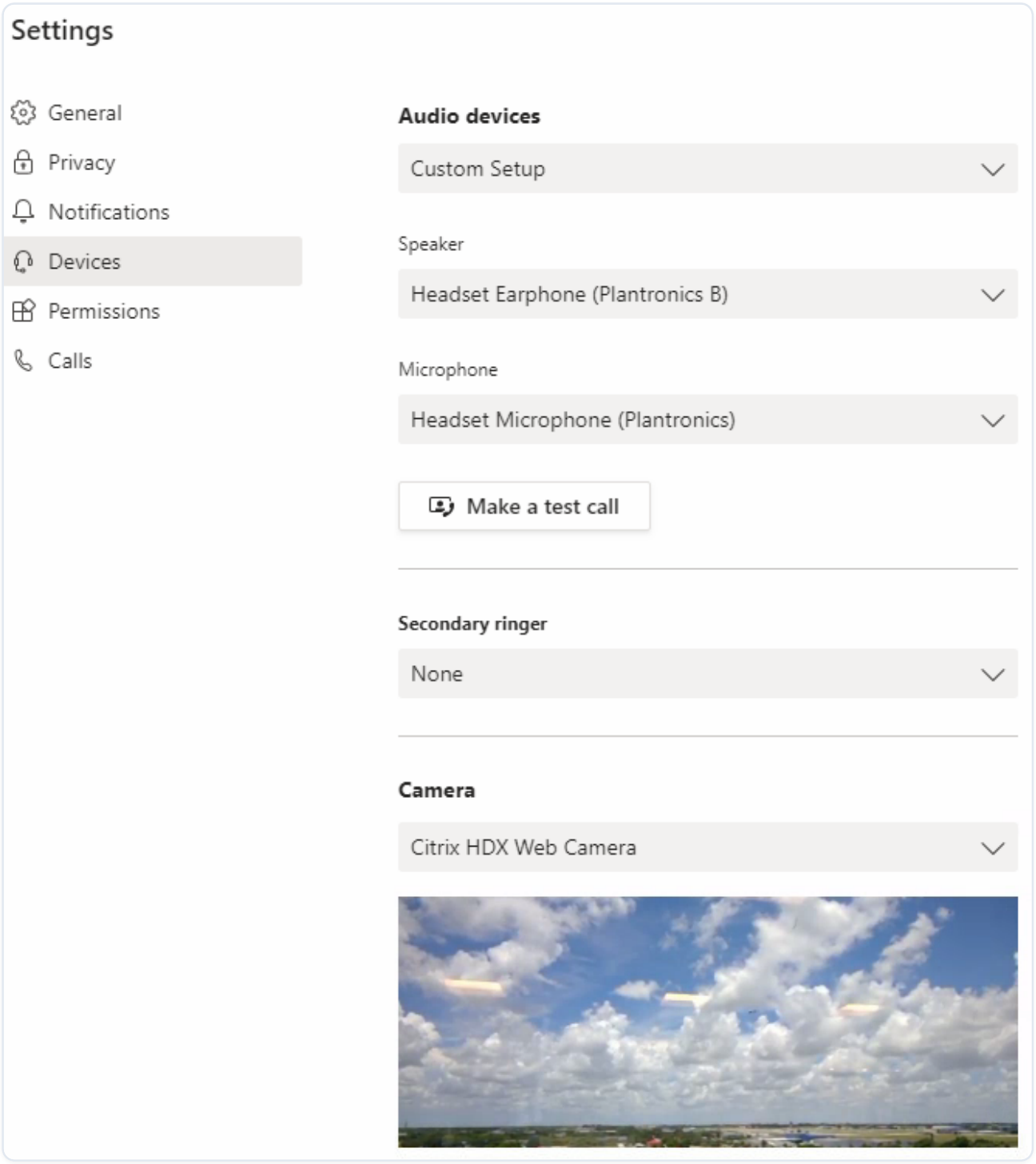
Modo de fallback

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Not Connected" em Microsoft Teams/Sobre/Versão), o VDA retorna às tecnologias HDX legadas. As tecnologias HDX legadas podem ser redirecionamento de webcam e redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão do aplicativo Workspace/SO de plataforma que não suporta a otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam. No modo de fallback, os periféricos são mapeados para o VDA. Os periféricos aparecem para o aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no VDA. Para obter mais informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados por meio do registro.

Este recurso requer a versão 1.3.0.13565 ou posterior do Microsoft Teams.

Para determinar se você está no modo otimizado ou não otimizado ao olhar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX legadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX**, conforme mostrado na imagem a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) em comparação com o modo otimizado.



Quando as tecnologias HDX legadas são usadas, o Microsoft Teams não descarrega o processamento de áudio, vídeo e compartilhamento de tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do endpoint. Em vez disso, as tecnologias HDX usam a renderização do lado do servidor. Espere alto consumo de CPU no VDA ao ligar o vídeo. O desempenho de áudio em tempo real pode não ser ideal.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- As configurações de QoS no Centro de Administração para Microsoft Teams não se aplicam a usuários VDI.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo poderá ser capturado.

Limitação no VDA:

- Quando você configura a definição **Citrix Workspace app High DPI** para `Yes`, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente — não no VDA.

Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams no Windows e Mac. Para Linux, verifique com o fornecedor do seu thin client. Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes endpoints são aprimoradas, adaptando-se à resolução adequada para a melhor experiência de chamada para todos os participantes.

Com esta experiência aprimorada, cada usuário pode entregar múltiplos fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p, e assim por diante) dependendo de vários fatores, incluindo a capacidade do endpoint, condições de rede, e assim por diante. O endpoint receptor então solicita a resolução de qualidade máxima que ele pode manipular, proporcionando assim a todos os usuários a experiência de vídeo ideal.

> **Nota:**

> Este recurso está disponível somente após o lançamento de uma atualização do Microsoft Teams. Para obter informações sobre a ETA, acesse `<https://www.microsoft.com/>` e procure por roteiro do Microsoft 365. Quando a atualização for lançada pela Microsoft, você poderá verificar CTX253754 para a atualização da documentação e o anúncio.

Limitações do Microsoft

- A visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams – entre em contato com a Microsoft para saber quando esperar uma grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.
- A resolução máxima do fluxo de vídeo de entrada e saída é 720p.
- O tom de retorno de chamada PSTN não é suportado.
- O desvio de mídia para Roteamento Direto não é suportado.
- As funções de produtor e apresentador de transmissão e evento ao vivo não são suportadas. A função de participante é suportada, mas não otimizada (renderiza no VDA em vez disso).
- A função de zoom in e zoom out no Microsoft Teams não é suportada.
- O Roteamento Baseado em Localização e o Desvio de Mídia não são suportados.
- A fusão de chamadas não é suportada (opção não exibida na interface do usuário).

Limitações do Citrix e Microsoft

- Ao compartilhar a tela, a opção **incluir áudio do sistema** não está disponível.
- Simulcast não é suportado no ChromeOS.

Próximo EOL do Microsoft Teams de Janela Única

Em January 31, 2024, a Microsoft descontinuará o suporte do Microsoft Teams para a interface de usuário de janela única ao usar a otimização do Microsoft Teams VDI e oferecerá suporte apenas à experiência de múltiplas janelas. A Microsoft notificou essa descontinuação em 9/8/2023 no Centro de Administração do M365 (ID da Postagem: MC674419). Detalhes públicos sobre o recurso de múltiplas janelas podem ser encontrados no artigo da Comunidade Técnica: New Meeting and Calling Experience in Microsoft Teams.

> **Observação:**

A Citrix recomenda que você atualize seu VDA e o aplicativo Citrix Workspace para as versões compatíveis para continuar usando o Microsoft Teams no modo otimizado para vídeo e compartilhamento de tela. Se você não atualizar sua infraestrutura e endpoints para oferecer suporte a múltiplas janelas, suas chamadas, chamadas de vídeo e compartilhamento de tela se tornarão não otimizados. Isso pode resultar em problemas de qualidade de chamada, aumento da latência e aumento da carga no servidor.

A tabela a seguir ilustra as versões mínima, LTSR e recomendada do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams em Citrix VDI:

COMPONENTE	VERSÃO MÍNIMA (1)	VERSÃO LTSR COMPATÍVEL (2)	VERSÃO RECOMENDADA (3)
Microsoft Teams	1.5.00.11865	Não aplicável	Mais recente
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Aplicativo Citrix Workspace para Windows	2112.1 CR	2203 CU2+ (4)	2309 CR+
Aplicativo Citrix Workspace para Mac	2203 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para Linux	2202 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para ChromeOS ou HTML5	2303 CR	Não aplicável	2309 CR+

Notas:

1. Versão Mínima: Esta é a versão onde o Multi-window foi introduzido pela primeira vez. Algumas versões mínimas listadas aqui podem estar no fim da vida útil.
2. Versão LTSR Suportada: Esta é a versão LTSR que é suportada pela Citrix para Multi-window. Versões mais antigas dessas versões LTSR podem funcionar, mas o suporte não está mais disponível para essas versões assim que uma nova versão LTSR CU é lançada. Para mais informações sobre as políticas de suporte LTSR, consulte `<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`.
3. Versão Recomendada: Esta é a versão do software que a Citrix recomenda se o usuário/cliente optar por atualizar seu software. Todas estas são versões CR.
4. A versão 2203 LTSR para VDA e as versões base do CWA incluem a funcionalidade de múltiplas janelas. Essas versões foram substituídas pela CU mais recente, que é a versão oficialmente suportada. Os clientes podem continuar a usar essas versões não suportadas a seu critério. A Citrix incentiva os clientes na versão LTSR a atualizar para a CU mais recente.

Anúncio de descontinuação do formato SDP (Plano B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP atual (Plano B) do WebRTC em futuras versões. Você deve usar o Plano Unificado no WebRTC para oferecer suporte às funcionalidades otimizadas do Microsoft Teams.

Produtos afetados

Em uma das futuras versões do Citrix Workspace Application, chamadas entre endpoints com a próxima versão do aplicativo Citrix Workspace e endpoints com o aplicativo Citrix Workspace 2108 ou versões mais antigas não serão suportadas. Essa incompatibilidade de chamada inclui clientes do aplicativo Citrix Workspace 1912 LTSR (CWA). Os seguintes clientes CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

Substituição para o Plano B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior a 2109, você deve atualizar para uma versão suportada (preferencialmente a versão CR mais recente). Caso contrário, quaisquer chamadas com uma versão futura ou endpoints mais recentes falharão ao conectar. Chamadas entre versões futuras e seus parceiros de comunicação federados também podem falhar ao serem concluídas se o parceiro federado não tiver atualizado seu Citrix Workspace.

A versão 2108 do aplicativo Citrix Workspace concluiu sua data de suporte em março de 2023 e deve ser atualizada para uma versão mais recente. Para mais informações, consulte Workspace App para detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plano B, consulte a documentação do WebRTC.

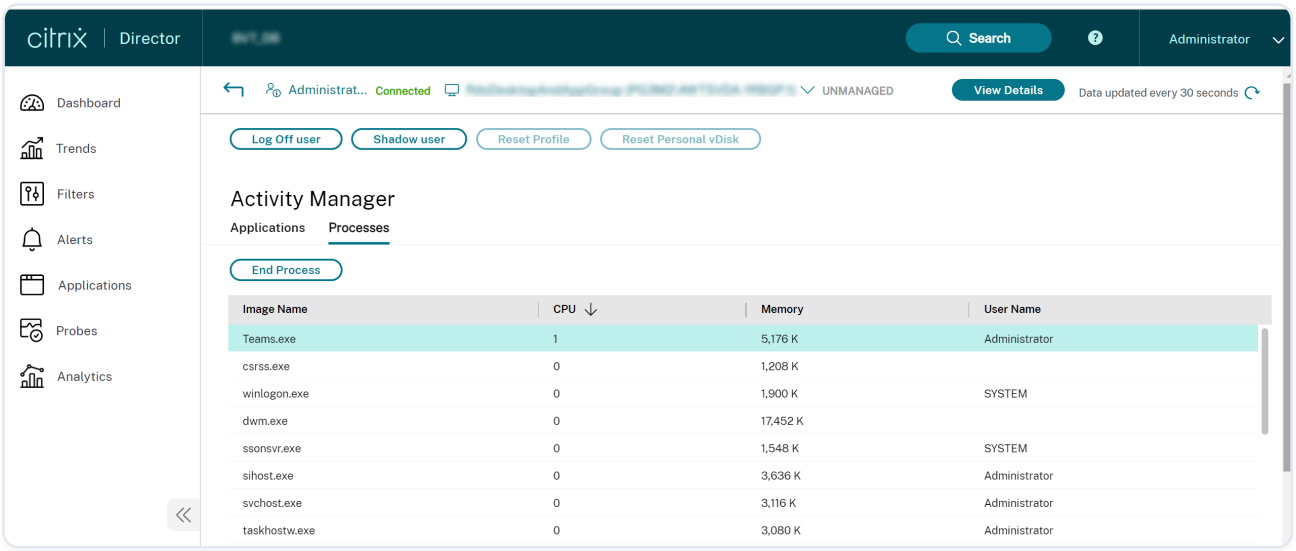
Informações adicionais

- Monitorar, solucionar problemas e dar suporte ao Microsoft Teams
- Implantar o aplicativo de desktop do Microsoft Teams na VM
- Instalar o Microsoft Teams usando MSI (seção Instalação VDI)
- Thin clients
- Ferramenta de Avaliação de Rede do Skype for Business
- Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business

Monitorar, solucionar problemas e dar suporte ao Microsoft Teams

Monitorar o Teams

Esta seção fornece diretrizes para monitorar a otimização do Microsoft Teams com HDX. Se você estiver executando no modo otimizado e `HdxRtcEngine.exe` estiver sendo executado na máquina cliente, um processo no VDA chamado `WebSocketAgent.exe` estará sendo executado na sessão. Use o **Activity Manager** no Director para ver o aplicativo.



O status de otimização do Microsoft Teams pode ser visualizado no Director > página **User Details** > painel **Session Details** > campo **MS Teams Optimization**. A otimização do Microsoft Teams é fundamental para uma melhor experiência do usuário, como áudio e vídeo nítidos. Este recurso está disponível para VDA versão 2311 e posterior. As versões do aplicativo Citrix Workspace™ suportadas estão listadas em Otimização para Microsoft Teams. O Director exibe o status da otimização do Microsoft Teams somente se o Microsoft Teams estiver sendo executado como um aplicativo publicado ou dentro de um desktop publicado. Para obter mais informações, consulte Status de otimização do Microsoft Teams.

Com a versão mínima do VDA 1912, você pode monitorar chamadas ativas do Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`. Com a versão mínima do VDA 1912, você pode monitorar chamadas ativas do Microsoft Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`.

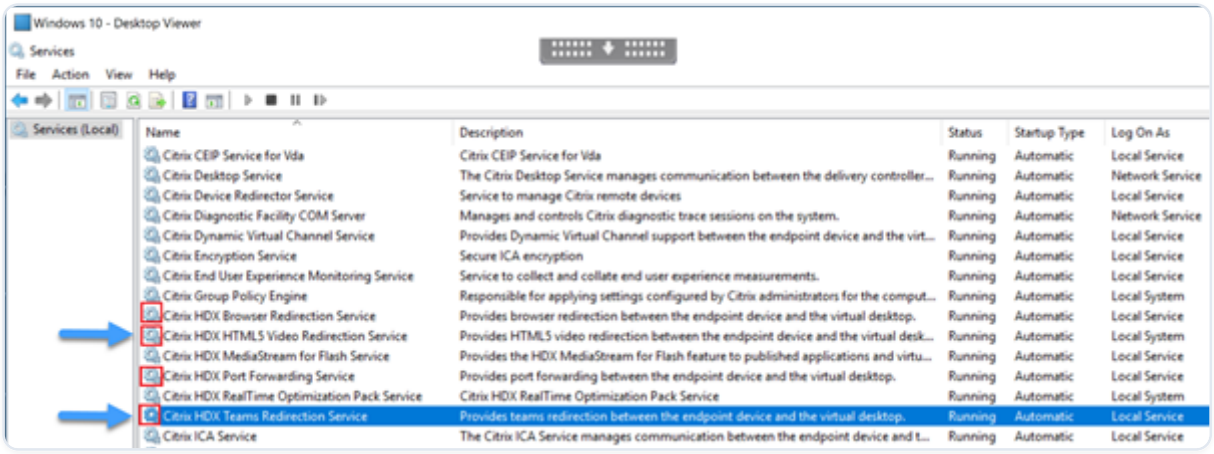
Para obter mais informações, consulte *Monitoramento* no artigo da Central de Conhecimento CTX253754.

Solução de problemas

Esta seção fornece dicas de solução de problemas para questões que você pode encontrar ao usar a otimização para Microsoft Teams. Para obter mais informações, consulte CTX253754.

No Virtual Delivery Agent

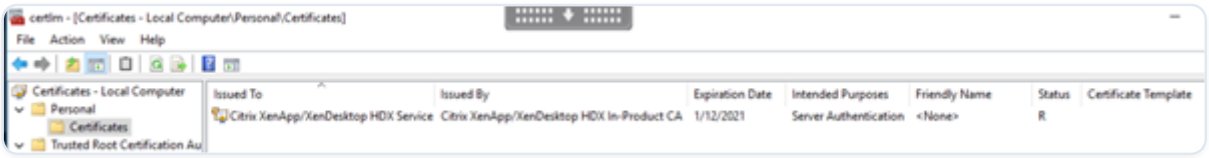
Existem quatro serviços instalados por BCR_x64.msi. Apenas dois são responsáveis pelo redirecionamento do Microsoft Teams no VDA.



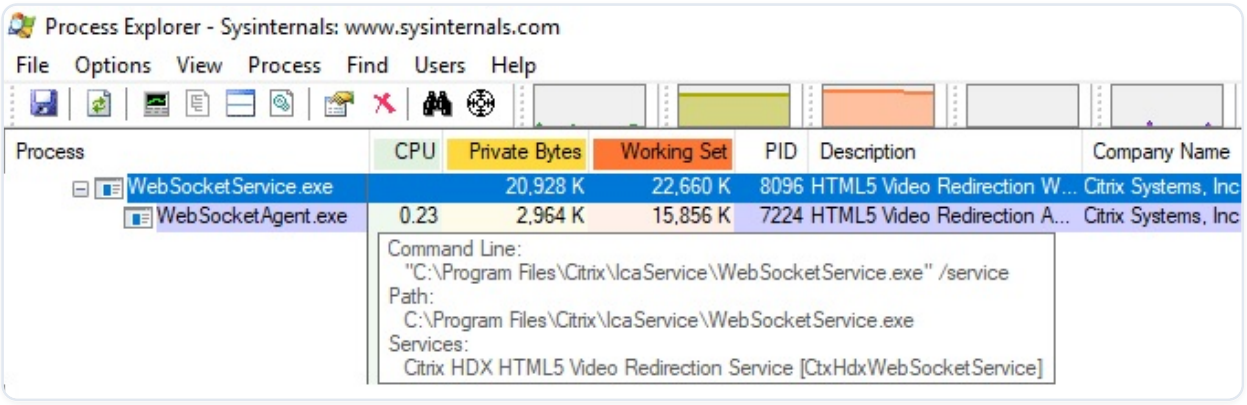
- O **Citrix HDX Teams Redirection Service** estabelece o canal virtual usado no Microsoft Teams. O serviço depende de CtxSvcHost.exe.
- O **Citrix HDX HTML5 Video Redirection Service** é executado como WebSocketService.exe, escutando em 127.0.0.1:9002 TCP. WebSocketService.exe executa duas funções principais:

  i. A **terminação TLS para WebSockets seguros** recebe uma conexão WebSocket segura de vdiCitrixPeerConnection.js, que é um componente dentro do aplicativo Microsoft Teams. Você pode rastreá-lo com o Process Monitor.

  Alguns softwares antivírus e de segurança de desktop interferem no funcionamento adequado de `WebSocketService.exe` e seus certificados. Embora o serviço Citrix HDX HTML5 Video Redirection possa estar sendo executado no console `services.msc`, o socket TCP localhost `127.0.0.1:9002` nunca está no modo de escuta, como visto no netstat. Tentar reiniciar o serviço faz com que ele trave ("Parando..."). Certifique-se de aplicar as exclusões adequadas para o processo `WebSocketService.exe`.



  ii. **Mapeamento de sessão do usuário.** Quando o aplicativo Microsoft Teams é iniciado, o WebSocketService.exe inicia o processo WebSocketAgent.exe na sessão do usuário no VDA. O WebSocketService.exe é executado na Sessão 0 como uma conta LocalSystem.



Você pode usar `netstat` para verificar se o serviço WebSocketService.exe está em um estado de escuta ativa no VDA.

Execute `netstat -anob -p tcp` a partir de uma janela de prompt de comando elevada:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

Em uma conexão bem-sucedida, o estado muda para ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

Importante:

O WebSocketService.exe escuta em dois TCP sockets, 127.0.0.1:9001 e 127.0.0.1:9002. A Port 9001 é usada para redirecionamento de conteúdo do navegador e HTML5 video redirection. A Port 9002 é usada para Microsoft Teams redirection. Certifique-se de que não há configurações de proxy no Windows OS do VDA que possam impedir uma comunicação direta entre Teams.exe e WebSocketService.exe. Às vezes, ao configurar um proxy explícito no Internet Explorer 11 (**Opções da Internet > Conexões > Configurações da LAN > Servidor proxy**), as conexões podem fluir através de um servidor proxy atribuído. Verifique se **Ignorar servidor proxy para endereços locais** está marcado ao usar uma configuração de proxy manual e explícita.

Localizações e descrições dos serviços

SERVIÇO	CAMINHO PARA O EXECUTÁVEL NO WINDOWS SERVER OS	FAZER LOGON COMO	DESCRIÇÃO
Serviço de Redirecionamento de Vídeo HTML5 da Citrix	"C:\Arquivos de Programas (x86)\Citrix\System32\WebSocketService.exe" /service	Conta do Sistema Local	Fornece vários serviços multimídia HDX com a estrutura inicial necessária para realizar o redirecionamento de mídia entre o desktop virtual e o dispositivo de endpoint.
Serviço de Redirecionamento de Navegador Citrix HDX	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	Esta conta (serviço local)	Fornece redirecionamento de conteúdo do navegador entre o dispositivo de endpoint e o desktop virtual.
Serviço de Encaminhamento de Porta Citrix	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	Esta conta (serviço local)	Fornece encaminhamento de porta entre o dispositivo de endpoint e o desktop virtual para redirecionamento de conteúdo do navegador.
Serviço de Redirecionamento de Teams Citrix HDX	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Conta do Sistema Local	Fornece redirecionamento do Microsoft Teams entre o dispositivo de endpoint e o desktop virtual.

Aplicativo Citrix Workspace

No endpoint do usuário, o aplicativo Citrix Workspace para Windows instancia um novo serviço chamado HdxTeams.exe ou HdxRtcEngine.exe. Ele faz isso quando o Microsoft Teams é iniciado no VDA e o usuário tenta ligar ou acessar os periféricos na pré-visualização. Se você não vir este serviço, verifique o seguinte:

1. Certifique-se de que você instalou no mínimo a versão 1905 do Workspace App para Windows. Você vê os binários HdxTeams.exe ou HdxRtcEngine.exe e webrpc.dll no caminho de instalação do aplicativo Workspace?
2. Se você validou a etapa 1, faça o seguinte para verificar se HdxTeams.exe ou HdxRtcEngine.exe está sendo iniciado.
    a. Saia do Microsoft Teams no VDA.
    b. Inicie services.msc no VDA.
    c. Pare o Serviço de Redirecionamento do Citrix HDX Teams.
    d. Desconecte a sessão ICA®.
    e. Conecte a sessão ICA.
    f. Inicie o Serviço de Redirecionamento do Citrix HDX Teams.
    g. Reinicie o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX.
    h. Inicie o Microsoft Teams no VDA.
3. Se você ainda não vir HdxTeams.exe ou HdxRtcEngine.exe sendo iniciado no endpoint do cliente, faça o seguinte:
    a. Reinicie o VDA.
    b. Reinicie o endpoint do cliente.

Suporte

A Citrix e a Microsoft dão suporte conjunto à entrega do Microsoft Teams a partir do Citrix Virtual Apps and Desktops™ usando a otimização para Microsoft Teams. Esse suporte conjunto é o resultado de uma estreita colaboração entre as duas empresas. Se você tiver contratos de suporte válidos e encontrar um problema com esta solução, abra um tíquete de suporte com o fornecedor cujo código você suspeita estar causando o problema. Ou seja, a Microsoft para o Teams ou a Citrix para os componentes de otimização. A Citrix ou a Microsoft recebe o tíquete, tria o problema e o escala conforme apropriado. Não há necessidade de você entrar em contato com a equipe de suporte de cada empresa.

Quando você tiver um problema, recomendamos que clique em **Ajuda > Relatar um Problema** na interface do usuário do Teams. Os logs do lado do VDA são compartilhados automaticamente entre a Citrix e a Microsoft para resolver problemas técnicos mais rapidamente.

Coleta de logs

Os logs do mecanismo de mídia HDX podem ser encontrados na máquina do usuário (não no VDA). Em caso de problemas, certifique-se de anexar os logs ao seu caso de suporte.

Logs do Windows:

Você pode localizar os logs do Windows em %TEMP% dentro da pasta **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Procure por um arquivo .txt chamado webrpc_Dia_Mês_carimbo_de_data_hora_Ano.txt. Se você estiver usando versões mais recentes do aplicativo Citrix Workspace, por exemplo, Citrix Workspace app 2009.5 ou posterior, armazene os logs em AppData\Local\Temp\HdxRtcEngine.

Cada sessão cria uma pasta separada para os logs.

Logs do Mac:

1. Log VDWEBRTC - registra a execução do canal virtual.

   Localização: `/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`
2. Log HdxRtcEngine - registra a execução dos processos no HdxRtcEngine.

   Local: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   O log HdxRtcEngine é habilitado por padrão.
3. Logs Webrpc - são os logs mais importantes que registram a execução do encerramento da biblioteca webrtc.

   Local: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Logs do Linux:

Você pode localizar os logs do Linux nas pastas `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`. Log Webrtc: `/tmp/webrpc/<current date>/webrtc.log` Log do Kernel: `/var/log/syslog`

Logs ICE/STUN/TURN:

Ao estabelecer uma chamada, estas quatro fases ICE são necessárias:

- Coleta de candidatos
- troca de candidatos
- Verificações de conectividade (solicitações de vinculação STUN)
- Promoção de candidatos

Nos logs do HdxRtcEngine.exe, as seguintes entradas são as entradas relevantes do Interactive Connectivity Establishment (ICE). Essas entradas devem estar presentes para que uma configuração de chamada seja bem-sucedida. Veja o trecho de exemplo a seguir para a fase de coleta:

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
```

```
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

Se houver vários candidatos ICE, a ordem de preferência é:

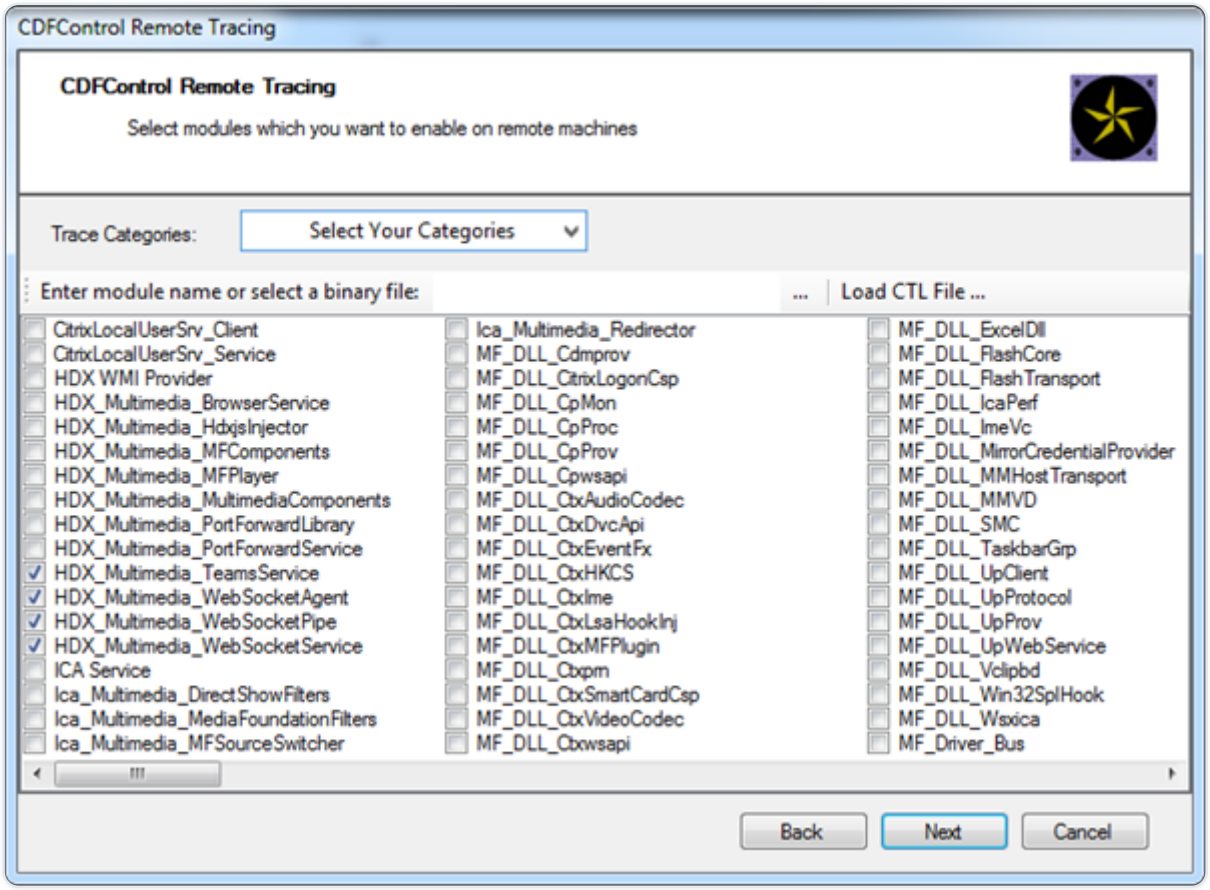
1. hospedeiro

2. reflexivo de par
3. reflexivo de servidor
4. retransmissão de transporte

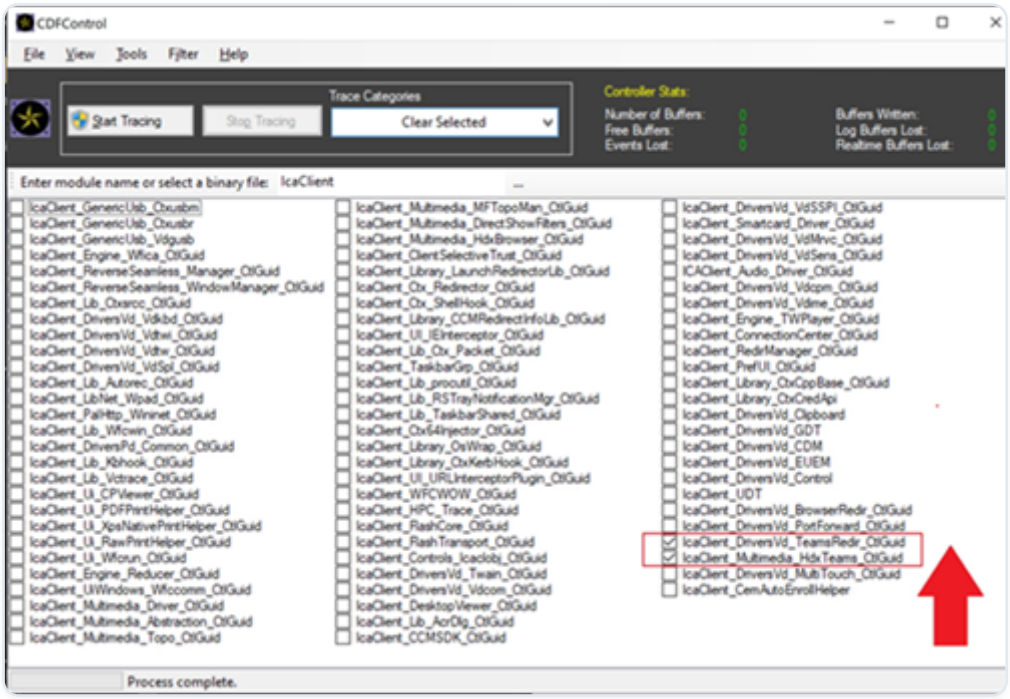
Se você encontrar um problema e puder reproduzi-lo consistentemente, recomendamos que clique em **Ajuda > Relatar um problema** no Microsoft Teams. Os logs são compartilhados entre a Citrix e a Microsoft para resolver problemas técnicos se você abriu um caso com a Microsoft. A captura de rastreamentos CDF antes de entrar em contato com o Suporte Citrix também é benéfica. Para obter mais informações, consulte o artigo da Central de Conhecimento CDFcontrol.

Para recomendações sobre a coleta de rastreamentos CDF, consulte o artigo da Central de Conhecimento Recomendações para Coletar os Rastros CDF.

Rastros CDF do lado do VDA - Habilite os seguintes provedores de rastreamento CDF:



Rastreamentos CDF do lado do aplicativo Workspace - Ative os seguintes provedores de rastreamento CDF:



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requer o aplicativo Citrix Workspace 2012 ou posterior)

Redirecionamento do Windows Media

O redirecionamento do Windows Media controla e otimiza a forma como os servidores entregam áudio e vídeo em streaming aos usuários. Ao reproduzir os arquivos de tempo de execução de mídia no dispositivo cliente, em vez de no servidor, o redirecionamento do Windows Media reduz os requisitos de largura de banda para a reprodução de arquivos multimídia. O redirecionamento do Windows Media melhora o desempenho do Windows Media Player e de reprodutores compatíveis executados em desktops virtuais do Windows.

Se os requisitos para a busca de conteúdo do lado do cliente do Windows Media não forem atendidos, a entrega de mídia usará automaticamente a busca do lado do servidor. Esse método é transparente para os usuários. Você pode usar o Citrix Scout para executar um rastreamento do Citrix Diagnosis Facility (CDF) 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 compactado nativo e redireciona o conteúdo para o dispositivo cliente. O dispositivo cliente então recria o pipeline de mídia para descompactar e renderizar os dados de mídia recebidos do servidor host. O redirecionamento do Windows Media funciona bem em dispositivos cliente que executam um sistema operacional Windows. Esses dispositivos possuem a estrutura multimídia necessária para reconstruir o pipeline de mídia como ele existia

no servidor host. Clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento do Windows Media** controla esse recurso e está **Permitido** por padrão. Geralmente, essa configuração aumenta a qualidade de áudio e vídeo renderizados 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 compressão ICA® básica e áudio regular. Você pode desabilitar esse recurso adicionando a configuração **Redirecionamento do Windows Media** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações de política, consulte Configurações de política de multimídia.

Limitação:

Ao usar o Windows Media Player e as Extensões de Áudio e Vídeo Remotas (RAVE) habilitadas dentro de uma sessão, uma tela preta pode aparecer. Essa tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Em Reprodução no topo**.

Gerenciador de Plug-ins de Canal Virtual

Introdução

O gerenciador de plug-ins de canal virtual foi projetado para implantar plug-ins em endpoints de cliente para aplicativos específicos. O gerenciador de plug-ins detecta aplicativos específicos em execução no VDA e solicita ao usuário que instale o plug-in no endpoint para obter a melhor experiência ao executar o aplicativo.

Os usuários podem optar por instalar o plug-in, ignorá-lo ou negar a instalação. O gerenciador de plug-ins oferece flexibilidade para gerenciar os plug-ins em todos os endpoints — gerenciados ou não gerenciados.

Por exemplo: o Microsoft Teams tem uma nova arquitetura (Otimização SlimCore), que exige que um plug-in seja instalado nos endpoints para que a otimização funcione. O gerenciador de plug-ins de canal virtual pode implantar os plug-ins em seus endpoints. Para obter mais informações, consulte nova solução VDI para Teams

Requisitos do Sistema

A seguir estão os requisitos mínimos para o gerenciador de plug-ins de canal virtual.

- Virtual Desktop Agent (VDA)
  - 2411 CR
- DDC
  - Cloud 121 Release
  - 2407 CR
- Citrix Workspace™ App (Aplicativo Citrix Workspace)
  - Aplicativo Citrix Workspace para Windows 2409

> **Observação:**
>
> Este recurso é atualmente aplicável a endpoints Windows.

Aplicativos suportados

- Os aplicativos atualmente suportados estão listados abaixo:
  - Microsoft Teams - Consulte nova solução VDI para Teams

Visão geral do Gerenciador de Plug-ins de Canal Virtual

Compreendendo o Recurso

A Citrix® entende que os ambientes dos clientes podem ser complexos e que a implantação de um plug-in em endpoints gerenciados e não gerenciados exige um esforço significativo. Este recurso foi projetado para simplificar o processo.

Este recurso inclui dois componentes: um no lado do VDA (processo detector) e outro no lado do Citrix Workspace™ App (processo instalador). Quando os administradores atendem aos pré-requisitos mencionados acima, como habilitar políticas, fazer entradas de registro e especificar um aplicativo para monitorar:

- O processo detector do lado do VDA monitora o lançamento do aplicativo pelo usuário final assim que ele faz logon na área de trabalho virtual

- O processo detector informa o lado do Citrix Workspace App para solicitar ao usuário que instale o plug-in necessário para otimizar o aplicativo especificado
- Os usuários recebem um pop-up em sua tela com breves detalhes sobre o plug-in. Os usuários podem optar por instalar o plug-in, ignorar ou optar por nunca instalá-lo
    - Se os usuários ignorarem o processo de instalação, eles não verão o pop-up novamente nessa sessão. O prompt de instalação aparecerá ao reconectar a sessão.
    - Se os usuários optarem por nunca instalar o plug-in, a escolha será registrada em seu perfil de usuário para visibilidade do administrador.
- Se os usuários optarem por instalar o plug-in, o lado do Citrix Workspace App fará o download e instalará o plug-in no endpoint.
    - Após a instalação bem-sucedida, o usuário receberá uma mensagem para reconectar a sessão para que o plug-in entre em vigor. O usuário pode optar por fazer isso imediatamente ou fechar a mensagem de sucesso e reconectar mais tarde.
    - Se a instalação falhar, o usuário verá uma mensagem de erro e a falha será registrada para visibilidade do administrador.

Configuração do Gerenciador de Plug-ins de Canal Virtual

Implantação

1. Verifique se a política de redirecionamento do Microsoft Teams está ativada: Consulte política de redirecionamento do Microsoft Teams para obter mais detalhes.

   Esta política deve ser ativada independentemente do aplicativo que está sendo monitorado. No futuro, se mais aplicativos forem suportados e você quiser monitorar esses aplicativos em vez do Microsoft Teams, esta política ainda deverá ser ativada. Observe que esta política é ativada por padrão.

2. A política do gerenciador de plug-ins de canal virtual deve ser ativada: Consulte configurações da política do gerenciador de plug-ins de canal virtual para obter instruções detalhadas sobre como ativar a política.

   Esta política está disponível nas Configurações de Política Multimídia no Citrix Studio. A ativação da política permite especificar o nome do aplicativo a ser monitorado, por exemplo, “Microsoft Teams”. Esta política é desativada por padrão.

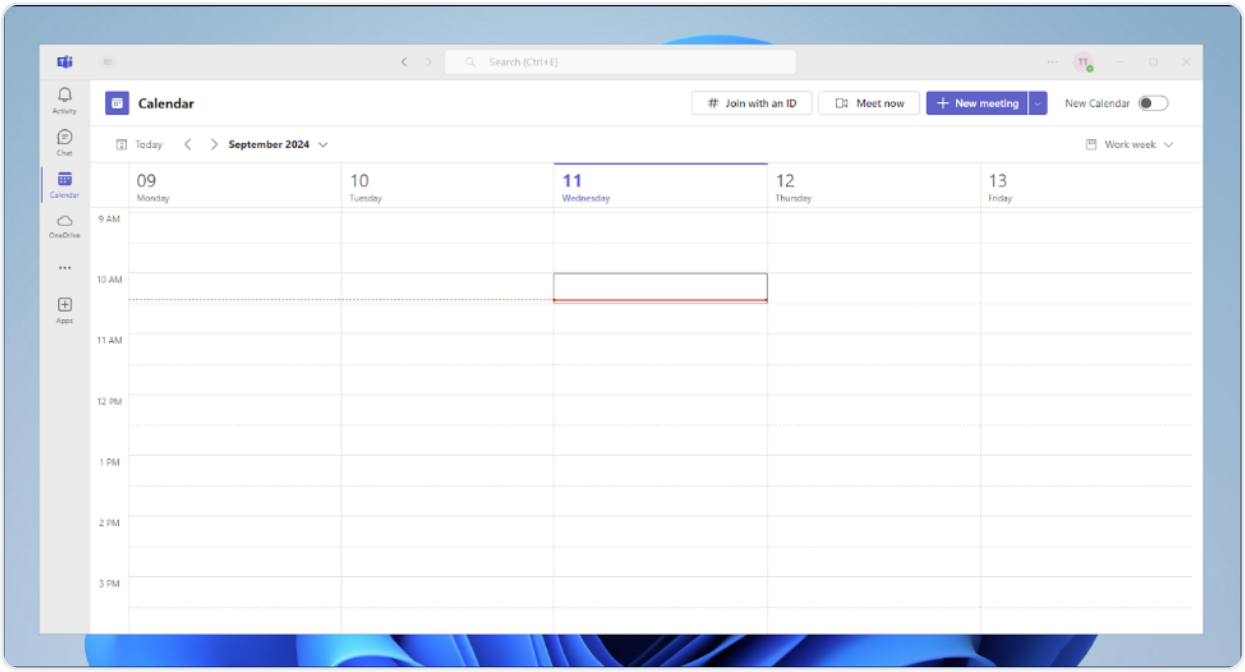
3. O aplicativo Citrix Workspace™ deve ser instalado no modo de sistema.

Nota:

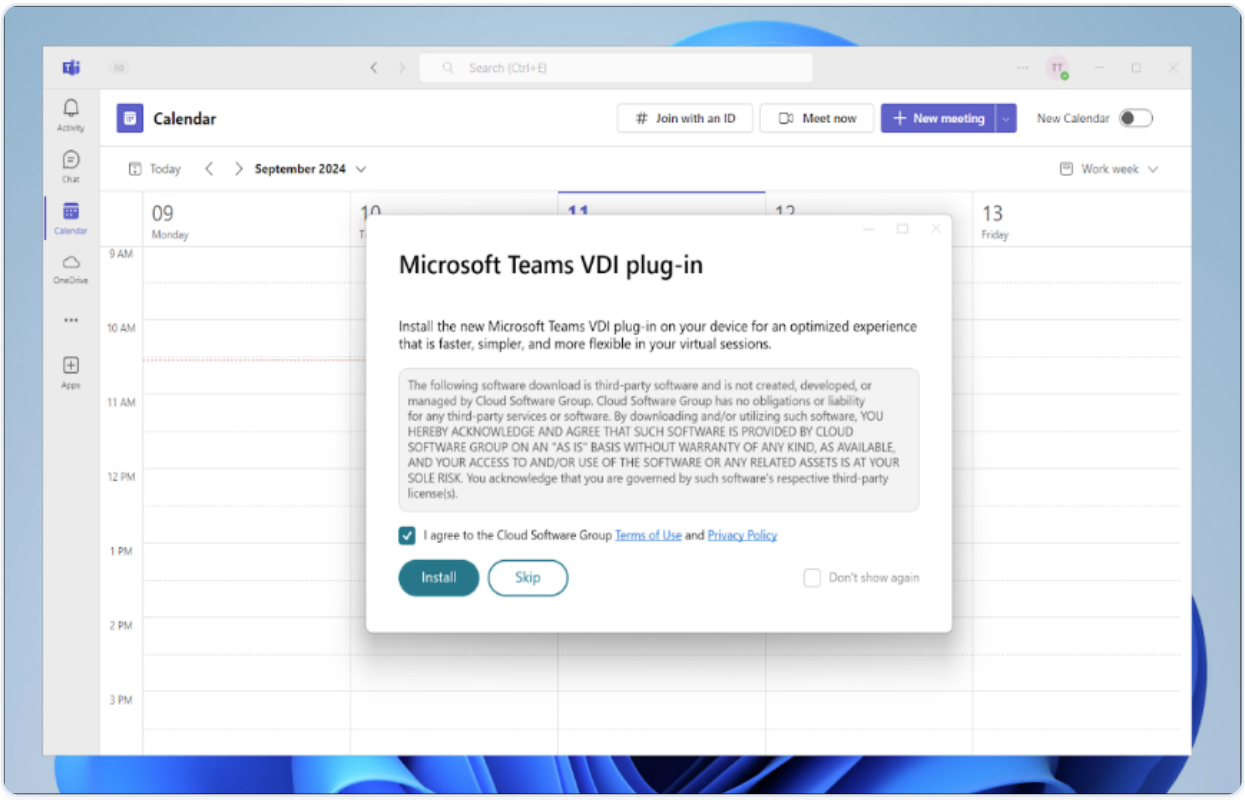
Os plug-ins são baixados para o endpoint a partir da CDN de terceiros. Por exemplo, se você selecionar o Microsoft Teams, o plug-in será baixado da CDN da Microsoft. Portanto, o endpoint deve ter acesso à CDN de terceiros. Caso contrário, a instalação do plug-in falhará.

Procedimento

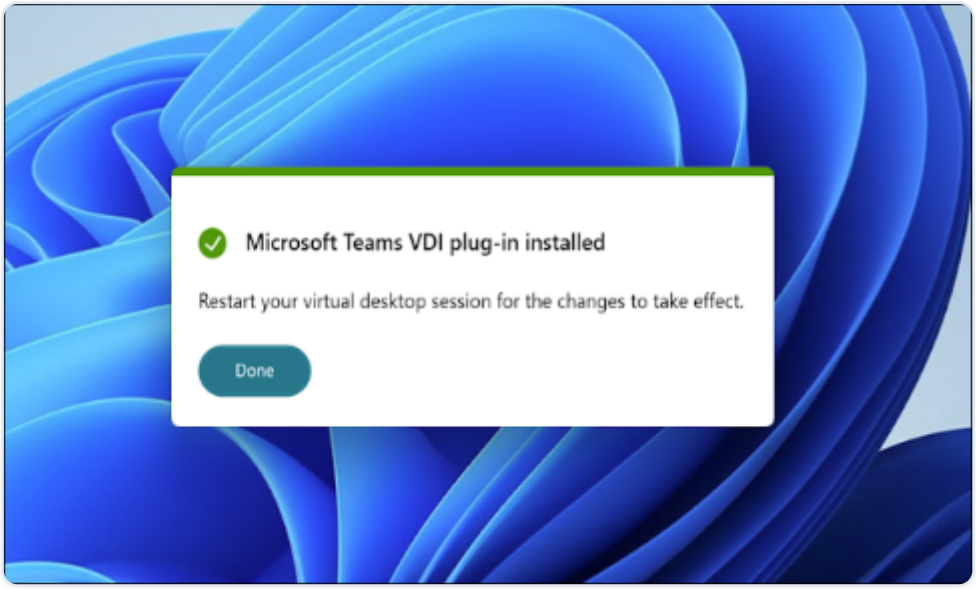
1. O usuário inicia o aplicativo na sessão Citrix. Por exemplo, Microsoft Teams.



2. O usuário recebe um pop-up para instalar o plug-in VDI do Teams no endpoint para uma melhor experiência. O pop-up aparece acima da sessão e não dentro da sessão, pois o plug-in será instalado no endpoint.



3. O usuário clica no botão de instalação e o plug-in é instalado. Os usuários precisam reiniciar a sessão da área de trabalho virtual para que as alterações entrem em vigor.



Problemas Conhecidos e Limitações

- No VDA 2407, a seguinte configuração de registro precisa ser definida como 1 no VDA, além da política, para que o recurso seja ativado. Essa configuração de registro é automaticamente permitida e não precisa ser configurada a partir do VDA 2411.

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

Name: EnableAppDetector Type: DWORD`

- Mais limitações a serem adicionadas

Redirecionamento geral de conteúdo

O redirecionamento de conteúdo permite controlar se os usuários acessam informações usando aplicativos publicados em servidores ou usando aplicativos executados localmente em dispositivos de usuário.

Redirecionamento de pasta do cliente(/pt-br/citrix-virtual-apps-desktops/2407/general-content-redirection/client-folder-redirection.html)

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host.

- Quando você habilita apenas o mapeamento de unidade do cliente no servidor, os volumes completos do lado do cliente são automaticamente mapeados para as sessões como links de Convenção Universal de Nomenclatura (UNC).
- Quando você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo de desktop Windows, a parte do volume local especificada pelo usuário é redirecionada.

Redirecionamento do host para o cliente(/pt-br/citrix-virtual-apps-desktops/2407/general-content-redirection/host-to-client-redirection.html)

Considere usar o redirecionamento do host para o cliente para casos de uso incomuns específicos. Normalmente, outras formas de redirecionamento de conteúdo podem ser melhores. Oferecemos suporte a esse tipo de redirecionamento apenas em VDAs de SO de múltiplas sessões e não em VDAs de SO de sessão única.

Acesso a aplicativos locais e redirecionamento de URL(/pt-br/citrix-virtual-apps-desktops/2407/general-content-redirection/laa-url-redirect.html)

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de desktop hospedado. Isso é feito sem a necessidade de alternar de um computador para outro.

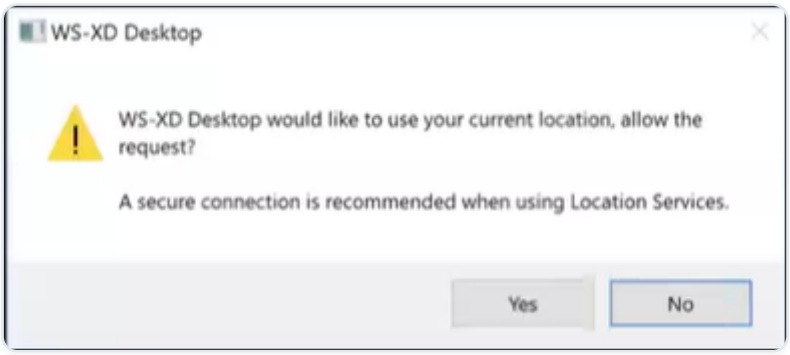
A tecnologia HDX™ oferece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde ele é inadequado.

Redirecionamento de localização do cliente

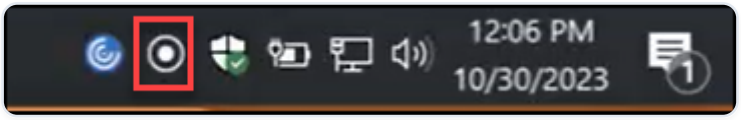
O redirecionamento de localização do cliente, quando ativado, permite que aplicativos e sessões de desktop hospedados em VDA acessem perfeitamente a localização atual do cliente. Em um sistema operacional multi-sessão (TS VDA ou Multi-Session WS VDA), cada sessão tem sua própria localização exclusiva fornecida pelo cliente conectado. Usando esse recurso, os aplicativos no VDA que dependem da localização têm a localização precisa do cliente.

Para obter mais informações, consulte a documentação Microsoft.

Depois que o redirecionamento de localização do cliente é ativado e o acesso à localização é permitido tanto no lado do servidor quanto no lado do cliente, ao iniciar um aplicativo ou desktop que acessa a localização, o cliente solicita que você compartilhe sua localização atual com a seguinte caixa de diálogo:



Ao ativar o redirecionamento de localização do cliente, o seguinte ícone aparece na barra de tarefas do cliente se/quando o aplicativo ou desktop hospedado no VDA consulta informações de localização atuais.



Requisitos do sistema

Para servidores:

- VDA de SO de Sessão Única (Win10/11) ou Multi-Sessão (Win 11 22H2 e Server 2022 23H2 ou posterior)
- Citrix Workspace™ app para Windows, iOS ou Android

Configuração

O redirecionamento de localização do cliente deve ser ativado usando a política Citrix® para que o recurso funcione. O redirecionamento de localização do cliente é desativado por padrão.

Para ativar o redirecionamento de localização do cliente, conclua as seguintes etapas:

No lado do VDA e do Cliente Windows:

1. Em **Configurações > Privacidade > Localização**, ative as seguintes opções:
    - **Permitir acesso à localização neste dispositivo**
    - **Permitir que aplicativos acessem sua localização**
    - **Permitir que aplicativos de desktop acessem sua localização**
2. Para SO de múltiplas sessões, habilite a configuração **Location Override**.

No lado do Controller/DDC:

Habilite a política **Studio > Policies > Location > Settings > Permitir que o aplicativo use a localização física do dispositivo cliente**. Para obter mais informações, consulte Configurações da política de sensores do cliente.

Redirecionamento de conteúdo bidirecional

O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS em navegadores da web, ou incorporadas em aplicativos, sejam encaminhadas entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Uma URL inserida em um navegador em execução na sessão Citrix pode ser aberta usando o navegador padrão do cliente. Por outro lado, uma URL inserida em um navegador em execução no cliente pode ser aberta em uma sessão Citrix, seja com um aplicativo ou desktop publicado. Alguns casos de uso comuns para o redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da web em casos em que o navegador inicial não tem acesso à rede para a origem.
- Redirecionamento de URLs da web por motivos de compatibilidade do navegador e segurança.
- Redirecionamento de URLs da web incorporadas em aplicativos quando não se deseja executar um navegador da web na sessão Citrix ou no cliente.

Requisitos do sistema

- VDAs de SO de sessão única ou multi-sessão
- Aplicativo Citrix Workspace™ para Windows 2311 ou superior
- Aplicativo Citrix Workspace™ para Linux 2503 ou superior

- Aplicativo Citrix Workspace™ para Mac 2607 ou superior

Navegadores:

- Google Chrome com Extensão de Redirecionamento de Navegador Citrix
  - Extensão do Google Chrome
- Microsoft Edge com Extensão de Redirecionamento de Navegador Citrix
  - Extensão do Microsoft Edge

Configuração

A partir da versão 2311 do Citrix Virtual Apps and Desktops™, o redirecionamento de conteúdo bidirecional é configurado apenas através do Citrix Studio. As versões anteriores tinham configurações de política configuradas tanto no endpoint do cliente quanto no Studio. O redirecionamento de conteúdo bidirecional é desabilitado por padrão.

Para configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações da **política ICA**.

Para que o redirecionamento do navegador funcione, as extensões do navegador devem ser registradas no navegador de origem (de onde a URL é redirecionada) usando os comandos mostrados. Execute os comandos conforme necessário no VDA e no cliente, com base no navegador em uso.

NAVEGADOR	VDA	CLIENTE
Google Chrome	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
Microsoft Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
Todos os Navegadores Disponíveis	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /RegAll	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /RegAll

Para cancelar o registro de uma extensão de navegador:

NAVEGADOR	VDA	CLIENTE
Google Chrome	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
Microsoft Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
Todos os Navegadores Disponíveis	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall

Nota:

- Execute esses comandos em uma janela do Prompt de Comando (CMD) com privilégios de administrador.
- O comando de registro faz com que os navegadores Chrome e Edge solicitem aos usuários que habilitem a Extensão de Redirecionamento de Navegador Citrix durante o primeiro lançamento.
- O comando de registro também vincula a Extensão de Redirecionamento de Navegador ao host de mensagens nativas, o que permite que a extensão se comunique com o código nativo. Sem isso, o navegador bloqueia a comunicação.
- Você também pode instalar a extensão do navegador manualmente na Google Chrome Web Store. Para usar a Extensão de Redirecionamento de Navegador da loja de Complementos do Microsoft Edge, você precisa da versão 2503 ou posterior do Virtual Delivery Agent (VDA). Para versões mais antigas do VDA, instale a extensão da Google Chrome Web Store dentro do seu navegador Microsoft Edge (consulte Adicionar uma extensão ao Microsoft Edge da Chrome Web Store).

- As versões do aplicativo Citrix Workspace listadas nos requisitos do sistema são as versões mínimas necessárias para suportar o redirecionamento de conteúdo bidirecional e o redirecionamento OAuth.
- Para Mac: devido aos requisitos de segurança do macOS para aplicativos autenticados, os esquemas de URL de retorno de chamada OAuth personalizados devem ser pré-registrados com a Citrix e não podem ser alterados dinamicamente após a instalação. Apenas `citrix-oauth-redir` é suportado por padrão. Entre em contato com a equipe de produto da Citrix para registrar seu esquema de URL.

Redirecionamento curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de curingas ao definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

Redirecionamento de protocolo personalizado do VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao redirecionamento de protocolos personalizados do Citrix VDA para o cliente. Protocolos diferentes de HTTP ou HTTPS são suportados. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Web Studio, defina o protocolo personalizado em **Redirecionamento de conteúdo bidirecional**.

Observação:

- Você deve ter privilégios de administrador para executar esses comandos.
- O cliente deve ter um aplicativo registrado para manipular o protocolo. Caso contrário, a URL redireciona para o cliente e falha ao iniciar.
- URLs de protocolo personalizado que você insere ou inicia nos navegadores Chrome e Edge não são suportadas e não são redirecionadas.
- Os seguintes protocolos não são suportados: `rtsp://, rtspu://, pnm://, mms://`.

Outras considerações

- Os requisitos e configurações do navegador são aplicáveis apenas ao navegador que inicia o redirecionamento. O navegador de destino, onde a URL é aberta após o redirecionamento ser bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, uma configuração de navegador suportada é necessária apenas no VDA. Por outro lado, ao redirecionar URLs do cliente para um VDA, uma configuração de navegador suportada é necessária apenas no cliente. As URLs redirecionadas são entregues ao navegador padrão configurado na máquina de destino, seja o cliente ou o VDA, dependendo da direção. 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 `https://www.citrix.com`, e a política do cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Encurtadores de URL não são suportados.
- O redirecionamento de cliente para VDA requer que o cliente Windows seja instalado com direitos de administrador.
- Se o navegador de destino já estiver aberto, a URL redirecionada será aberta em uma nova guia. Caso contrário, a URL será aberta em uma nova janela do navegador.
- O redirecionamento bidirecional de conteúdo não funciona quando o Acesso a Aplicativos Locais (LAA) está ativado.

Redirecionamento do host para o cliente

O redirecionamento do host para o cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix®, sejam abertas usando o aplicativo correspondente no dispositivo de endpoint do usuário. Alguns casos de uso comuns para o redirecionamento do host para o cliente incluem:

- Redirecionamento de sites em casos em que o servidor Citrix não tem acesso à Internet ou à rede para a origem.
- Redirecionamento de sites quando a execução de um navegador da web dentro da sessão Citrix não é desejada por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos em casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento do host para o cliente não se destina a URLs que você acessa em uma página da web ou digita na barra de endereços do navegador da web em execução na sessão Citrix. Para redirecionamento de URLs em navegadores da web, consulte Redirecionamento de URL bidirecional ou Redirecionamento de conteúdo do navegador.

Requisitos do sistema

- VDA de SO multissessão
- Clientes compatíveis:
  - Citrix Workspace™ app 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 Redirecionamento do host para o cliente para habilitar esta funcionalidade. O **Redirecionamento do host para o cliente** está desabilitado por padrão. Depois de habilitar a política de redirecionamento do host para o cliente, o aplicativo Citrix Launcher se registra com o servidor Windows para garantir que ele possa interceptar URLs e enviá-las para o dispositivo cliente.

Em seguida, você deve configurar a Política de Grupo do Windows para usar o Citrix Launcher como o aplicativo padrão para os tipos de URL necessários. No VDA do servidor Citrix, crie o arquivo ServerFTAdefaultPolicy.xml e insira o seguinte código XML.

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
```

```
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

No console de gerenciamento de Política de Grupo, vá para **Configuração do computador > Modelos Administrativos > Componentes do Windows > Explorador de Arquivos > Definir um arquivo de configuração de associações padrão**, e salve seu arquivo ServerFTAdefaultPolicy.xml.

> **Observação:**
>
> Se um servidor Citrix não tiver as configurações da Política de Grupo, o Windows solicitará aos usuários que selecionem um aplicativo para abrir URLs.
>
> Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Para incluir tipos de URL padrão ou personalizados adicionais na lista para redirecionamento, crie uma nova linha **Association Identifier** no arquivo ServerFTAdefaultPolicy.xml referenciado anteriormente. Por exemplo:

`<Association Identifier="ftp" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />`

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

Adicionar tipos de URL à lista também requer configuração do cliente. Crie a seguinte chave de registro e valores no cliente Windows.

> **Observação:**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome do valor: ExtraURLProtocols
- Tipo de valor: REG_SZ
- Dados do valor: Especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade da URL. Por exemplo: `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL apenas para clientes Windows. Clientes que não possuem as configurações de registro acima rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para manipular os tipos de URL especificados.

Para remover tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD

- Dados do valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm`, ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

`http`

`https`

`rtsp`

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, crie uma chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: ValidSites
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este curinga corresponde a um único nível de domínio, o que é consistente com as regras no RFC 6125. Por exemplo:

`www.exmaple.com`

`*.example.com`

> **Observação:**
>
> Você não pode usar a chave **ValidSites** com as chaves **DisableServerFTA** e **NoRedirectClasses**.

Configuração do navegador padrão do VDA do servidor

A habilitação do redirecionamento do host para o cliente, conforme referenciado nesta seção, substitui qualquer configuração anterior do navegador padrão no VDA do servidor. Se um URL da web não for redirecionado, o Citrix Launcher passará o URL para o navegador configurado na

chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente. Para obter mais informações, consulte Configuração do navegador padrão do VDA do servidor na lista de recursos gerenciados por meio do registro.

Acesso a Aplicativos Locais e redirecionamento de URL

Introdução

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Com o Acesso a Aplicativos Locais, você pode:

- Acessar aplicativos instalados localmente em um laptop físico, PC ou outro dispositivo diretamente da área de trabalho virtual.
- Fornecer uma solução flexível de entrega de aplicativos. Se os usuários tiverem aplicativos locais que você não pode virtualizar ou que a TI não mantém, esses aplicativos ainda se comportarão como se estivessem instalados em uma área de trabalho virtual.
- Eliminar a latência de salto duplo quando os aplicativos são hospedados separadamente da área de trabalho virtual. Faça isso colocando um atalho para o aplicativo publicado no dispositivo Windows do usuário.
- Usar aplicativos como:
    - Software de videoconferência, como o GoToMeeting.
    - Aplicativos especializados ou de nicho que ainda não foram virtualizados.
    - Aplicativos e periféricos que, de outra forma, transfeririam grandes quantidades de dados de um dispositivo de usuário para um servidor e de volta para o dispositivo de usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops™, as sessões de área de trabalho hospedada usam o redirecionamento de URL para iniciar aplicativos de Acesso a Aplicativos Locais. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de bloqueio de URL do navegador) selecionando links incorporados em um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueio, o URL será aberto novamente na sessão da área de trabalho.

O redirecionamento de URL funciona apenas para sessões de área de trabalho, não para sessões de aplicativo. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo host-para-cliente, que é um tipo de redirecionamento FTA (Associação de Tipo de Arquivo) do servidor. Este FTA redireciona certos protocolos para o cliente, como HTTP, HTTPS, RTSP ou MMS. Por exemplo, se você abrir apenas links incorporados com HTTP, os links serão abertos diretamente com o aplicativo cliente. Não há suporte para lista de bloqueio ou lista de permissões de URL.

Quando o Acesso a Aplicativos Locais está ativado, os URLs exibidos aos usuários como links de aplicativos em execução localmente, de aplicativos hospedados pelo usuário ou como atalhos na área de trabalho são redirecionados de uma das seguintes maneiras:

- Do computador do usuário para a área de trabalho hospedada
- Do servidor Citrix Virtual Apps and Desktops para o computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento de conteúdo de sites específicos, configure a lista de permissões de URL e a lista de bloqueios de URL no Virtual Delivery Agent. Essas listas contêm chaves de registro de várias strings que especificam as configurações da política de redirecionamento de URL. Para obter mais informações, consulte as configurações da política de Acesso a Aplicativos Locais.

As URLs podem ser renderizadas no VDA com as seguintes exceções:

- Informações de Geo/Localidade — Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na Geo). Por exemplo, se o VDA for provisionado de um data center no Reino Unido e o cliente estiver se conectando da Índia, o usuário espera ver in.msn.com. Em vez disso, o usuário vê uk.msn.com.
- Conteúdo multimídia — Sites que contêm conteúdo de mídia rica, quando renderizados no dispositivo cliente, proporcionam aos usuários finais uma experiência nativa e também economizam largura de banda, mesmo em redes de alta latência. Esse recurso redireciona sites com outros tipos de mídia, como Silverlight. Esse processo ocorre em um ambiente seguro. Ou seja, as URLs que o administrador aprova são executadas no cliente, enquanto o restante das URLs é redirecionado para o VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, ele deverá ter acesso ao arquivo para abri-lo. Portanto, você só pode abrir arquivos que residem em

compartilhamentos de rede ou em unidades de cliente (usando o mapeamento de unidade de cliente) usando aplicativos locais. Por exemplo, ao abrir um arquivo PDF, se um leitor de PDF for um aplicativo local, o arquivo será aberto usando esse leitor de PDF. Como o aplicativo local pode acessar o arquivo diretamente, não há transferência de rede do arquivo via ICA® para abri-lo.

Requisitos, considerações e limitações

Oferecemos suporte ao Acesso a Aplicativos Locais nos sistemas operacionais válidos para VDAs para Windows Multi-session OS e para VDAs para Windows Single-session OS. O Acesso a Aplicativos Locais requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são suportados:

- Edge, versão mais recente
- Firefox, versão mais recente e versão de suporte estendido
- Chrome, versão mais recente

Revise as seguintes considerações e limitações ao usar o Acesso a Aplicativos Locais e o redirecionamento de URL.

- O Acesso a Aplicativos Locais foi projetado para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o Acesso a Aplicativos Locais com um desktop virtual que é executado no modo de janela ou não cobre todos os monitores.
  - Vários monitores — Quando um monitor é maximizado, ele se torna o desktop padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo que os aplicativos subsequentes normalmente iniciem em outro monitor.
  - O recurso suporta um VDA. Não há integração com múltiplos VDAs simultâneos.
- Alguns aplicativos podem se comportar de forma inesperada, afetando os usuários:
  - As letras das unidades podem confundir os usuários, como C: local em vez da unidade C: da área de trabalho virtual.
  - As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
  - Aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados no cliente.
  - Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).

  - Aplicativos locais aparecem com o tema do Windows da máquina local.
  - Aplicativos em tela cheia não são suportados. Esses aplicativos incluem aplicativos que abrem em tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem a área de trabalho inteira.
  - O Acesso a Aplicativos Locais copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e no menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
  - Aplicativos que personalizam como a ordem das janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
  - Atalhos não são suportados, incluindo Meu Computador, Lixeira, Painel de Controle, atalhos de Unidade de Rede e atalhos de pasta.
  - Os seguintes tipos de arquivo e arquivos não são suportados: tipos de arquivo personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
  - O agrupamento da barra de tarefas não é suportado para aplicativos hospedados no cliente ou VDA mistos de 32 bits e 64 bits. Ou seja, agrupar aplicativos locais de 32 bits com aplicativos VDA de 64 bits.
  - Aplicativos não podem ser iniciados usando COM. Por exemplo, se você clicar em um documento do Office incorporado de dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local falhará.

- Cenários de salto duplo, onde um usuário está iniciando uma área de trabalho virtual de dentro de outra sessão de área de trabalho virtual, não são suportados.
- O redirecionamento de URL suporta apenas URLs explícitas (ou seja, URLs que aparecem na barra de endereços do navegador ou encontradas usando a navegação no navegador, dependendo do navegador).
- O redirecionamento de URL funciona apenas com sessões de desktop, não com sessões de aplicativo.
- A pasta de desktop local em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução localmente se comportam de acordo com as configurações da barra de tarefas estabelecidas para o desktop virtual. No entanto, os atalhos para aplicativos em execução localmente não são agrupados com instâncias em execução desses aplicativos. Eles também não são agrupados com instâncias em execução de aplicativos hospedados ou atalhos fixados para aplicativos hospedados. Os usuários podem fechar apenas janelas de aplicativos em execução localmente a partir da Barra de Tarefas. Embora os usuários possam fixar janelas de aplicativos locais na Barra de Tarefas e no menu

Iniciar do desktop, os aplicativos podem não iniciar de forma consistente ao usar esses atalhos.

- Se você definir a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**, o redirecionamento de conteúdo do navegador não é suportado. Por padrão, o Acesso a Aplicativos Locais é proibido.

Interação com o Windows

A interação do Acesso a Aplicativos Locais com o Windows inclui os seguintes comportamentos.

- Comportamento de atalho do Windows 8 e Windows Server 2012
  - Os aplicativos da Windows Store instalados no cliente não são enumerados como parte dos atalhos do Acesso a Aplicativos Locais.
  - Arquivos de imagem e vídeo são abertos por padrão usando aplicativos da Windows Store. No entanto, o Acesso a Aplicativos Locais enumera os aplicativos da Windows Store e abre atalhos com aplicativos de desktop.
- Programas Locais
  - Para o Windows 7, a pasta está disponível no menu Iniciar.
  - Para o Windows 8, Programas Locais está disponível apenas quando o usuário escolhe **Todos os Aplicativos** como uma categoria na tela Iniciar. Nem todas as subpastas são exibidas em Programas Locais.
- Recursos gráficos do Windows 8 para aplicativos
  - Os aplicativos de desktop são restritos à área de trabalho e são cobertos pela tela Iniciar e aplicativos estilo Windows 8.
  - Os aplicativos de Acesso a Aplicativos Locais não se comportam como aplicativos de desktop no modo de vários monitores. No modo de vários monitores, a tela Iniciar e a área de trabalho são exibidas em monitores diferentes.
- Windows 8 e Redirecionamento de URL de Acesso a Aplicativos Locais
  - Como o Internet Explorer do Windows 8 não tem complementos habilitados, use o Internet Explorer da área de trabalho para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desabilita os complementos por padrão. Para implementar o Redirecionamento de URL, desabilite a configuração aprimorada do Internet

Explorer. Em seguida, redefina as opções do Internet Explorer e reinicie para garantir que os complementos estejam habilitados para usuários padrão.

Configurar Acesso a Aplicativos Locais e redirecionamento de URL

Para usar o Acesso a Aplicativos Locais e o redirecionamento de URL com o aplicativo Citrix Workspace™:

- Instale o aplicativo Citrix Workspace na máquina cliente local. Você pode habilitar ambos os recursos durante a instalação do aplicativo Citrix Workspace ou pode habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo.
- Defina a configuração de política **Permitir Acesso a Aplicativos Locais** como **Ativado**. Você também pode configurar as configurações de política de lista de permissões e lista de bloqueios de URL para redirecionamento de URL. Para obter mais informações, consulte Configurações de política de Acesso a Aplicativos Locais.

Habilitar Acesso a Aplicativos Locais e redirecionamento de URL

Para habilitar o Acesso a Aplicativos Locais para todos os aplicativos locais, siga estas etapas:

1. Faça login no Web Studio e clique em **Políticas** no painel esquerdo.
2. Na barra de ações, clique em **Criar Política**.
3. Na janela Criar Política, digite "Permitir Acesso a Aplicativos Locais" na caixa de pesquisa e clique em **Selecionar**.
4. Na janela Editar Configuração, selecione **Permitido**. Por padrão, a política **Permitir acesso a aplicativos locais** é proibida. Quando essa configuração é permitida, o VDA permite que o usuário final decida se os aplicativos publicados e os atalhos de Acesso a Aplicativos Locais são habilitados na sessão. (Quando essa configuração é proibida, tanto os aplicativos publicados quanto os atalhos de Acesso a Aplicativos Locais não funcionam para o VDA.) Essa configuração de política se aplica a toda a máquina e à política de redirecionamento de URL.
5. Na janela Criar Política, digite "Lista de permissões de redirecionamento de URL" na caixa de pesquisa e clique em **Selecionar**. A lista de permissões de redirecionamento de URL especifica URLs a serem abertas no navegador padrão da sessão remota.
6. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.

7. Na janela Criar Política, digite "Lista de bloqueios de redirecionamento de URL" na caixa de pesquisa e clique em **Selecionar**. A lista de bloqueios de redirecionamento de URL especifica URLs que são redirecionadas para o navegador padrão em execução no endpoint.
8. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
9. Na página Configurações, clique em **Avançar**.
10. Na página Usuários e Máquinas, atribua a política aos Grupos de Entrega aplicáveis e, em seguida, clique em **Avançar**.
11. Na página Resumo, revise as configurações e, em seguida, clique em **Concluir**.

Para habilitar o redirecionamento de URL para todos os aplicativos locais durante a instalação do aplicativo Citrix Workspace, siga estas etapas:

1. Habilite o redirecionamento de URL ao instalar o aplicativo Citrix Workspace para todos os usuários em uma máquina. Isso também registra os complementos do navegador necessários para o redirecionamento de URL.
2. No prompt de comando, execute o comando apropriado para instalar o aplicativo Citrix Workspace usando uma das seguintes opções:
   - Para CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Para CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo

Observação:

- Antes de habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, adicione os arquivos de modelo receiver.admx/adml ao GPO local.
- Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Modelos Administrativos > Componentes Citrix > Citrix Workspace** somente quando você adiciona o CitrixBase.admx/CitrixBase.adml à pasta %systemroot%\policyDefinitions.

> Para habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá para **Configuração do Computador > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Clique em **Configurações de Acesso a Aplicativos Locais**.
4. Selecione **Habilitado** e, em seguida, selecione **Permitir Redirecionamento de URL**. Para redirecionamento de URL, registre os complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais adiante neste artigo.

Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o SDK do PowerShell.

Para o Editor do Registro, consulte O Acesso a Aplicativos Locais para aplicativos publicados na lista de recursos gerenciados através do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina onde o Delivery Controller™ está sendo executado.
2. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Para ter acesso a **Adicionar Aplicativo de Acesso a Aplicativos Locais** em uma implantação de serviço de Nuvem, use o SDK do PowerShell Remoto do Citrix DaaS. Para obter mais informações, consulte SDK do PowerShell Remoto do Citrix DaaS.

1. Baixe o instalador:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`
2. Execute estes comandos:
   a. `asnp citrix.*`.
   b. `Get-XdAuthentication`
3. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Depois de concluir as etapas anteriores aplicáveis, siga estas etapas para continuar.

1. Faça login no Web Studio e selecione **Aplicativos** no painel esquerdo.
2. No painel superior central, clique com o botão direito na área em branco e selecione **Adicionar Aplicativo de Acesso a Aplicativo Local** no menu de contexto. Você também pode clicar em **Adicionar Aplicativo de Acesso a Aplicativo Local** na barra de ações. Para exibir a opção Adicionar Aplicativo de Acesso a Aplicativo Local na barra de ações, clique em **Atualizar**.
3. Publique o aplicativo Local App Access.

    - O assistente de Acesso a Aplicativos Locais é iniciado com uma página de Introdução, que você pode remover de futuras inicializações do assistente.
    - O assistente o guiará pelas páginas Grupos, Localização, Identificação, Entrega e Resumo, descritas abaixo. Ao terminar cada página, clique em **Next** até chegar à página Resumo.
    - Na página Grupos, selecione um ou mais Delivery Groups onde os novos aplicativos serão adicionados e, em seguida, clique em **Next**.
    - Na página Localização, digite o caminho executável completo do aplicativo na máquina local do usuário e digite o caminho para a pasta onde o aplicativo está localizado. A Citrix recomenda que você use o caminho da variável de ambiente do sistema; por exemplo, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
    - Na página Identificação, aceite os valores padrão ou digite as informações desejadas e, em seguida, clique em **Next**.
    - Na página Entrega, configure como este aplicativo é entregue aos usuários e então clique em **Avançar**. 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 é visível no menu Iniciar, na área de trabalho ou em ambos.
    - Na página Resumo, revise as configurações e, em seguida, clique em **Finish** para sair do assistente de Acesso a Aplicativos Locais.

Registrar complementos do navegador

> **Observação:**

> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente ao instalar o aplicativo Citrix Workspace a partir da linha de comando usando a opção /ALLOW_CLIENTHOSTEDAPPSURL=1.

> Você pode usar os seguintes comandos para registrar e cancelar o registro de um ou todos os complementos:

- Para registrar complementos em um dispositivo cliente: \<*pasta-de-instalação-do-cliente*>\redirector.exe /reg\<*navegador*>
- Para cancelar o registro de complementos em um dispositivo cliente: \<*pasta-de-instalação-do-cliente*>\redirector.exe /unreg\<*navegador*>
- Para registrar complementos em um VDA: \<*pasta-de-instalação-do-VDA*>\VDARedirector.exe /reg\<*navegador*>
- Para cancelar o registro de complementos em um VDA: \<*pasta-de-instalação-do-VDA*>\VDARedirector.exe /unreg\<*navegador*>

Onde \<*navegador*> é Internet Explorer, Firefox, Chrome ou Todos.

Por exemplo, o seguinte comando registra complementos do Internet Explorer em um dispositivo que executa o aplicativo Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

O seguinte comando registra todos os complementos em um VDA de SO multissessão do Windows.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

Intercepção de URL entre navegadores

- Por padrão, o Internet Explorer redireciona a URL especificada. Se a URL não estiver na lista de bloqueio, mas o navegador ou site a redirecionar para outra URL, a URL final não será redirecionada. Ela não é redirecionada mesmo que esteja na lista de bloqueio.

Para que o redirecionamento de URL funcione corretamente, habilite o complemento quando solicitado pelo navegador. Se os complementos que usam as opções da Internet ou os complementos no prompt estiverem desabilitados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam as URLs.

Quando um complemento é instalado, o Firefox solicita que você permita ou impeça a instalação do complemento em uma nova página de guia. Permita o complemento para que o recurso funcione.

- O complemento do Chrome sempre redireciona a URL final para a qual se navega, e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desativa a extensão, o recurso de redirecionamento de URL não funciona no Chrome. Se o redirecionamento de URL for necessário no modo de navegação anônima, permita que a extensão seja executada nesse modo nas configurações do navegador.

Configurar o comportamento do aplicativo local ao fazer logoff e desconectar

> **Observação:**
>
> Se você não seguir estas etapas para configurar as definições, por padrão, os aplicativos locais continuarão a ser executados quando um usuário fizer logoff ou se desconectar da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.

Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, consulte Comportamento do aplicativo local ao fazer logoff e desconectar na lista de recursos gerenciados por meio do registro.

Redirecionamento USB genérico e considerações sobre unidades de cliente

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes com alta latência ou sensíveis à segurança.

A tecnologia HDX oferece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde este é inadequado, por exemplo:

- O dispositivo USB possui recursos mais avançados que não fazem parte do suporte otimizado, como um mouse ou webcam com mais botões.

- Os usuários precisam de funções que não fazem parte do suporte otimizado.
- O dispositivo USB é um dispositivo especializado, como equipamento de teste e medição ou um controlador industrial.
- Um aplicativo requer acesso direto ao dispositivo como um dispositivo USB.
- O dispositivo USB possui apenas um driver Windows disponível. Por exemplo, um leitor de cartão inteligente pode não ter um driver disponível para o aplicativo Citrix Workspace™ para Android.
- A versão do aplicativo Citrix Workspace não oferece suporte otimizado para este tipo de dispositivo USB.

Com o redirecionamento USB genérico:

- Os usuários não precisam instalar drivers de dispositivo no dispositivo do usuário.
- Os drivers de cliente USB são instalados na máquina VDA.

Importante:

- O redirecionamento USB genérico pode ser usado em conjunto com o suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as configurações de política de dispositivos USB da Citrix para redirecionamento USB genérico e suporte otimizado.
- A configuração de política da Citrix em Regras de otimização de dispositivo USB do cliente é uma configuração específica para redirecionamento USB genérico, para um dispositivo USB específico. Ela não se aplica ao suporte otimizado conforme descrito aqui.

Considerações de desempenho para dispositivos USB

A latência da rede e a largura de banda podem afetar a experiência do usuário e a operação do dispositivo USB ao usar o redirecionamento USB genérico para alguns tipos de dispositivos USB. Por exemplo, dispositivos sensíveis ao tempo podem não operar corretamente em links de alta latência e baixa largura de banda. Use o suporte otimizado em vez disso, sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para serem utilizáveis, por exemplo, um mouse 3D (usado com aplicativos 3D que também geralmente exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você poderá mitigar o problema ajustando o uso da

largura de banda de outros componentes usando as configurações da política de largura de banda. Para obter mais informações, consulte Configurações da política de largura de banda para redirecionamento de dispositivo USB do cliente e Configurações da política de conexão multi-stream.

Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartão inteligente, leitores de impressão digital e mesas digitalizadoras de assinatura. Outros dispositivos USB, como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser confidenciais.

Dispositivos USB são frequentemente usados para distribuir malware. A configuração do Citrix Workspace app e do Citrix Virtual Apps and Desktops™ pode reduzir, mas não eliminar, o risco desses dispositivos USB. Essa situação se aplica independentemente de ser usado o redirecionamento USB genérico ou o suporte otimizado.

Importante:

Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX, consulte Comunicação entre cliente e VDA.

Habilite o suporte apenas para os dispositivos USB de que você precisa. Configure o redirecionamento USB genérico e o suporte otimizado para atender a essa necessidade.

Forneça orientação aos usuários para o uso seguro de dispositivos USB:

- Use apenas dispositivos USB que foram obtidos de uma fonte confiável.
- Não deixe dispositivos USB sem vigilância em ambientes abertos - por exemplo, um pen drive em um cybercafé.
- Explique os riscos de usar um dispositivo USB em mais de um computador.

Compatibilidade com redirecionamento USB genérico

O redirecionamento USB genérico é compatível com dispositivos USB 2.0 e anteriores. O redirecionamento USB genérico também é compatível com dispositivos USB 3.0 conectados a uma porta USB 2.0 ou USB 3.0. O redirecionamento USB genérico não oferece suporte a recursos USB introduzidos no USB 3.0, como super velocidade.

Estes aplicativos Citrix Workspace oferecem suporte ao redirecionamento USB genérico:

- Citrix Workspace app para Windows, consulte Configurando a entrega de aplicativos.
- Citrix Workspace app para Mac, consulte Citrix Workspace app for Mac.
- Citrix Workspace app para Linux, consulte Otimizar.
- Citrix Workspace app para Chrome OS, consulte Citrix Workspace app for Chrome.

Para as versões do Citrix Workspace app, consulte a matriz de recursos do Citrix Workspace app.

Se você estiver usando versões anteriores do Citrix Workspace app, consulte a documentação do Citrix Workspace app para confirmar se o redirecionamento genérico de USB é compatível. Consulte a documentação do Citrix Workspace app para quaisquer restrições sobre os tipos de dispositivos USB compatíveis.

O redirecionamento genérico de USB é compatível com sessões de desktop do VDA para SO de sessão única, da versão 7.6 até a atual.

O redirecionamento genérico de USB é compatível com sessões de desktop do VDA para SO de múltiplas sessões, da versão 7.6 até a atual, com estas restrições:

- O VDA deve estar executando o Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o Host da Sessão da Área de Trabalho Remota (RDSH) para o SO do VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não são compatíveis com o redirecionamento genérico de USB porque não seria útil redirecioná-los:

- Modems USB.
- Adaptadores de rede USB.
- Hubs USB. Os dispositivos USB conectados aos hubs USB são tratados individualmente.

- Portas COM virtuais USB. Use o redirecionamento de porta COM em vez do redirecionamento genérico de USB.

Para obter informações sobre dispositivos USB que foram testados com o redirecionamento genérico de USB, consulte Citrix Ready Marketplace. Alguns dispositivos USB não funcionam corretamente com o redirecionamento genérico de USB.

Configurar redirecionamento USB genérico

Você pode controlar e configurar separadamente quais tipos de dispositivos USB usam o redirecionamento USB genérico:

- No VDA, usando as configurações de política do Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações de política de dispositivos USB na referência de configurações de política.
- No aplicativo Citrix Workspace, usando mecanismos dependentes do aplicativo Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações de registro que configuram o aplicativo Citrix Workspace para Windows. Por padrão, o redirecionamento USB é permitido para certas classes de dispositivos USB e negado para outras. Para obter mais informações, consulte Configurar na documentação do aplicativo Citrix Workspace para Windows.

Essa configuração separada oferece flexibilidade. Por exemplo:

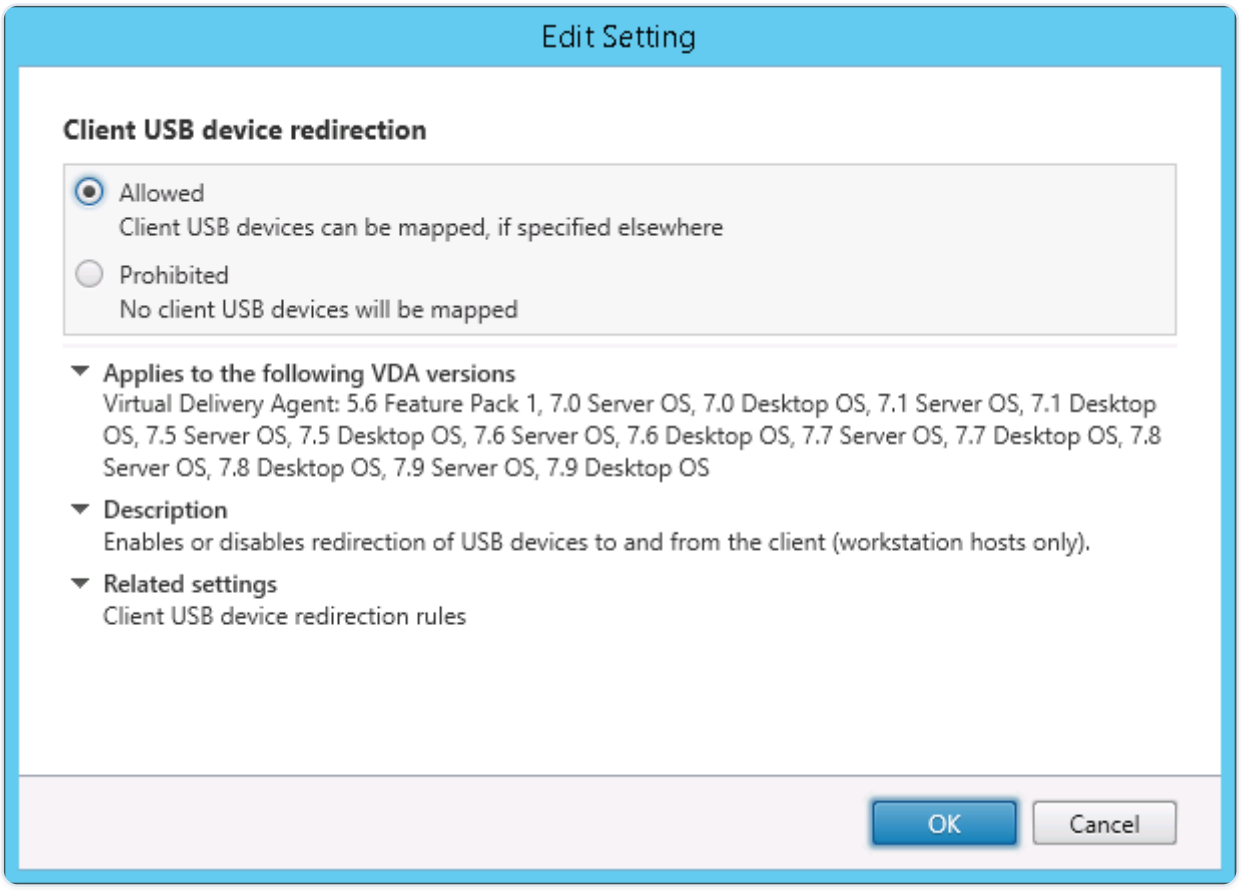
- Se duas organizações ou departamentos diferentes forem responsáveis pelo aplicativo Citrix Workspace e pelo VDA, eles poderão impor o controle separadamente. Essa configuração se aplica quando um usuário em uma organização acessa um aplicativo em outra organização.
- As configurações de política do Citrix podem controlar dispositivos USB que são permitidos apenas para determinados usuários ou para usuários que se conectam apenas por uma LAN (em vez de usar o Citrix Gateway).

Habilitar redirecionamento USB genérico

Para habilitar o redirecionamento USB genérico e não exigir redirecionamento manual pelo usuário, configure as configurações de política do Citrix e as preferências de conexão do aplicativo Citrix Workspace.

Nas configurações de política do Citrix:

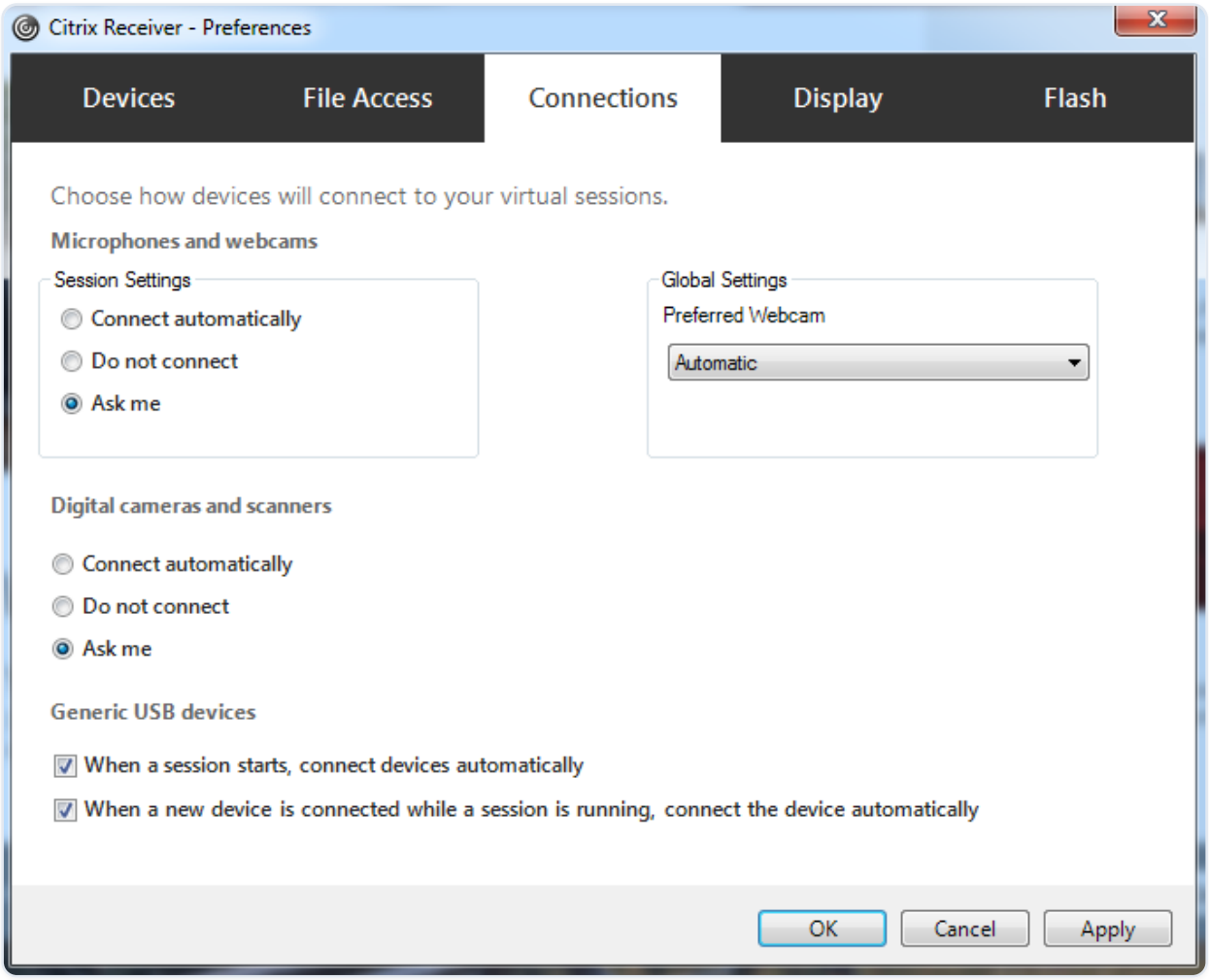
1. Adicione o Redirecionamento de dispositivo USB do cliente a uma política e defina seu valor como **Permitido**.



2. (Opcional) Para atualizar a lista de dispositivos USB disponíveis para redirecionamento, adicione a configuração Regras de redirecionamento de dispositivo USB do cliente a uma política e especifique as regras de política USB.

   Depois que as configurações de política estiverem concluídas, no aplicativo Citrix Workspace:

3. Especifique que os dispositivos sejam conectados automaticamente sem redirecionamento manual. Você pode fazer isso usando um modelo administrativo ou no aplicativo Citrix Workspace para **Windows > Preferências > Conexões**.



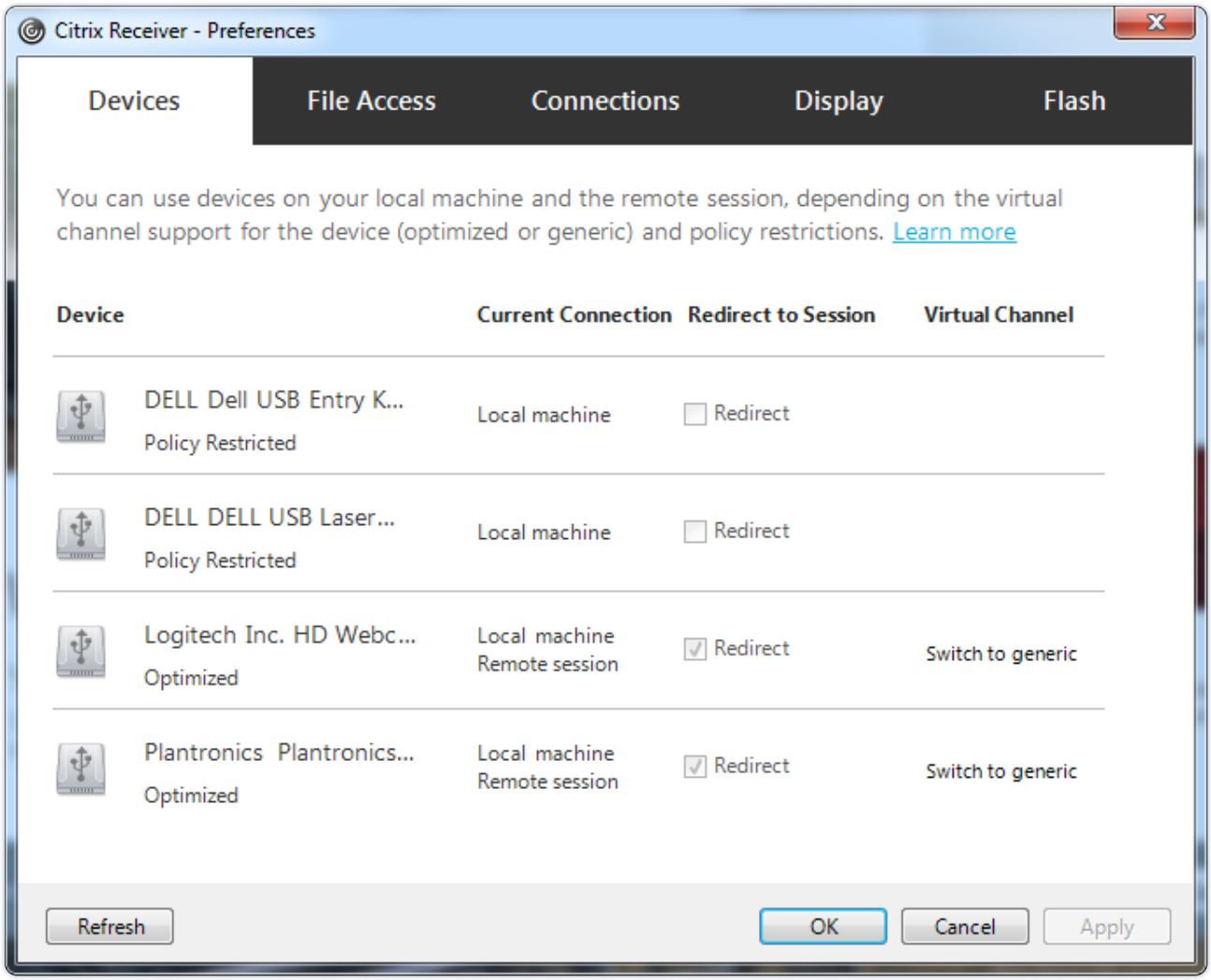
Se você especificou as regras de política USB para o VDA na etapa anterior, especifique essas mesmas regras de política para o aplicativo Citrix Workspace.

Para thin clients, consulte o fabricante para obter detalhes sobre o suporte USB e qualquer configuração necessária.

Configurando os tipos de dispositivos USB disponíveis para redirecionamento USB genérico

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado e as configurações de preferência do usuário USB estão definidas para conectar dispositivos USB automaticamente. Os dispositivos USB também são redirecionados automaticamente quando a barra de conexão não está presente.

Os usuários podem redirecionar explicitamente dispositivos que não são redirecionados automaticamente, selecionando os dispositivos na lista de dispositivos USB. Para obter mais informações, consulte o artigo de ajuda do usuário do aplicativo Citrix Workspace para Windows, Exibir seus dispositivos no Desktop Viewer.



Para usar o redirecionamento USB genérico em vez do suporte otimizado, você pode:

- No aplicativo Citrix Workspace, selecione manualmente o dispositivo USB para usar o redirecionamento USB genérico, escolha **Alternar para genérico** na guia Dispositivos da caixa de diálogo Preferências.
- Selecione automaticamente o dispositivo USB para usar o redirecionamento USB genérico, configurando o redirecionamento automático para o tipo de dispositivo USB (por exemplo, AutoRedirectStorage=1) e defina as configurações de preferência do usuário USB para conectar dispositivos USB automaticamente. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

> **Observação:**
>
> Configure o redirecionamento USB genérico para uso com uma webcam apenas se a webcam for considerada incompatível com o redirecionamento multimídia HDX.

> Para evitar que os dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e o VDA.

Para o redirecionamento USB genérico, você precisa saber pelo menos a classe e a subclasse do dispositivo USB. Nem todos os dispositivos USB usam sua classe e subclasse de dispositivo USB óbvias. Por exemplo:

- Canetas usam a classe de dispositivo mouse.
- Leitores de cartão inteligente podem usar a classe de dispositivo definida pelo fornecedor ou HID.

Para um controle mais preciso, você precisa saber o ID do Fornecedor, o ID do Produto e o ID da Versão. Você pode obter essas informações do fornecedor do dispositivo.

> **Importante:**

> Dispositivos USB maliciosos podem apresentar características de dispositivo USB que não correspondem ao seu uso pretendido. As regras de dispositivo não se destinam a impedir esse comportamento.

> Você controla os dispositivos USB disponíveis para redirecionamento USB genérico especificando regras de redirecionamento de dispositivo USB, para substituir as regras de política USB padrão.

Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops):

- Na maioria dos casos, baixe o MSI do Console de Gerenciamento de Política de Grupo do Citrix (`CitrixGroupPolicyManagement_x64.msi`) e instale-o em seu sistema Active Directory e, em seguida, gerencie as políticas de grupo do AD. (Não instale o MSI em um VDA.)
- Para o Citrix Workspace app para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: raiz do DVD `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops no local:

- Para o VDA, edite as regras de substituição do administrador para as máquinas de SO de várias sessões por meio de regras de política de grupo. O Console de Gerenciamento de Política de Grupo está incluído na mídia de instalação:
  - x64: raiz do DVD `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: raiz do DVD `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Para o Citrix Workspace app para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: raiz do DVD `\os\lang\Support\Configuration\icaclient_usb.adm`

Aviso:

A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

As regras padrão do produto são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB. Não edite essas regras padrão do produto. Em vez disso, use-as como um guia para criar regras de substituição do administrador, o que é explicado mais adiante neste artigo. As substituições de GPO são avaliadas antes das regras padrão do produto.

As regras de substituição do administrador são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. As regras de política de GPO têm o formato **{Allow: `|` Deny:}** seguido por um conjunto de expressões *tag=value* separadas por espaço em branco.

As seguintes tags são suportadas:

TAG	DESCRIÇÃO
VID	ID do Fornecedor do descritor do dispositivo

TAG	DESCRIÇÃO
PID	ID do Produto do descritor do dispositivo
REL	ID de Lançamento do descritor do dispositivo
Classe	Classe do descritor do dispositivo ou de um descritor de interface; consulte o site da USB em `<http://www.usb.org/>` para obter os Códigos de Classe USB disponíveis
Subclasse	Subclasse do descritor do dispositivo ou de um descritor de interface
Prot	Protocolo do descritor do dispositivo ou de um descritor de interface

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por `#`. Um delimitador não é necessário, e o comentário é ignorado para fins de correspondência.
- Linhas em branco e de comentário puro são ignoradas.
- Espaços em branco são usados como separadores, mas não podem aparecer no meio de um número ou identificador. Por exemplo, Deny: Class = 08 SubClass=05 é uma regra válida, mas Deny: Class=0 Sub Class=05 não é.
- As tags devem usar o operador de correspondência =. Por exemplo, VID=1230.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.

Observação:

- A partir do Citrix Virtual Apps and Desktops versão 2212, alguns dos dispositivos USB são desabilitados de usar o recurso de Redirecionamento USB Genérico. Você deve adicionar esses dispositivos explicitamente usando seus respectivos ID de Fornecedor (VID) e ID de Produto (PID).

- 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 Citrix Workspace app para Windows, o seguinte se aplica:

- Dispositivos conectados após o início de uma sessão aparecem imediatamente no menu USB do Desktop Viewer.
- Se um dispositivo USB não estiver sendo redirecionado corretamente, você pode tentar resolver o problema esperando para conectar o dispositivo até depois que a sessão virtual for iniciada.
- Para evitar 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. Este suporte faz parte do mapeamento de unidade cliente do Citrix Virtual Apps and Desktops. As unidades no dispositivo do usuário são mapeadas automaticamente para letras de unidade na área de trabalho virtual quando os usuários fazem logon. As unidades são exibidas como pastas compartilhadas que têm letras de unidade mapeadas. Para configurar o mapeamento de unidade cliente, use a

configuração **Unidades removíveis do cliente**. Essa configuração está na seção Configurações de política de redirecionamento de arquivo das configurações de política ICA.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos. Controle-os usando políticas Citrix. As principais diferenças são:

RECURSO	MAPEAMENTO DE UNIDADE CLIENTE	REDIRECIONAMENTO USB GENÉRICO
Habilitado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado	Sim
Dispositivos BitLocker To Go	Não	Não
Seguro para excluir o dispositivo durante uma sessão	Não	Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura

Se as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estiverem habilitadas e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidade cliente. Quando as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estão habilitadas e um dispositivo é configurado para redirecionamento automático e um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão, ele é redirecionado usando o redirecionamento USB genérico. Para obter mais informações, consulte o artigo do Knowledge Center CTX123015.

> **Observação:**
>
> O redirecionamento USB é suportado em conexões de menor largura de banda, por exemplo, 50 Kbps. No entanto, a cópia de arquivos grandes não funciona.

Imprimir

Gerenciar impressoras em seu ambiente é um processo de várias etapas:

1. Familiarize-se com os conceitos de impressão, se ainda não o fez.
2. Planeje sua arquitetura de impressão. Isso inclui analisar suas necessidades de negócios, sua infraestrutura de impressão existente, como seus usuários e aplicativos interagem com a impressão hoje e qual modelo de gerenciamento de impressão melhor se aplica ao seu ambiente.
3. Configure seu ambiente de impressão selecionando um método de provisionamento de impressora e, em seguida, criando políticas para implantar seu design de impressão. Atualize as políticas quando novos funcionários ou servidores forem adicionados.
4. Teste uma configuração de impressão piloto antes de implantá-la para os usuários.
5. Mantenha seu ambiente de impressão Citrix® gerenciando drivers de impressora e otimizando o desempenho da impressão.
6. Solucione problemas que possam surgir.

Conceitos de impressão

Antes de começar a planejar sua implantação, certifique-se de que você entende estes conceitos essenciais para impressão:

- Os tipos de provisionamento de impressora disponíveis
- Como os trabalhos de impressão são roteados
- Os fundamentos do gerenciamento de drivers de impressora

Os conceitos de impressão são baseados nos conceitos de impressão do Windows. Para configurar e gerenciar com sucesso a impressão em seu ambiente, você deve entender como a impressão de rede e cliente do Windows funciona e como isso se traduz em comportamento de impressão neste ambiente.

Processo de impressão

Nesse ambiente, toda a impressão é iniciada (pelo usuário) em máquinas que hospedam aplicativos. Os trabalhos de impressão são redirecionados através do servidor de impressão de rede ou dispositivo do usuário para o dispositivo de impressão.

Não há espaço de trabalho persistente para usuários de desktops e aplicativos virtuais. Quando uma sessão termina, o espaço de trabalho do usuário é excluído, portanto, todas as configurações precisam ser reconstruídas no início de cada sessão. Como resultado, cada vez que um usuário inicia uma nova sessão, o sistema deve reconstruir o espaço de trabalho do usuário.

Quando um usuário imprime:

- Determina quais impressoras fornecer ao usuário. Isso é conhecido como provisionamento de impressora.
- Restaura as preferências de impressão do usuário.
- Determina qual impressora é a padrão para a sessão.

Você pode personalizar como executar essas tarefas configurando opções para provisionamento de impressoras, roteamento de trabalhos de impressão, retenção de propriedades de impressora e gerenciamento de drivers. Certifique-se de avaliar como as várias configurações de opção podem alterar o desempenho da impressão em seu ambiente e a experiência do usuário.

Provisionamento de impressora

O processo que torna as impressoras disponíveis em uma sessão é conhecido como provisionamento. O provisionamento de impressoras é tipicamente tratado dinamicamente. Ou seja, as impressoras que aparecem em uma sessão não são predeterminadas e armazenadas. Em vez disso, as impressoras são montadas, com base em políticas, à medida que a sessão é construída durante o logon e a reconexão. Como resultado, as impressoras podem mudar de acordo com a política, localização do usuário e alterações de rede, desde que sejam refletidas nas políticas. Assim, usuários que se deslocam para um local diferente podem ver alterações em seu espaço de trabalho.

O sistema também monitora as impressoras do lado do cliente e ajusta dinamicamente as impressoras criadas automaticamente na sessão com base em adições, exclusões e alterações nas impressoras do lado do cliente. Essa descoberta dinâmica de impressoras beneficia usuários móveis à medida que se conectam de vários dispositivos.

Os métodos mais comuns de provisionamento de impressoras são:

- **Universal Print Server** — O Citrix Universal Print Server oferece suporte de impressão universal para impressoras de rede. O Universal Print Server usa o driver de impressão universal. Essa solução permite que você use um único driver em uma máquina de SO multi-sessão para permitir a impressão em rede a partir de qualquer dispositivo.

A Citrix recomenda o Citrix Universal™ Print Server para cenários de servidor de impressão remoto. O Universal Print Server transfere o trabalho de impressão pela rede em um formato otimizado e compactado, minimizando assim o uso da rede e melhorando a experiência do usuário.

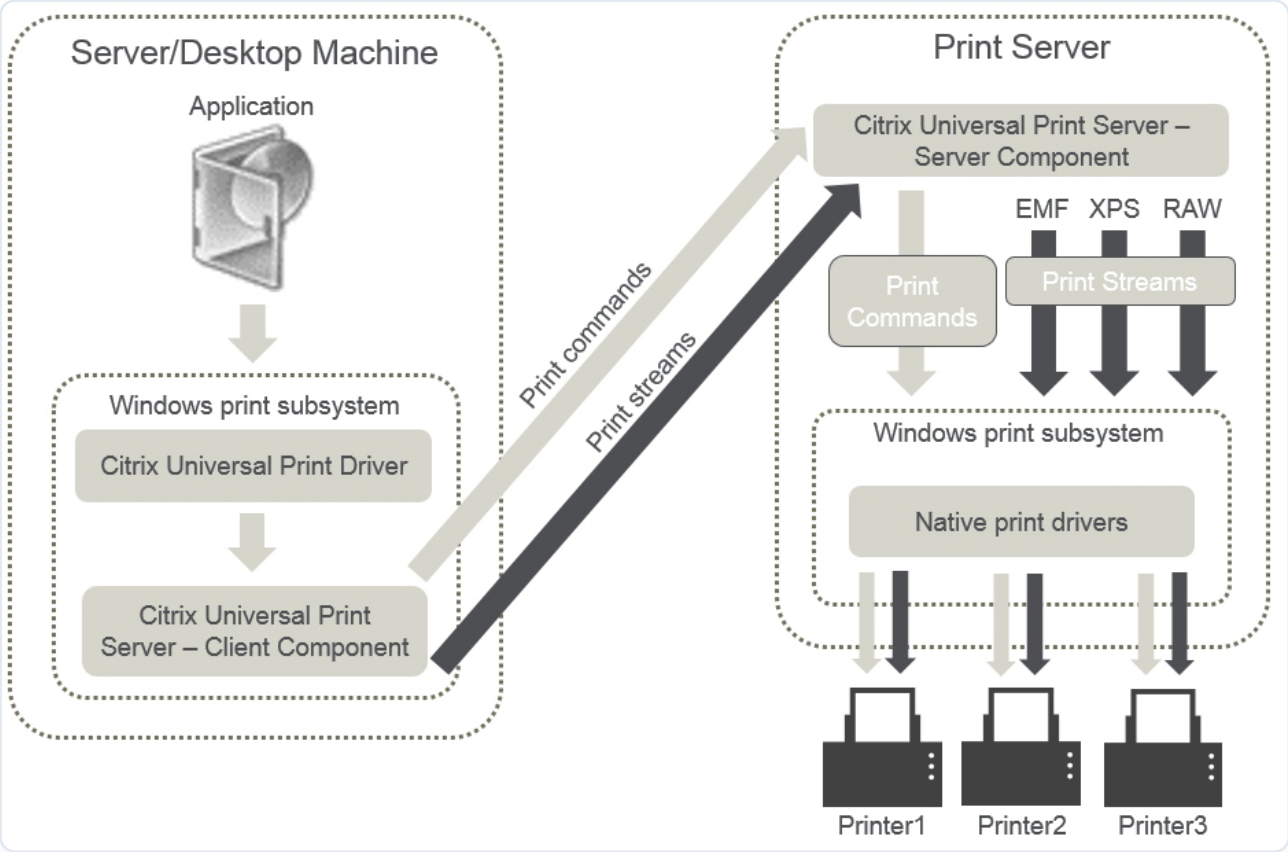
O recurso Universal Print Server compreende:

Um componente cliente, **UPClient** — Habilite o UPClient em cada máquina de SO multi-sessão que provisiona impressoras de rede de sessão e usa o driver de impressão universal.

Um componente de servidor, **UPServer** - Instale o UPServer em cada servidor de impressão que provisiona impressoras de rede de sessão e usa o driver de impressão Universal para as impressoras de sessão (independentemente de as impressoras de sessão serem provisionadas centralmente ou não).

Para requisitos e detalhes de configuração do Universal Print Server, consulte os artigos de requisitos do sistema e instalação.

A ilustração a seguir mostra o fluxo de trabalho típico para uma impressora baseada em rede em um ambiente que usa o Universal Print Server.



Ao habilitar o Citrix Universal Print Server, todas as impressoras de rede conectadas o utilizam automaticamente por meio da descoberta automática.

- **Criação automática** - *Criação automática* refere-se a impressoras criadas automaticamente no início de cada sessão. Tanto impressoras de rede remotas quanto impressoras cliente conectadas localmente podem ser criadas automaticamente. Considere criar automaticamente apenas a impressora cliente padrão para ambientes com um grande número de impressoras por usuário. A criação automática de um número menor de impressoras usa menos sobrecarga (memória e CPU) em máquinas de SO de múltiplas sessões. Minimizar as impressoras criadas automaticamente também pode reduzir os tempos de logon do usuário.

  As impressoras criadas automaticamente são baseadas em:

  - As impressoras instaladas no dispositivo do usuário.
  - Quaisquer políticas que se apliquem à sessão.

    As configurações da política de criação automática permitem limitar o número ou o tipo de impressoras que são criadas automaticamente. Por padrão, as impressoras estão disponíveis nas sessões ao configurar automaticamente todas as impressoras no dispositivo do usuário, incluindo impressoras conectadas localmente e de rede.

  Depois que o usuário encerra a sessão, as impressoras para essa sessão são excluídas.

A criação automática de impressoras cliente e de rede tem manutenção associada. Por exemplo, adicionar uma impressora exige que você:

- Atualize a configuração da política de impressoras de sessão.
- Adicione o driver a todas as máquinas de SO de múltiplas sessões usando a configuração da política de mapeamento e compatibilidade de driver de impressora.

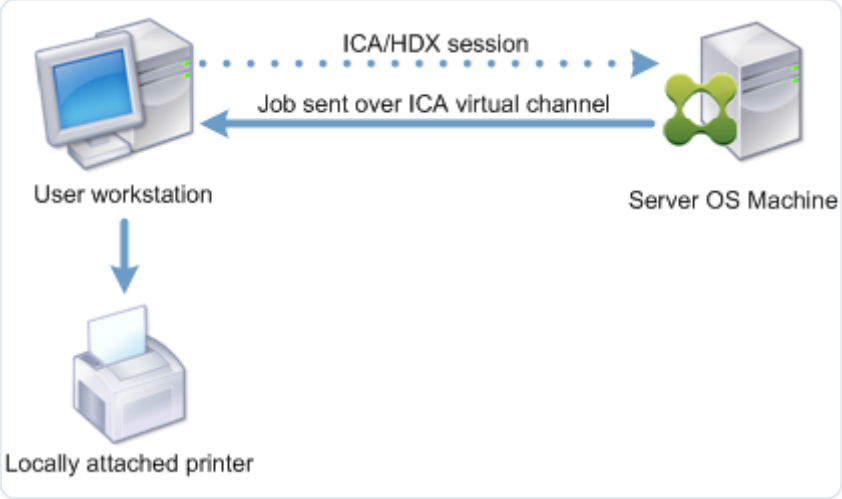
Roteamento de trabalho de impressão

O termo caminho de impressão abrange tanto o caminho pelo qual os trabalhos de impressão são roteados quanto o local onde os trabalhos de impressão são armazenados em spool. Ambos os aspectos desse conceito são importantes. O roteamento afeta o tráfego de rede. O spooling afeta a utilização de recursos locais no dispositivo que processa o trabalho.

Nesse ambiente, os trabalhos de impressão podem seguir dois caminhos para um dispositivo de impressão: através do cliente ou através de um servidor de impressão de rede. Esses caminhos são chamados de caminho de impressão do cliente e caminho de impressão de rede. Qual caminho é escolhido por padrão depende do tipo de impressora utilizada.

Impressoras conectadas localmente

O sistema roteia trabalhos para impressoras conectadas localmente a partir da máquina Multi-session OS, através do cliente e, em seguida, para o dispositivo de impressão. O protocolo ICA® otimiza e compacta o tráfego do trabalho de impressão. Quando um dispositivo de impressão é conectado localmente ao dispositivo do usuário, os trabalhos de impressão são roteados pelo canal virtual ICA.



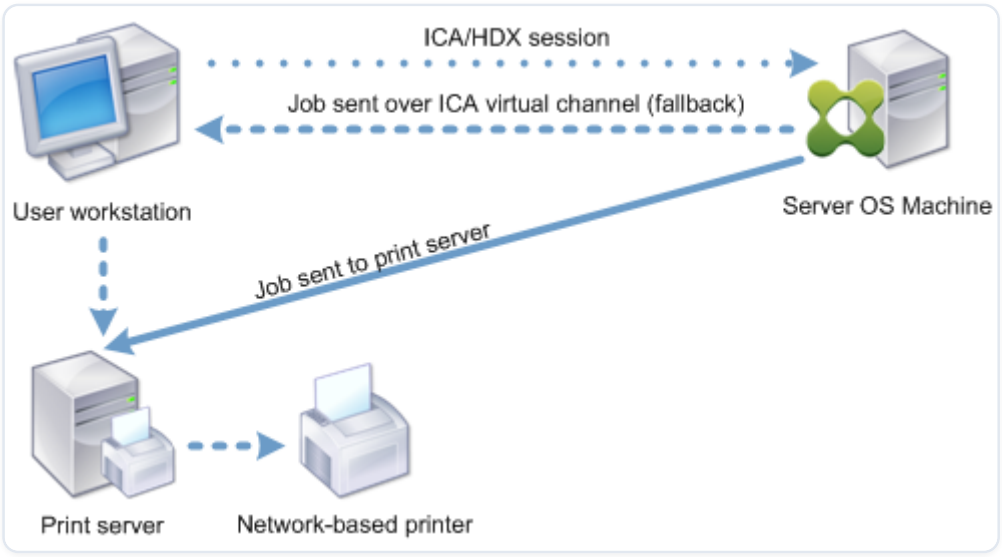
Impressoras baseadas em rede

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina Multi-session OS, através da rede e diretamente para o servidor de impressão. No entanto, os trabalhos de impressão são roteados automaticamente pela conexão ICA nas seguintes situações:

- Se o desktop virtual ou aplicativo não conseguir contatar o servidor de impressão.
- Se o driver de impressora nativo não estiver disponível na máquina Multi-session OS.

Se o Universal Print Server não estiver habilitado, configurar o caminho de impressão do cliente para impressão em rede é útil para conexões de baixa largura de banda, como redes de longa distância, que podem se beneficiar da otimização e compressão de tráfego resultantes do envio de trabalhos pela conexão ICA.

O caminho de impressão do cliente também permite limitar o tráfego ou restringir a largura de banda alocada para trabalhos de impressão. Se o roteamento de trabalhos através do dispositivo do usuário não for possível, como para thin clients sem recursos de impressão, a Qualidade de Serviço deve ser configurada para priorizar o tráfego ICA/HDX e garantir uma boa experiência do usuário na sessão.



Gerenciamento de driver de impressão

O Citrix Universal Printer Driver (UPD) é um driver de impressão independente de dispositivo, compatível com a maioria das impressoras. O Citrix UPD consiste em dois componentes:

Componente do servidor. O Citrix UPD é instalado como parte da instalação do VDA do Citrix Virtual Apps and Desktops™. O VDA instala os seguintes drivers com o Citrix UPD: "Citrix Universal Printer" (driver EMF) e "Citrix XPS Universal Printer" (driver XPS).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

Os instaladores do VDA não oferecem mais opções para controlar a instalação do driver de impressora PDF do Universal Print Server. O driver de impressora PDF agora é sempre instalado automaticamente. Ao atualizar para o VDA 7.17 (ou uma versão posterior compatível), qualquer driver de impressora PDF Citrix instalado anteriormente é automaticamente removido e substituído pela versão mais recente.

Quando um trabalho de impressão é iniciado, o driver registra a saída do aplicativo e a envia, sem qualquer modificação, para o dispositivo de ponto de extremidade.

Componente do cliente. O Citrix UPD é instalado como parte da instalação do aplicativo Citrix Workspace™. Ele busca o fluxo de impressão de entrada para a sessão do Citrix Virtual Apps and Desktops. Em seguida, ele encaminha o fluxo de impressão para o subsistema de impressão local, onde o trabalho de impressão é renderizado usando os drivers de impressora específicos do dispositivo.

O Citrix UPD oferece suporte aos seguintes formatos de impressão:

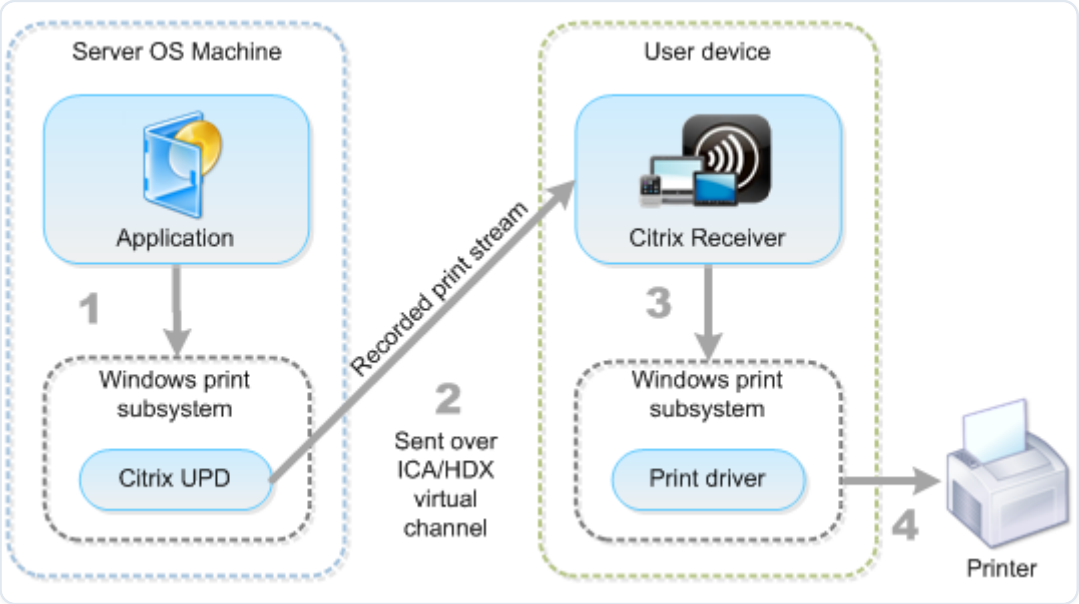
- Formato de Meta-arquivo Aprimorado (**EMF**), padrão. EMF é a versão de 32 bits do formato Windows Metafile (WMF). O driver EMF só pode ser usado por clientes baseados em Windows.
- Especificação de Papel XML (**XPS**). O driver XPS usa XML para criar um "papel eletrônico" independente de plataforma, semelhante ao formato Adobe PDF.
- Linguagem de Comando de Impressora (**PCL5c** e **PCL4**). PCL é um protocolo de impressão desenvolvido originalmente pela Hewlett-Packard para impressoras a jato de tinta. É usado para imprimir texto e gráficos básicos e é amplamente suportado em periféricos multifuncionais e HP LaserJet.
- PostScript (**PS**). PostScript é uma linguagem de computador que pode ser usada para imprimir texto e gráficos vetoriais. O driver é amplamente utilizado em impressoras de baixo custo e periféricos multifuncionais.

Os drivers PCL e PS são mais adequados ao usar dispositivos não baseados em Windows, como um cliente Mac ou UNIX. A ordem em que o Citrix UPD tenta usar os drivers pode ser alterada usando a configuração de política preferência de driver universal.

O Citrix UPD (drivers EMF e XPS) oferece suporte a recursos avançados de impressão, como grampeamento e seleção de origem do papel. Esses recursos estão disponíveis se o driver nativo os disponibilizar usando a tecnologia Microsoft Print Capability. O driver nativo deve usar as

Palavras-chave de Esquema de Impressão padronizadas no XML de Capacidades de Impressão. Se forem usadas palavras-chave não padronizadas, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

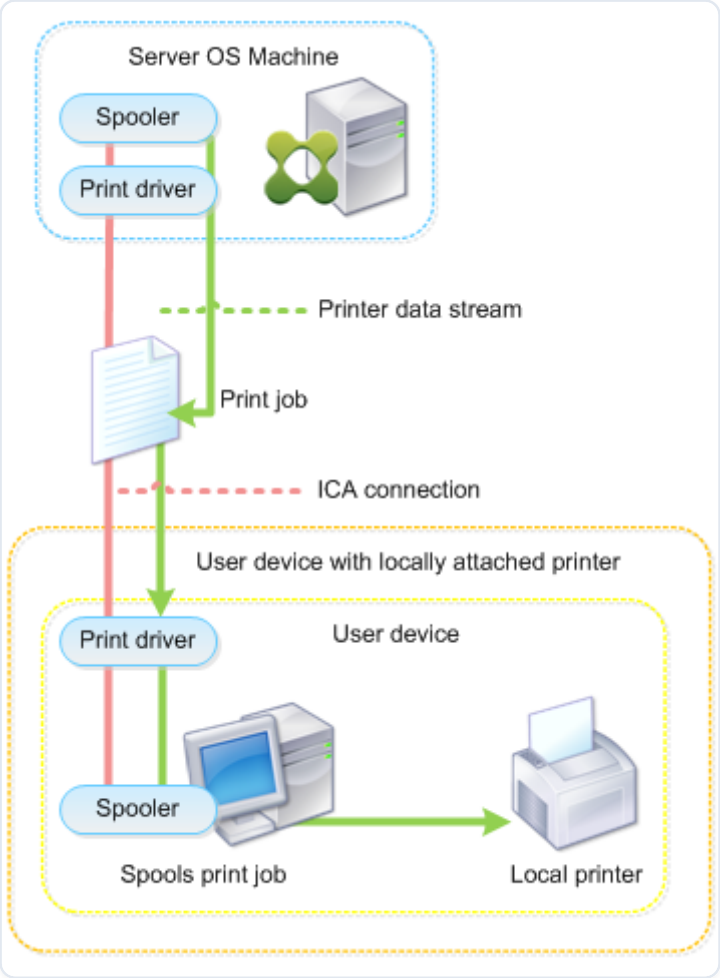
A ilustração a seguir mostra os componentes do driver de impressão universal e um fluxo de trabalho típico para uma impressora conectada localmente a um dispositivo.



Ao planejar sua estratégia de gerenciamento de drivers, determine se você oferecerá suporte ao driver de impressão universal, a drivers específicos do dispositivo ou a ambos. Se você oferece suporte a drivers padrão, deve determinar:

Durante a autocriação da impressora, se o sistema detectar uma nova impressora local conectada a um dispositivo de usuário, ele verificará a máquina do SO de várias sessões em busca do driver de impressora necessário. Por padrão, se um driver nativo do Windows não estiver disponível, o sistema usará o driver de impressão universal.

O driver da impressora na máquina do SO de múltiplas sessões e o driver no dispositivo do usuário devem corresponder para que a impressão seja bem-sucedida. A ilustração a seguir mostra como um driver de impressora é usado em dois locais para impressão do cliente.



- Os tipos de drivers a serem suportados.
- Se deve instalar drivers de impressora automaticamente quando eles estiverem ausentes nas máquinas do SO de múltiplas sessões.
- Se deve criar listas de compatibilidade de drivers.

Conteúdo relacionado

- Exemplo de configuração de impressão
- Melhores práticas, considerações de segurança e operações padrão
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

Exemplo de configuração de impressão

Escolher as opções de configuração de impressão mais apropriadas para suas necessidades e ambiente pode simplificar a administração. Embora a configuração de impressão padrão permita que os usuários imprimam na maioria dos ambientes, os padrões podem não fornecer a experiência de usuário esperada ou o uso ideal da rede e a sobrecarga de gerenciamento para seu ambiente.

Sua configuração de impressão depende de:

- Suas necessidades de negócios e sua infraestrutura de impressão existente.

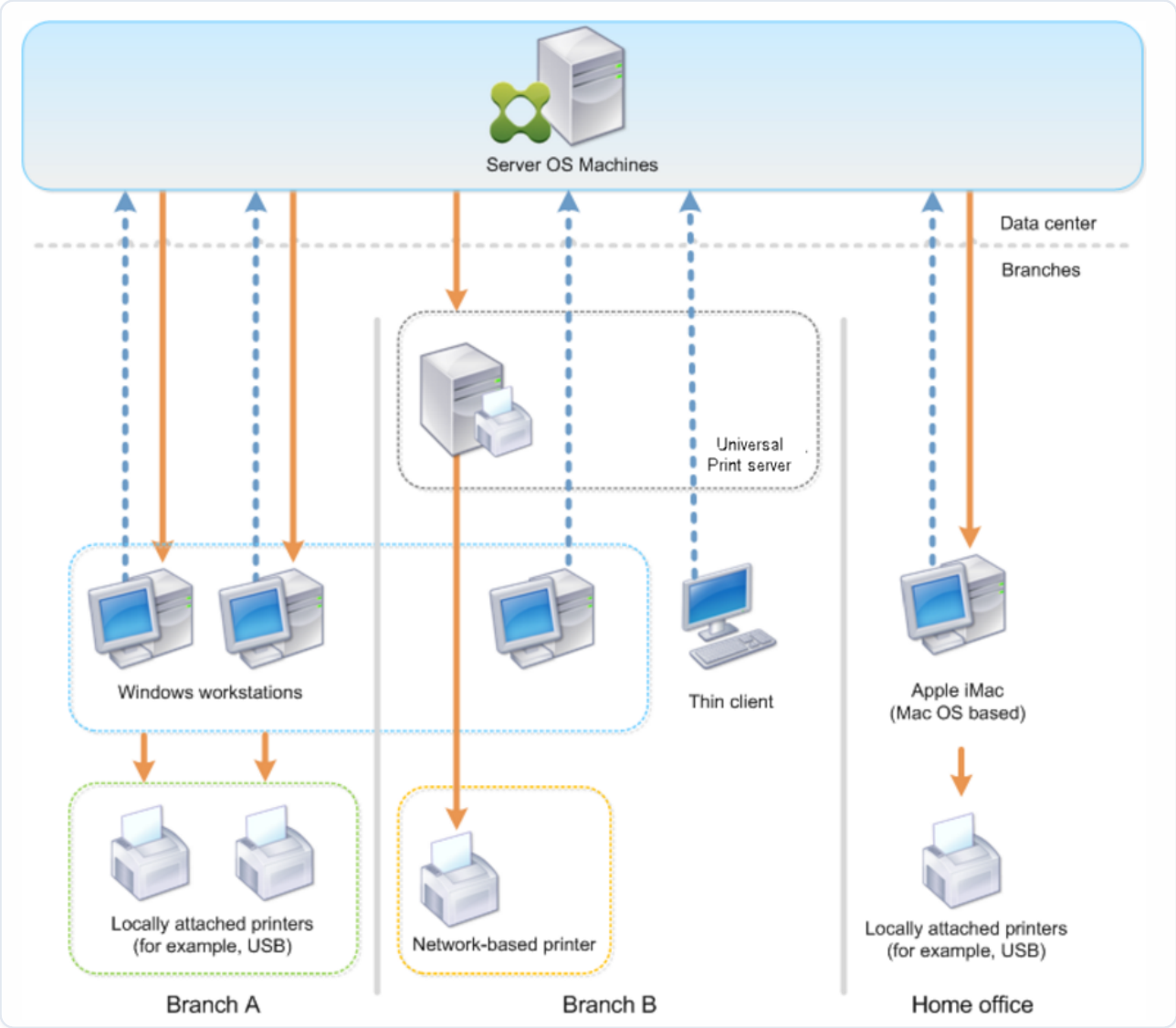
  Projete sua configuração de impressão em torno das necessidades de sua organização. Sua implementação de impressão existente (se os usuários podem adicionar impressoras, quais usuários têm acesso a quais impressoras e assim por diante) pode ser um guia útil ao definir sua configuração de impressão.
- Se sua organização tem políticas de segurança que reservam impressoras para certos usuários (por exemplo, impressoras para Recursos Humanos ou folha de pagamento).
- Se os usuários precisam imprimir enquanto estão longe de seu local de trabalho principal, como trabalhadores que se movem entre estações de trabalho ou viajam a negócios.

Ao projetar sua configuração de impressão, tente dar aos usuários a mesma experiência em uma sessão que eles têm ao imprimir de dispositivos de usuário locais.

Exemplo de implantação de impressão

A ilustração a seguir mostra a implantação de impressão para estes casos de uso:

- **Filial A** - Um pequeno escritório de filial no exterior com algumas estações de trabalho Windows. Cada estação de trabalho de usuário tem uma impressora privada conectada localmente.
- **Filial B** - Um grande escritório de filial com thin clients e estações de trabalho baseadas em Windows. Para maior eficiência, os usuários desta filial compartilham impressoras baseadas em rede (uma por andar). Servidores de impressão baseados em Windows localizados na filial gerenciam as filas de impressão.
- **Home office** - Um home office com um dispositivo de usuário baseado em Mac OS que acessa a infraestrutura Citrix® da empresa. O dispositivo de usuário tem uma impressora conectada localmente.



As seções a seguir descrevem as configurações que minimizam a complexidade do ambiente e simplificam seu gerenciamento.

Impressoras cliente criadas automaticamente e driver de impressora Citrix Universal™

Na Filial A, todos os usuários trabalham em estações de trabalho baseadas em Windows, portanto, são usadas impressoras cliente criadas automaticamente e o driver de impressora Universal. Essas tecnologias oferecem os seguintes benefícios:

- Desempenho - Os trabalhos de impressão são entregues através do canal de impressão ICA®, permitindo que os dados de impressão sejam compactados para economizar largura de banda.

  Para garantir que um único usuário imprimindo um documento grande não degrade o desempenho da sessão de outros usuários, uma política Citrix é configurada para especificar a largura de banda máxima de impressão.

Uma solução alternativa é aproveitar uma conexão ICA multi-stream, na qual o tráfego de impressão é transferido dentro de uma conexão TCP separada de baixa prioridade. O ICA multi-stream é uma opção quando a Qualidade de Serviço (QoS) não está implementada na conexão WAN.

- Flexibilidade - O uso do driver de impressora Citrix Universal garante que todas as impressoras conectadas a um cliente também possam ser usadas a partir de uma sessão de desktop virtual ou aplicativo sem a necessidade de integrar um novo driver de impressora no data center.

Servidor de Impressão Universal Citrix

Na Filial B, todas as impressoras são baseadas em rede e suas filas são gerenciadas em um servidor de impressão Windows, portanto, o Servidor de Impressão Universal Citrix é a configuração mais eficiente.

Todos os drivers de impressora necessários são instalados e gerenciados no servidor de impressão por administradores locais. O mapeamento das impressoras para a sessão de desktop virtual ou aplicativo funciona da seguinte forma:

- Para estações de trabalho baseadas em Windows - A equipe de TI local ajuda os usuários a conectar a impressora baseada em rede apropriada às suas estações de trabalho Windows. Isso permite que os usuários imprimam a partir de aplicativos instalados localmente.

  Durante uma sessão de desktop virtual ou aplicativo, as impressoras configuradas localmente são enumeradas por meio de autocriação. O desktop virtual ou aplicativo então se conecta ao servidor de impressão como uma conexão de rede direta, se possível.

  Os componentes do Servidor de Impressão Universal Citrix são instalados e habilitados, portanto, drivers de impressora nativos não são necessários. Se um driver for atualizado ou uma fila de impressão for modificada, nenhuma configuração adicional será necessária no data center.
- Para thin clients - Para usuários de thin client, as impressoras devem ser conectadas dentro da sessão de desktop virtual ou aplicativo. Para proporcionar aos usuários a experiência de impressão mais simples, os administradores configuram uma única política de Impressora de Sessão Citrix por andar para conectar a impressora de um andar como a impressora padrão.

  Para garantir que a impressora correta seja conectada mesmo que os usuários se desloquem entre andares, as políticas são filtradas com base na sub-rede ou no nome do thin client. Essa

configuração, conhecida como impressão por proximidade, permite a manutenção local do driver da impressora (de acordo com o modelo de administração delegada).

Se uma fila de impressão precisar ser modificada ou adicionada, os administradores Citrix devem modificar a respectiva política de impressora de sessão dentro do ambiente.

Como o tráfego de impressão de rede será enviado fora do canal virtual ICA, o QoS é implementado. O tráfego de rede de entrada e saída nas portas usadas pelo tráfego ICA/HDX é priorizado sobre todo o outro tráfego de rede. Essa configuração garante que as sessões de usuário não sejam impactadas por grandes trabalhos de impressão.

Impressoras cliente criadas automaticamente e driver de impressora universal Citrix

Para escritórios domésticos onde os usuários trabalham em estações de trabalho não padronizadas e usam dispositivos de impressão não gerenciados, a abordagem mais simples é usar impressoras cliente criadas automaticamente e o driver de impressora universal.

Resumo da implantação

Em resumo, a implantação de exemplo é configurada da seguinte forma:

- Nenhum driver de impressora é instalado em máquinas com SO de múltiplas sessões. Apenas o driver de impressora universal Citrix é usado. O fallback para impressão nativa e a instalação automática de drivers de impressora estão desabilitados.
- Uma política é configurada para criar automaticamente todas as impressoras cliente para todos os usuários. As máquinas com SO de múltiplas sessões se conectarão diretamente aos servidores de impressão por padrão. A única configuração necessária é habilitar os componentes do Universal Print Server.
- Uma política de impressora de sessão é configurada para cada andar da Filial B e aplicada a todos os thin clients do respectivo andar.
- O QoS é implementado para a Filial B para garantir uma excelente experiência do usuário.

Melhores práticas, considerações de segurança e operações padrão

Melhores práticas

Muitos fatores determinam a melhor solução de impressão para um ambiente específico. Algumas dessas melhores práticas podem não se aplicar ao seu Site.

- Use o Citrix Universal™ Print Server.
- Use o driver de impressora Universal ou drivers nativos do Windows.
- Minimize o número de drivers de impressora instalados em máquinas com SO de múltiplas sessões.
- Use o mapeamento de drivers para drivers nativos.
- Nunca instale drivers de impressora não testados em um site de produção.
- Evite atualizar um driver. Sempre tente desinstalar um driver, reiniciar o servidor de impressão e, em seguida, instalar o driver de substituição.
- Desinstale drivers não utilizados ou use a política de mapeamento e compatibilidade de drivers de impressora para evitar que impressoras sejam criadas com o driver.
- Tente evitar o uso de drivers de modo kernel versão 2.
- Para determinar se um modelo de impressora é suportado, entre em contato com o fabricante ou consulte o guia de produtos Citrix Ready em www.citrix.com/ready.

  Em geral, todos os drivers de impressora fornecidos pela Microsoft são testados com os Serviços de Terminal e têm garantia de funcionamento com o Citrix. No entanto, antes de usar um driver de impressora de terceiros, consulte o fornecedor do seu driver de impressora para que o driver seja certificado para os Serviços de Terminal pelo programa Windows Hardware Quality Labs (WHQL). A Citrix não certifica drivers de impressora.

Considerações de segurança

As soluções de impressão Citrix são seguras por design.

- O Serviço Citrix Print Manager monitora e responde constantemente a eventos de sessão, como logon e logoff, desconexão, reconexão e término de sessão. Ele lida com solicitações de serviço, personificando o usuário real da sessão.
- A impressão Citrix atribui a cada impressora um namespace exclusivo em uma sessão.
- A impressão Citrix define o descritor de segurança padrão para impressoras criadas automaticamente para garantir que as impressoras cliente criadas automaticamente em uma sessão sejam inacessíveis a usuários executando em outras sessões. Por padrão, usuários administrativos não podem acidentalmente imprimir em uma impressora cliente de outra sessão, mesmo que possam ver e ajustar manualmente as permissões para qualquer impressora cliente.

Operações de impressão padrão

Por padrão, se você não configurar nenhuma regra de política, o comportamento de impressão é o seguinte:

- O Universal Print Server está desabilitado.
- Todas as impressoras configuradas no dispositivo do usuário são criadas automaticamente no início de cada sessão.

  Este comportamento é equivalente a configurar a definição de política Citrix Auto-create client printers com a opção Auto-create all client printers.
- O sistema roteia todos os trabalhos de impressão enfileirados para impressoras anexadas localmente a dispositivos de usuário como trabalhos de impressão de cliente (ou seja, sobre o canal ICA® e através do dispositivo do usuário).
- O sistema roteia todos os trabalhos de impressão enfileirados para impressoras de rede diretamente de máquinas Multi-session OS. Se o sistema não conseguir rotear os trabalhos pela rede, ele os roteará através do dispositivo do usuário como um trabalho de impressão de cliente redirecionado.

  Este comportamento é equivalente a desabilitar a definição de política Citrix Direct connection to print servers.
- O sistema tenta armazenar as propriedades de impressão, uma combinação das preferências de impressão do usuário e das configurações específicas do dispositivo de impressão, no dispositivo do usuário. Se o cliente não suportar esta operação, o sistema armazena as propriedades de impressão em perfis de usuário na máquina Multi-session OS.

  Este comportamento é equivalente a configurar a definição de política Citrix Printer properties retention com a opção Held in profile only if not saved on client.
- Em VDAs versão 7.16 e posteriores, a definição de política Citrix "Automatic installation of inbox printer drivers" não tem efeito nas versões do Windows 8 e posteriores do sistema operacional Windows porque os drivers de impressora V3 in-box não estão incluídos no sistema operacional.
- Em VDAs anteriores a 7.16, o sistema usa a versão Windows do driver da impressora se estiver disponível na máquina Multi-session OS. Se o driver da impressora não estiver disponível, o sistema tenta instalar o driver do sistema operacional Windows. Se o driver não estiver disponível no Windows, ele usa um driver de impressão universal Citrix.

Este comportamento é equivalente a habilitar a definição de política Citrix "Automatic installation of in-box printer drivers" e configurar a definição de Universal printing com a opção "Use universal printing only if requested driver is unavailable".

Habilitar "Instalação automática de drivers de impressora embutidos" pode resultar na instalação de um grande número de drivers de impressora nativos.

Observação:

Se você não tiver certeza sobre quais são os padrões de envio para impressão, exiba-os criando uma nova política e definindo todas as regras da política de impressão como Habilitadas. A opção que aparece é o padrão.

Registro Sempre Ativo

Um recurso de registro Sempre Ativo está disponível para o servidor de impressão e o subsistema de impressão no VDA.

Para agrupar os logs como um ZIP para envio por e-mail, ou para carregar automaticamente os logs para o Citrix Insight Services, use o cmdlet do PowerShell **Start-TelemetryUpload**.

Políticas e preferências de impressão

Quando os usuários acessam impressoras de aplicativos publicados, você pode configurar as políticas do Citrix® para especificar:

- Como as impressoras são provisionadas (ou adicionadas às sessões)
- Como os trabalhos de impressão são roteados
- Como os drivers de impressora são gerenciados

Você pode ter diferentes configurações de impressão para diferentes dispositivos de usuário, usuários ou quaisquer outros objetos nos quais as políticas são filtradas.

A maioria das funções de impressão é configurada por meio das configurações de política de impressão do Citrix. As configurações de impressão seguem o comportamento padrão da política do Citrix.

O sistema pode gravar as configurações da impressora no objeto da impressora no final de uma sessão ou em um dispositivo de impressão cliente, desde que a conta de rede do usuário tenha

permissões suficientes. Por padrão, o aplicativo Citrix Workspace™ usa as configurações armazenadas no objeto da impressora na sessão, antes de procurar em outros locais por configurações e preferências.

Por padrão, o sistema armazena, ou retém, as propriedades da impressora no dispositivo do usuário (se suportado pelo dispositivo) ou no perfil do usuário na máquina do SO multissessão. Quando um usuário altera as propriedades da impressora durante uma sessão, essas alterações são atualizadas no perfil do usuário na máquina. Na próxima vez que o usuário fizer logon ou se reconectar, o dispositivo do usuário herdará essas configurações retidas. Ou seja, as alterações nas propriedades da impressora no dispositivo do usuário não afetam a sessão atual até que o usuário faça logoff e, em seguida, faça logon novamente.

Locais de preferência de impressão

Em ambientes de impressão Windows, as alterações feitas nas preferências de impressão podem ser armazenadas no computador local ou em um documento. Neste ambiente, quando os usuários modificam as configurações de impressão, as configurações são armazenadas nestes locais:

- **No próprio dispositivo do usuário** - Os usuários do Windows podem alterar as configurações do dispositivo no dispositivo do usuário clicando com o botão direito do mouse na impressora no Painel de Controle e selecionando Preferências de Impressão. Por exemplo, se Paisagem for selecionado como orientação da página, paisagem será salvo como a preferência de orientação de página padrão para essa impressora.
- **Dentro de um documento** - Em programas de processamento de texto e editoração eletrônica, as configurações do documento, como a orientação da página, são frequentemente armazenadas dentro dos documentos. Por exemplo, quando você enfileira um documento para imprimir, o Microsoft Word geralmente armazena as preferências de impressão que você especificou, como a orientação da página e o nome da impressora, dentro do documento. Essas configurações aparecem por padrão na próxima vez que você imprimir esse documento.
- **De alterações feitas por um usuário durante uma sessão** - O sistema mantém apenas as alterações nas configurações de impressão de uma impressora criada automaticamente se a alteração foi feita no Painel de Controle na sessão; ou seja, na máquina do SO multissessão.
- **Na máquina do SO multissessão** - Estas são as configurações padrão associadas a um driver de impressora específico na máquina.

As configurações preservadas em qualquer ambiente baseado em Windows variam de acordo com onde o usuário fez as alterações. Isso também significa que as configurações de impressão que aparecem em um lugar, como em um programa de planilha, podem ser diferentes daquelas

em outros, como documentos. Como resultado, as configurações de impressão aplicadas a uma impressora específica podem mudar ao longo de uma sessão.

Hierarquia de preferências de impressão do usuário

Como as preferências de impressão podem ser armazenadas em vários locais, o sistema as processa de acordo com uma prioridade específica. Além disso, é importante notar que as configurações do dispositivo são tratadas de forma distinta e geralmente têm precedência sobre as configurações do documento.

Por padrão, o sistema sempre aplica quaisquer configurações de impressão que um usuário modificou durante uma sessão (ou seja, as configurações retidas) antes de considerar quaisquer outras configurações. Quando o usuário imprime, o sistema mescla e aplica as configurações padrão da impressora armazenadas na máquina do sistema operacional multi-sessão com quaisquer configurações de impressora retidas ou do cliente.

Salvando preferências de impressão do usuário

A Citrix recomenda que você não altere onde as propriedades da impressora são armazenadas. A configuração padrão, que salva as propriedades da impressora no dispositivo do usuário, é a maneira mais fácil de garantir propriedades de impressão consistentes. Se o sistema não conseguir salvar as propriedades no dispositivo do usuário, ele automaticamente recorrerá ao perfil do usuário na máquina do sistema operacional multi-sessão.

Revise a configuração da política de retenção de propriedades da impressora se estes cenários se aplicarem:

- Se você usa plug-ins legados que não permitem que os usuários armazenem propriedades da impressora em um dispositivo de usuário.
- Se você usa perfis obrigatórios em sua rede Windows e deseja reter as propriedades da impressora do usuário.

Provisionar impressoras

Citrix Universal™ Print Server

Ao determinar a melhor solução de impressão para seu ambiente, considere o seguinte:

- O Universal Print Server oferece recursos não disponíveis para o Provedor de Impressão do Windows: cache de imagem e fonte, compactação avançada, otimização e suporte a QoS.

- O driver de impressão Universal suporta as configurações públicas independentes de dispositivo definidas pela Microsoft. Se os usuários precisarem de acesso a configurações de dispositivo específicas de um fabricante de driver de impressão, o Universal Print Server emparelhado com um driver nativo do Windows pode ser a melhor solução. Com essa configuração, você mantém os benefícios do Universal Print Server enquanto fornece aos usuários acesso a funcionalidades especializadas da impressora. Uma desvantagem a considerar é que os drivers nativos do Windows exigem manutenção.
- O Citrix Universal Print Server oferece suporte de impressão universal para impressoras de rede. O Universal Print Server usa o driver de impressão Universal, um único driver na máquina do SO de múltiplas sessões que permite a impressão local ou em rede de qualquer dispositivo, incluindo thin clients e tablets.

Para usar o Universal Print Server com um driver nativo do Windows, habilite o Universal Print Server. Por padrão, se o driver nativo do Windows estiver disponível, ele será usado. Caso contrário, o driver de impressão Universal será usado. Para especificar alterações nesse comportamento, como usar apenas o driver nativo do Windows ou apenas o driver de impressão Universal, atualize a configuração da política de uso do driver de impressão Universal.

Instalar o Universal Print Server

Para usar o Universal Print Server, instale o componente UpsServer em seus servidores de impressão, conforme descrito nos documentos de instalação, e configure-o. Para obter mais informações, consulte Instalar componentes principais e Instalar usando a linha de comando.

Para ambientes onde você deseja implantar o componente UPClient separadamente, por exemplo com **XenApp 6.5**:

1. Baixe o pacote autônomo do Citrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) para Windows Single-session SO ou Windows Multi-session SO.
2. Extraia o VDA usando as instruções da linha de comando descritas em Instalar usando a linha de comando.
3. Instale os pré-requisitos de `\\Image-Full\Support\VcRedist_2013_RTM`
    - Vcredist_x64 / vcredist_x86
        - Execute x86 apenas para 32 bits, e ambos para implantações de 64 bits
4. Instale o pré-requisito cdf de `\\Image-Full\x64\Virtual Desktop Components` ou `\\Image-Full\x86\Virtual Desktop Components`.
    - Cdf_x64 / Cdf_x86

    - x86 para 32 bits, x64 para 64 bits

5. Encontre o componente UPClient em `\\Image-Full\x64\Virtual Desktop Components` ou `\\Image-Full\x86\Virtual Desktop Components`.
6. Instale o componente UPClient extraindo e, em seguida, iniciando o MSI do componente.
7. É necessário reiniciar após a instalação do componente UPClient.

Desativar o CEIP para o Universal Print Server

Você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente Citrix (CEIP) ao instalar o Universal Print Server. O primeiro upload de dados ocorre sete dias após a data e hora da instalação.

Para desativar o CEIP, edite a chave do registro `HKLM\Software\Citrix\Universal Print Server\CEIPEnabled` e defina o valor **DWORD** como **0**.

Para reativar, defina o valor DWORD como 1.

Cuidado: Editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Para obter mais informações, consulte Citrix Insight Services.

Configurar o Universal Print Server

Use as seguintes configurações de política Citrix para configurar o Universal Print Server. Para obter mais informações, consulte a ajuda das configurações de política na tela.

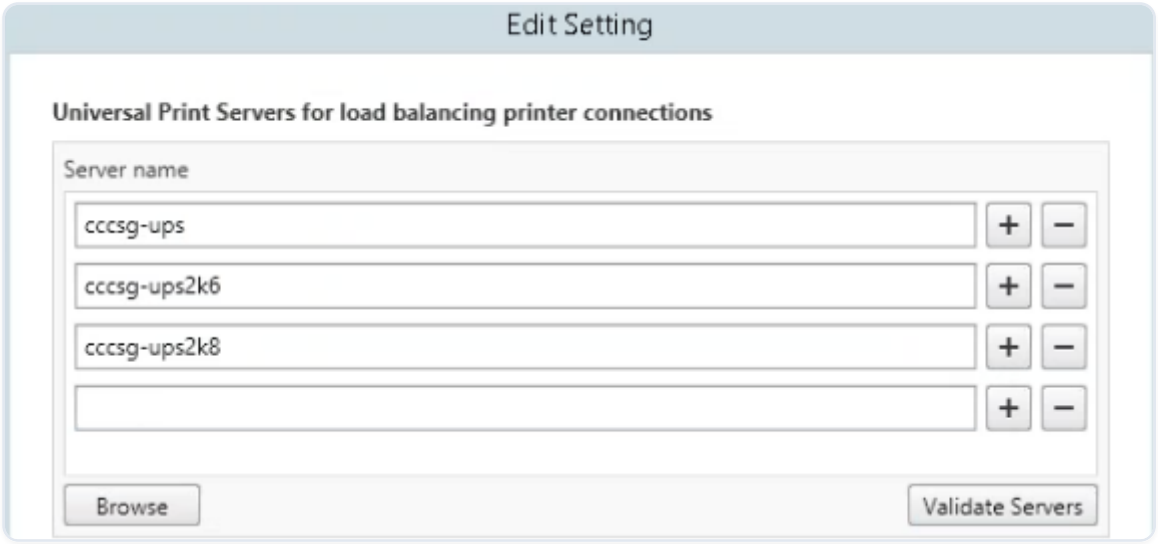
- **Ativar Universal Print Server**. O Universal Print Server é desativado por padrão. Ao ativar o Universal Print Server, você escolhe se deseja usar o Provedor de Impressão do Windows caso o Universal Print Server esteja indisponível. Depois de ativar o Universal Print Server, um usuário pode adicionar e enumerar impressoras de rede por meio das interfaces do Provedor de Impressão do Windows e do Provedor Citrix.
- **Porta do fluxo de dados de impressão do Universal Print Server (CGP)**. Especifica o número da porta TCP usado pelo listener CGP (Common Gateway Protocol) do fluxo de dados de impressão do Universal Print Server. O padrão é **7229**.
- **Porta do serviço web do Universal Print Server (HTTP/SOAP)**. Especifica o número da porta TCP usado pelo listener do Universal Print Server para solicitações HTTP/SOAP de entrada. O padrão é **8080**.

Para alterar a porta padrão HTTP 8080 para a comunicação do Universal Print Server com os VDAs do Citrix Virtual Apps and Desktops, o seguinte registro também deve ser criado e o valor do número da porta modificado no(s) computador(es) do Universal Print Server:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

Este número de porta deve corresponder à porta do serviço web (HTTP/SOAP) do Universal Print Server da Política HDX, no Studio.

- **Limite de largura de banda de entrada do fluxo de impressão do Universal Print Server (kbps)**. Especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão entregues de cada trabalho de impressão para o Universal Print Server usando CGP. O padrão é 0 (ilimitado).
- **Universal Print Servers para balanceamento de carga**. Esta configuração lista os Universal Print Servers a serem usados para balancear a carga das conexões de impressora estabelecidas no início da sessão, após avaliar outras configurações de política de impressão do Citrix. Para otimizar o tempo de criação da impressora, a Citrix recomenda que todos os servidores de impressão tenham o mesmo conjunto de impressoras compartilhadas.



- **Limite de Universal Print Servers fora de serviço**. Especifica quanto tempo o balanceador de carga deve esperar que um servidor de impressão indisponível se recupere antes de determinar que o servidor está permanentemente offline e redistribuir sua carga para outros servidores de impressão disponíveis. O padrão é 180 (segundos).

Depois que as políticas de impressão são modificadas no Delivery Controller™, pode levar alguns minutos para que as alterações de política sejam aplicadas aos VDAs.

Interações com outras configurações de política - O Universal Print Server respeita outras configurações de política de impressão do Citrix e interage com elas conforme observado na tabela a seguir. As informações fornecidas pressupõem que a configuração de política do Universal Print Server esteja habilitada, os componentes do Universal Print Server estejam instalados e as configurações de política sejam aplicadas.

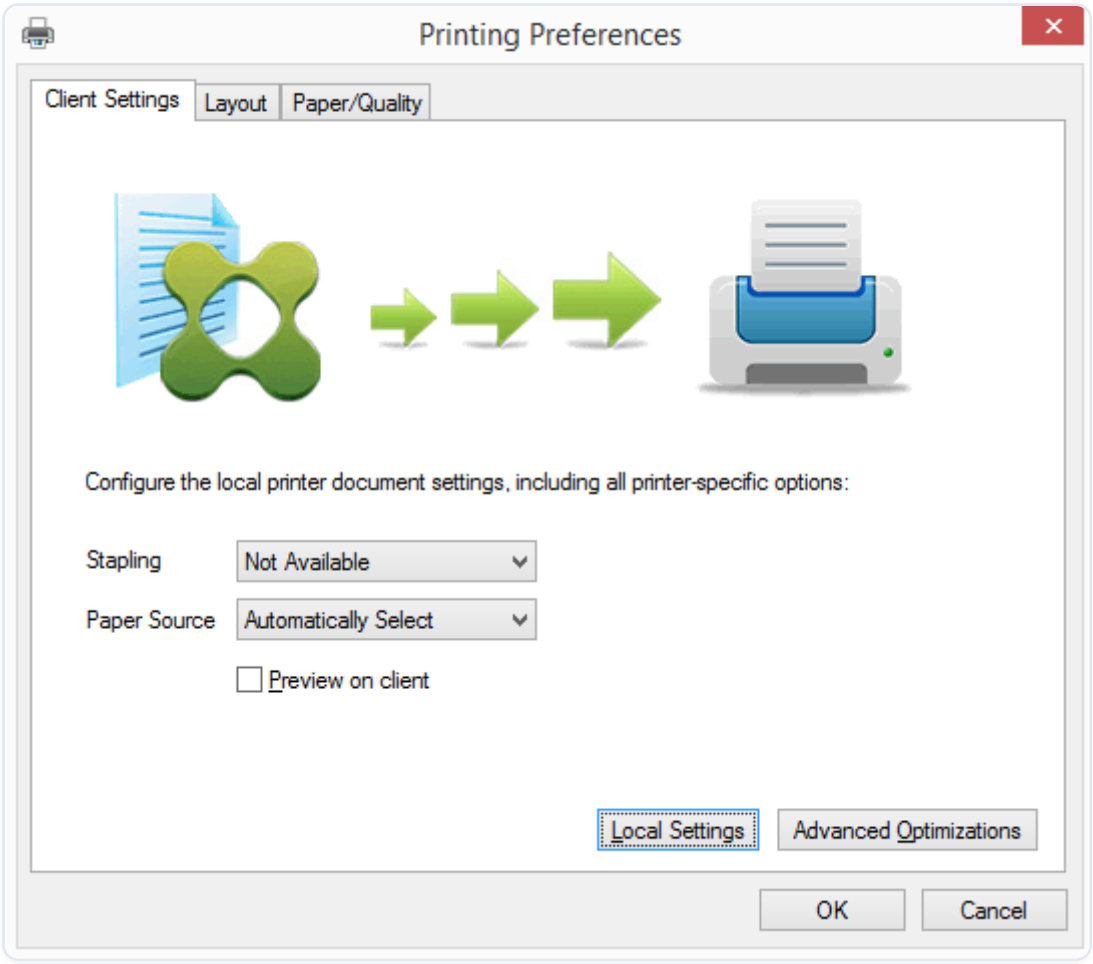
Configuração de política	Interação
Redirecionamento de impressora cliente, Criar impressoras cliente automaticamente	Depois que o Universal Print Server é habilitado, as impressoras de rede cliente são criadas usando o driver de impressão Universal em vez dos drivers nativos. Os usuários veem o mesmo nome de impressora de antes.
Impressoras de sessão	Ao usar a solução Citrix Universal Print Server, as configurações de política do driver de impressão universal são respeitadas.
Conexões diretas com o servidor de impressão	Quando o Universal Print Server está habilitado e a configuração da política de uso do driver de impressão universal está configurada para usar apenas a impressão universal, uma conexão direta de impressora de rede pode ser criada com o servidor de impressão, usando o driver de impressão universal.
Preferência UPD	Suporta drivers EMF e XPS.

Efeitos nas interfaces de usuário - O driver de impressão universal Citrix usado pelo Universal Print Server desabilita os seguintes controles de interface de usuário:

- Na caixa de diálogo Propriedades da Impressora, o botão Configurações da Impressora Local
- Na caixa de diálogo Propriedades do Documento, os botões Configurações da Impressora Local e Visualizar no cliente

O driver de impressão universal Citrix (drivers EMF e XPS) suporta recursos de impressão avançados, como grampeamento e origem do papel. O usuário pode selecionar as opções de

Grampeamento ou Origem do Papel na caixa de diálogo de impressão UPD personalizada se o cliente ou as impressoras de rede mapeadas para o UPD na sessão suportarem esses recursos.



Para definir configurações de impressora não padrão, como grampeamento e PIN seguro, selecione **Configurações Locais** na caixa de diálogo de impressão UPD do cliente para quaisquer impressoras mapeadas do cliente que usem os drivers Citrix UPD EMF ou XPS. A caixa de diálogo **Preferências de Impressão** da impressora mapeada é exibida fora da sessão no cliente, permitindo que o usuário altere qualquer opção da impressora, e as configurações de impressora modificadas são usadas na sessão ativa ao imprimir esse documento.

Esses recursos estão disponíveis se o driver nativo os disponibilizar usando a tecnologia Microsoft Print Capability. O driver nativo deve usar as palavras-chave padronizadas do Print Schema no XML de Print Capabilities. Se forem usadas palavras-chave não padrão, os recursos de impressão avançados não estarão disponíveis usando o driver de impressão universal Citrix.

Ao usar o Universal Print Server, o Assistente para Adicionar Impressora para o Citrix Print Provider é o mesmo que o Assistente para Adicionar Impressora para o Windows Print Provider, com as seguintes exceções:

- Ao adicionar uma impressora por nome ou endereço, você pode fornecer um número de porta HTTP/SOAP para o servidor de impressão. Esse número de porta se torna parte do nome da impressora e aparece nas exibições.
- Se a configuração da política de uso do driver de impressão universal Citrix especificar que a impressão universal deve ser usada, o nome do driver de impressão universal aparecerá ao selecionar uma impressora. O Provedor de Impressão do Windows não pode usar o driver de impressão universal.

O Provedor de Impressão Citrix não oferece suporte à renderização do lado do cliente.

Para obter mais informações sobre o Servidor de Impressão Universal, consulte CTX200328.

Impressoras cliente criadas automaticamente

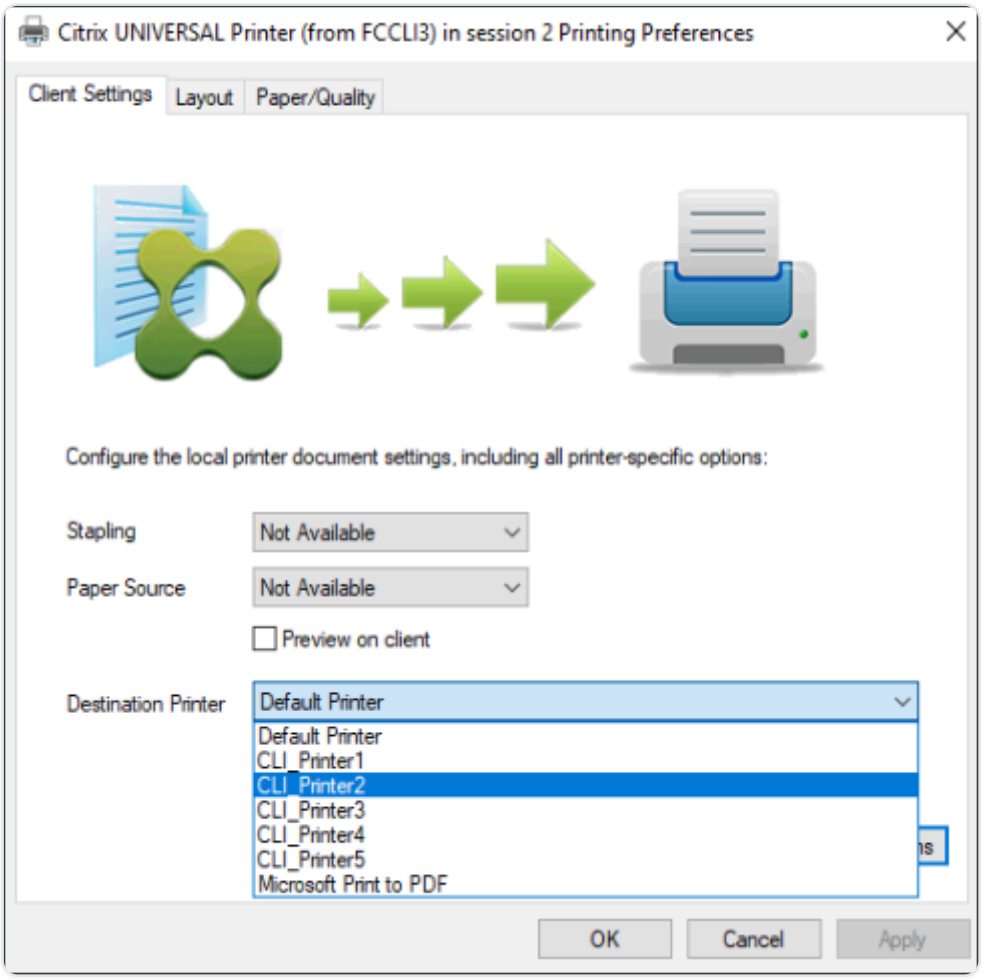
Estas soluções de impressão universal são fornecidas para impressoras cliente:

- **Impressora Universal Citrix** - Uma impressora genérica criada no início das sessões que não está vinculada a um dispositivo de impressão. Ao criar automaticamente e usar apenas a Impressora Universal Citrix, você pode experimentar menor uso de recursos e tempos de logon do usuário. A Impressora Universal pode imprimir em qualquer dispositivo de impressão do lado do cliente.

  A Impressora Universal Citrix pode não funcionar para todos os dispositivos de usuário ou aplicativos Citrix Workspace™ em seu ambiente. A Impressora Universal Citrix requer um ambiente Windows e não oferece suporte ao Citrix Offline Plug-in ou a aplicativos transmitidos para o cliente. Considere usar impressoras cliente criadas automaticamente e o driver de impressão universal para esses ambientes.

  Para usar uma solução de impressão universal para aplicativos Citrix Workspace não-Windows, use um dos outros drivers de impressão universal baseados em Postscript ou PCL.

  A Impressora Universal Citrix permite selecionar a impressora padrão do cliente ou uma impressora cliente específica como destino de impressão. Para escolher uma impressora específica para um trabalho de impressão, abra a caixa de diálogo **Preferências de Impressão**. Selecione o menu suspenso **Impressora de Destino**. A opção **Impressora Padrão** envia trabalhos de impressão para a impressora padrão do cliente. Quaisquer impressoras redirecionadas do cliente anexadas ao endpoint que executa a sessão também são listadas. A impressora que você selecionar é salva como a impressora de destino para quaisquer trabalhos de impressão futuros.



- **Drivers de impressão universal Citrix** - Um driver de impressora independente de dispositivo. Se você configurar um driver de impressão universal Citrix, o sistema usará o driver de impressão universal baseado em EMF por padrão.

  O driver de impressão universal Citrix pode criar trabalhos de impressão menores do que drivers de impressora mais antigos ou menos avançados. No entanto, um driver específico do dispositivo pode ser necessário para otimizar trabalhos de impressão para uma impressora especializada.

Configurar impressão universal - Use as seguintes configurações de política Citrix para configurar a impressão universal. Para obter mais informações, consulte a ajuda das configurações de política na tela.

- Uso do driver de impressão universal. Especifica quando usar a impressão universal.
- Criar automaticamente impressora universal genérica. Habilita ou desabilita a criação automática do objeto Impressora Universal Citrix genérico para sessões quando um dispositivo de usuário compatível com Impressão Universal está em uso. Por padrão, o objeto Impressora Universal genérico não é criado automaticamente.

- Preferência de driver universal. Especifica a ordem em que o sistema tenta usar drivers de impressão universais, começando com a primeira entrada na lista. Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.
- Preferência de visualização de impressão universal. Especifica se deve usar a função de visualização de impressão para impressoras universais genéricas ou criadas automaticamente.
- Modo de processamento EMF de impressão universal. Controla o método de processamento do arquivo de spool EMF no dispositivo de usuário Windows. Por padrão, os registros EMF são enviados diretamente para a impressora. O envio direto para a impressora permite que o spooler processe os registros mais rapidamente e use menos recursos da CPU.

Para mais políticas, consulte Otimizar o desempenho da impressão. Para alterar os padrões de configurações como tamanho do papel, qualidade de impressão, cor, duplex e o número de cópias, consulte CTX113148.

Criar impressoras automaticamente a partir do dispositivo do usuário - No início de uma sessão, o sistema cria automaticamente todas as impressoras no dispositivo do usuário por padrão. Você pode controlar quais, se houver, tipos de impressoras são provisionados para os usuários e impedir a criação automática.

Use a configuração de política Citrix Criar impressoras cliente automaticamente para controlar a criação automática. Você pode especificar que:

- Todas as impressoras visíveis para o dispositivo do usuário, incluindo impressoras de rede e conectadas localmente, são criadas automaticamente no início de cada sessão (padrão)
- Todas as impressoras locais fisicamente conectadas ao dispositivo do usuário são criadas automaticamente
- Apenas a impressora padrão para o dispositivo do usuário é criada automaticamente
- A criação automática está desabilitada para todas as impressoras cliente

A configuração Criar impressoras cliente automaticamente exige que a configuração Redirecionamento de impressora cliente esteja Permitida (o padrão).

Atribuir impressoras de rede aos usuários

Por padrão, as impressoras de rede no dispositivo do usuário são criadas automaticamente no início das sessões. O sistema permite reduzir o número de impressoras de rede que são

enumeradas e mapeadas, especificando as impressoras de rede a serem criadas em cada sessão. Essas impressoras são chamadas de impressoras de sessão.

Você pode filtrar políticas de impressora de sessão por endereço IP para fornecer impressão por proximidade. A impressão por proximidade permite que usuários dentro de um intervalo de endereço IP especificado acessem automaticamente os dispositivos de impressão de rede que existem dentro do mesmo intervalo. A impressão por proximidade é fornecida pelo Citrix Universal Print Server e não requer a configuração descrita nesta seção.

A impressão por proximidade pode envolver o seguinte cenário:

- A rede interna da empresa opera com um servidor DHCP que designa automaticamente endereços IP aos usuários.
- Todos os departamentos da empresa possuem faixas de endereços IP designadas exclusivas.
- As impressoras de rede existem dentro da faixa de endereços IP de cada departamento.

Quando a impressão por proximidade é configurada e um funcionário se desloca de um departamento para outro, nenhuma configuração adicional do dispositivo de impressão é necessária. Uma vez que o dispositivo do usuário é reconhecido dentro da faixa de endereços IP do novo departamento, ele terá acesso a todas as impressoras de rede dentro dessa faixa.

Configurar impressoras específicas para serem redirecionadas em sessões - Para criar impressoras atribuídas pelo administrador, configure a configuração de política do Citrix Impressoras de sessão. Adicione uma impressora de rede a essa política usando um dos seguintes métodos:

- Insira o caminho UNC da impressora usando o formato `\\servername\printername`.
- Navegue até um local de impressora na rede.
- Procure impressoras em um servidor específico. Insira o nome do servidor usando o formato `\\servername` e clique em Procurar.

Importante: O servidor mescla todas as configurações de impressora de sessão habilitadas para todas as políticas aplicadas, começando das prioridades mais altas para as mais baixas. Quando uma impressora é configurada em vários objetos de política, as configurações padrão personalizadas são obtidas apenas do objeto de política de maior prioridade no qual essa impressora está configurada.

As impressoras de rede criadas com a configuração Impressoras de sessão podem variar de acordo com o local onde a sessão foi iniciada, filtrando por objetos como sub-redes.

Especificar uma impressora de rede padrão para uma sessão - Por padrão, a impressora principal do usuário é usada como a impressora padrão para a sessão. Use a configuração de política do Citrix Impressora padrão para alterar como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

1. Na página de configurações da Impressora padrão, selecione uma configuração para Escolher a impressora padrão do cliente:
    - Nome da impressora de rede. As impressoras adicionadas com a configuração de política Impressoras de sessão aparecem neste menu. Selecione a impressora de rede a ser usada como padrão para esta política.
    - Não ajustar a impressora padrão do usuário. Usa a configuração atual do perfil de usuário do Terminal Services ou Windows para a impressora padrão. Para obter mais informações, consulte a ajuda das configurações de política na tela.
2. Aplique a política ao grupo de usuários (ou outros objetos filtrados) que você deseja afetar.

Configurar impressão por proximidade - A impressão por proximidade também é fornecida pelo Citrix Universal Print Server, que não requer a configuração descrita aqui.

1. Crie uma política separada para cada sub-rede (ou para corresponder ao local da impressora).
2. Em cada política, adicione as impressoras na localização geográfica dessa sub-rede à configuração Impressoras de sessão.
3. Defina a configuração Impressora padrão como Não ajustar a impressora padrão do usuário.
4. Filtre as políticas por endereço IP do cliente. Certifique-se de atualizar essas políticas para refletir as alterações nos intervalos de endereços IP DHCP.

Manter o ambiente de impressão

A manutenção do ambiente de impressão inclui:

- Gerenciar drivers de impressora
- Otimizar o desempenho da impressão
- Exibir impressora e gerenciar filas de impressão

Gerenciar drivers de impressora

Para minimizar a sobrecarga administrativa e o potencial de problemas com drivers de impressão, a Citrix recomenda o uso do driver de impressão Citrix Universal™.

Se a autocriação falhar, por padrão, o sistema instala um driver de impressora nativo do Windows fornecido com o Windows. Se um driver não estiver disponível, o sistema retorna ao driver de impressão Universal. Para obter mais informações sobre os padrões do driver de impressora, consulte Melhores práticas, considerações de segurança e operações padrão.

Se o driver de impressão Citrix Universal não for uma opção para todos os cenários, mapeie os drivers de impressora para minimizar a quantidade de drivers instalados em máquinas Multi-session OS. Além disso, o mapeamento de drivers de impressora permite que você:

- Permitir que impressoras especificadas usem apenas o driver de impressão Citrix Universal
- Permitir ou impedir que impressoras sejam criadas com um driver especificado
- Substituir drivers de impressora bons por drivers desatualizados ou corrompidos
- Substituir um driver disponível no servidor Windows por um nome de driver de cliente

Impedir a instalação automática de drivers de impressora - A instalação automática de drivers de impressão deve ser desabilitada para garantir a consistência entre as máquinas Multi-session OS. Isso pode ser alcançado por meio de políticas Citrix®, políticas Microsoft ou ambas. Para impedir a instalação automática de drivers de impressora nativos do Windows, desabilite a configuração de política Citrix Instalação automática de drivers de impressora internos.

Mapear drivers de impressora de cliente - Cada cliente fornece informações sobre impressoras do lado do cliente durante o logon, incluindo o nome do driver da impressora. Durante a autocriação da impressora do cliente, os nomes dos drivers de impressora do servidor Windows são selecionados para corresponder aos nomes dos modelos de impressora fornecidos pelo cliente. O processo de autocriação então usa os drivers de impressora identificados e disponíveis para construir filas de impressão de cliente redirecionadas.

Aqui está o processo geral para definir regras de substituição de driver e editar configurações de impressão para drivers de impressora cliente mapeados:

1. Para especificar regras de substituição de driver para impressoras cliente criadas automaticamente, configure a definição de política do Citrix Mapeamento e compatibilidade de driver de impressora adicionando o nome do driver de impressora cliente e selecionando o driver de servidor que você deseja substituir pelo driver de impressora cliente no menu Localizar driver de impressora. Você pode usar curingas nesta definição. Por exemplo, para forçar todas as impressoras HP a usar um driver específico, especifique HP* na definição de política.
2. Para banir um driver de impressora, selecione o nome do driver e escolha a definição Não criar.

3. Conforme necessário, edite um mapeamento existente, remova um mapeamento ou altere a ordem das entradas de driver na lista.
4. Para editar as definições de impressão para drivers de impressora cliente mapeados, selecione o driver de impressora, clique em Definições e especifique definições como qualidade de impressão, orientação e cor. Se você especificar uma opção de impressão que o driver de impressora não suporta, essa opção não terá efeito. Essa definição substitui as definições de impressora retidas que o usuário definiu durante uma sessão anterior.
5. A Citrix recomenda testar o comportamento das impressoras em detalhes após mapear os drivers, pois algumas funcionalidades da impressora podem estar disponíveis apenas com um driver específico.

Quando os usuários fazem logon, o sistema verifica a lista de compatibilidade do driver da impressora cliente antes de configurar as impressoras cliente.

Otimizar o desempenho da impressão

Para otimizar o desempenho da impressão, use o Universal Print Server e o driver de impressão universal. As seguintes políticas controlam a otimização e a compactação da impressão:

- Padrões de otimização de impressão universal. Especifica as configurações padrão para a Impressora Universal quando ela é criada para uma sessão:
    - Qualidade de imagem desejada especifica o limite de compactação de imagem padrão aplicado à impressão universal. Por padrão, Qualidade Padrão está ativada, o que significa que os usuários só podem imprimir imagens usando compactação de qualidade padrão ou reduzida.
    - Ativar compactação pesada ativa ou desativa a redução da largura de banda além do nível de compactação definido por Qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compactação pesada está desativada.
    - As definições de Cache de Imagem e Fonte especificam se as imagens e fontes que aparecem várias vezes no fluxo de impressão devem ou não ser armazenadas em cache, garantindo que cada imagem ou fonte exclusiva seja enviada à impressora apenas uma vez. Por padrão, imagens e fontes incorporadas são armazenadas em cache.
    - Permitir que não administradores modifiquem essas definições especifica se os usuários podem ou não alterar as definições padrão de otimização de impressão dentro de uma sessão. Por padrão, os usuários não têm permissão para alterar as definições padrão de otimização de impressão.

- Limite de compactação de imagem de impressão universal. Define a qualidade máxima e o nível mínimo de compactação disponíveis para imagens impressas com o driver de impressão universal. Por padrão, o limite de compactação de imagem é definido como Melhor Qualidade (compactação sem perdas).
- Limite de qualidade de impressão universal. Especifica o máximo de pontos por polegada (dpi) disponível para gerar saída impressa na sessão. Por padrão, nenhum limite é especificado.

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados da máquina do SO de múltiplas sessões, através da rede e diretamente para o servidor de impressão. Considere rotear trabalhos de impressão pela conexão ICA® se a rede tiver latência substancial ou largura de banda limitada. Para fazer isso, desative a configuração da política Citrix Conexões diretas a servidores de impressão. Os dados enviados pela conexão ICA são compactados, de modo que menos largura de banda é consumida à medida que os dados viajam pela WAN.

Melhore o desempenho da sessão limitando a largura de banda de impressão - Ao imprimir arquivos de máquinas do SO de múltiplas sessões para impressoras de usuário, outros canais virtuais (como vídeo) podem ter desempenho reduzido devido à competição por largura de banda, especialmente se os usuários acessarem servidores por meio de redes mais lentas. Para evitar essa degradação, você pode limitar a largura de banda usada pela impressão do usuário. Ao limitar a taxa de transmissão de dados para impressão, você disponibiliza mais largura de banda no fluxo de dados HDX™ para transmissão de vídeo, teclas e dados do mouse.

> **Importante:**
>
> O limite de largura de banda da impressora é sempre imposto, mesmo quando nenhum outro canal está em uso.
>
> Use as seguintes configurações de largura de banda da impressora da política Citrix para configurar os limites de largura de banda da sessão de impressão. Para definir os limites para o site, execute esta tarefa usando o Studio. Para definir os limites para servidores individuais, execute esta tarefa usando o Console de Gerenciamento de Política de Grupo no Windows localmente em cada máquina do SO de múltiplas sessões.

- A configuração Limite de largura de banda de redirecionamento de impressora especifica a largura de banda disponível para impressão em kilobits por segundo (kbps).

- A configuração Limite de largura de banda de redirecionamento de impressora em porcentagem limita a largura de banda disponível para impressão a uma porcentagem da largura de banda geral disponível.

  Nota: Para especificar a largura de banda como uma porcentagem usando a configuração Limite de largura de banda de redirecionamento de impressora em porcentagem, ative também o Limite de largura de banda geral da sessão.

  Se você inserir valores para ambas as configurações, a configuração mais restritiva (o valor mais baixo) será aplicada.

Para obter informações em tempo real sobre a largura de banda de impressão, use o Citrix Director.

Balancear carga de Universal Print Servers

A solução Universal Print Server pode ser dimensionada adicionando mais servidores de impressão à solução de balanceamento de carga. Não há um único ponto de falha, pois cada VDA tem seu próprio balanceador de carga para distribuir a carga de impressão para todos os servidores de impressão.

Use as configurações de política, Universal Print Servers para balanceamento de carga e Limite de servidores de impressão universais fora de serviço, para distribuir a carga de impressão entre todos os servidores de impressão na solução de balanceamento de carga.

Se houver uma falha imprevista de um servidor de impressão, o mecanismo de failover do balanceador de carga em cada VDA redistribui automaticamente as conexões de impressora alocadas nos servidores de impressão com falha para os outros servidores de impressão disponíveis, de modo que todas as sessões existentes e futuras funcionem normalmente sem afetar a experiência do usuário e sem exigir a intervenção imediata do administrador.

Os administradores podem monitorar a atividade dos servidores de impressão com balanceamento de carga usando um conjunto de contadores de desempenho para rastrear o seguinte no VDA:

- Lista de servidores de impressão com balanceamento de carga no VDA e seu estado (disponível, indisponível)
- Número de conexões de impressora aceitas por cada servidor de impressão
- Número de conexões de impressora com falha em cada servidor de impressão
- Número de conexões de impressora ativas em cada servidor de impressão

- Número de conexões de impressora pendentes em cada servidor de impressão

Exibir e gerenciar filas de impressão

A tabela a seguir resume onde você pode exibir impressoras e gerenciar filas de impressão em seu ambiente.

	CAMINHO DE IMPRESSÃO	LOCALIZAÇÃO
Impressoras cliente (Impressoras conectadas ao dispositivo do usuário)	Caminho de impressão do cliente	UAC Ativado: Snap-in de Gerenciamento de Impressão localizado no Microsoft Management Console; UAC Desativado: Pré-Windows 8: Painel de Controle, Windows 8: Snap-in de Gerenciamento de Impressão
Impressoras de rede (Impressoras em um servidor de impressão de rede)	Caminho de impressão de rede	UAC Ativado: Servidor de Impressão \> Snap-in de Gerenciamento de Impressão localizado no Microsoft Management Console; UAC Desativado: Servidor de Impressão \> Painel de Controle
Impressoras de rede (Impressoras em um servidor de impressão de rede)	Caminho de impressão do cliente	UAC Ativado: Servidor de Impressão \> Snap-in de Gerenciamento de Impressão localizado no Microsoft Management Console; UAC Desativado: Pré-Windows 8: Painel de Controle, Windows 8: Snap-in de Gerenciamento de Impressão
Impressoras de servidor de rede local (Impressoras de um servidor de impressão de rede que são adicionadas a uma máquina de SO multi-sessão)	Caminho de impressão de rede	UAC Ativado: Servidor de Impressão \> Painel de Controle; UAC Desativado: Servidor de Impressão \> Painel de Controle

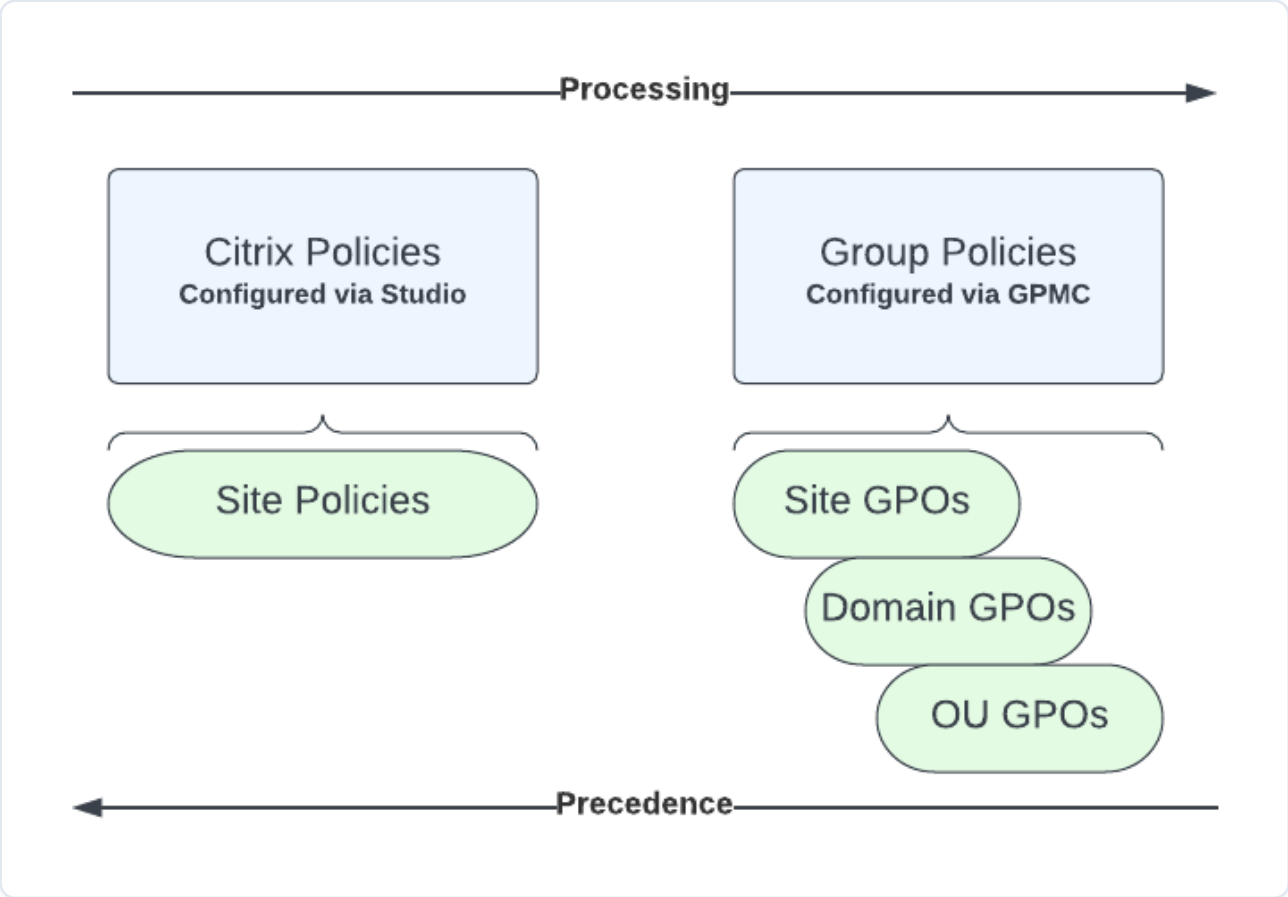
Observação:

As filas de impressão para impressoras de rede que usam o caminho de impressão de rede são privadas e não podem ser gerenciadas através do sistema.

Políticas

Políticas são uma coleção de configurações que definem como sessões, largura de banda e segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.

Você pode aplicar configurações de política a máquinas físicas e virtuais ou a usuários. Você pode aplicar configurações a usuários individuais no nível local ou em grupos de segurança em um Active Directory. As configurações definem critérios e regras específicos. Se você não atribuir as políticas especificamente, as configurações serão aplicadas a todas as conexões.



Você pode aplicar políticas em diferentes níveis da rede. As configurações de política colocadas no nível GPO da Unidade Organizacional têm a maior precedência na rede. As políticas no nível GPO do Domínio substituem as políticas no nível do Objeto de Política de Grupo do Site. O nível do Objeto de Política de Grupo do Site substitui quaisquer políticas conflitantes nos níveis de Políticas Locais da Microsoft e da Citrix.

Todas as Políticas Locais da Citrix são criadas e gerenciadas no console do Web Studio e armazenadas no Banco de Dados do Site. As Políticas de Grupo são criadas e gerenciadas usando o Console de Gerenciamento de Política de Grupo da Microsoft (GPMC) e armazenadas no Active Directory. As Políticas Locais da Microsoft são criadas no Sistema Operacional Windows e são armazenadas no registro.

O Studio usa um Assistente de Modelagem para ajudar os administradores a comparar as configurações dentro de modelos e políticas para ajudar a eliminar configurações conflitantes e redundantes. Os administradores podem definir GPOs usando o GPMC para configurar as configurações. Além disso, aplicá-las a um conjunto de usuários-alvo em diferentes níveis da rede.

Esses GPOs são salvos no Active Directory. O acesso ao gerenciamento dessas configurações é restrito para a maioria do pessoal de TI por questões de segurança.

As configurações são mescladas de acordo com a prioridade e sua condição. Qualquer configuração desabilitada substitui uma configuração habilitada de classificação inferior. As configurações de política não configuradas são ignoradas e não substituem as configurações de classificação inferior.

As políticas locais também podem ter conflitos com as políticas de grupo no Active Directory, que podem se sobrepor dependendo da situação.

Todas as políticas são processadas na seguinte ordem:

1. O usuário final faz logon em uma máquina usando credenciais de domínio.
2. As credenciais são enviadas para o controlador de domínio.
3. O Active Directory aplica todas as políticas (usuário final, endpoint, unidade organizacional e domínio).
4. O usuário final faz logon no aplicativo Citrix Workspace™ e acessa um aplicativo ou desktop.
5. As políticas da Citrix e da Microsoft são processadas para o usuário final e a máquina que hospeda o recurso.
6. O Active Directory determina a precedência para as configurações de política. Em seguida, as aplica aos registros do dispositivo endpoint e à máquina que hospeda o recurso.
7. O usuário final faz logoff do recurso. As políticas Citrix para o usuário final e o dispositivo de endpoint não estão mais ativas.
8. O usuário final faz logoff do dispositivo do usuário, o que libera as políticas de usuário do GPO.
9. O usuário final desliga o dispositivo, o que libera as políticas de máquina do GPO.

Ao criar políticas para grupos de usuários, dispositivos e máquinas, alguns membros podem ter requisitos diferentes e precisariam de exceções a algumas configurações de política. As exceções são feitas por meio de filtros no Studio e no GPMC que determinam quem ou o que a política afeta.

> **Observação:**
>
> Não oferecemos suporte à mistura de políticas do Windows e Citrix no mesmo GPO.

Trabalhar com políticas

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Configure as políticas do Citrix para controlar o acesso do usuário e os ambientes de sessão. As políticas do Citrix são o método mais eficiente para 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 do Citrix

Você pode usar as seguintes ferramentas com as políticas do Citrix.

- **Web Studio.** Se você é um administrador Citrix sem permissão para gerenciar a política de grupo, use o Web Studio para criar políticas para seu site. As políticas criadas usando o Web Studio são armazenadas no banco de dados do site, e as atualizações são enviadas para o VDA quando ele se registra com o broker ou quando um usuário se conecta a esse VDA.
- **Editor de Política de Grupo Local** (snap-in do Microsoft Management Console). Se o seu ambiente de rede usa o Active Directory e você tem permissão para gerenciar a política de grupo, você pode usar o Editor de Política de Grupo Local para criar políticas para o seu site.

As configurações que você configura afetam os Objetos de Política de Grupo (GPOs) que você especifica no Console de Gerenciamento de Política de Grupo.

Importante:

Recomendamos usar o Editor de Política de Grupo Local para configurar algumas configurações de política. Exemplos incluem configurações relacionadas ao registro de VDAs com um controlador e configurações relacionadas a servidores Microsoft App-V. Validações de política adicionais são adicionadas. Como resultado, fazer um upgrade in-place pode levar à perda de dados de política se configurações de política inválidas estiverem presentes. Se você criar ou editar as políticas usando um método diferente do Web Studio, a Citrix recomenda que você use a versão mais recente do SDK e do snap-in.

Ordem de processamento e precedência da política

As configurações da política de grupo são processadas na seguinte ordem:

1. GPO Local
2. GPO do site Virtual Apps and Desktops (armazenado no banco de dados do Site)
3. GPOs em nível de site
4. GPOs de nível de domínio
5. Unidades Organizacionais

No entanto, se ocorrer um conflito, as configurações de política processadas por último sobrescrevem as configurações processadas anteriormente. A ordem de precedência para as configurações de política é a seguinte:

1. Unidades Organizacionais
2. GPOs de nível de domínio
3. GPOs no nível do site
4. GPO do site Virtual Apps and Desktops (armazenado no banco de dados do Site)
5. GPO local

Por exemplo, um administrador Citrix usa o Web Studio para criar uma política (Política A) que habilita o redirecionamento de arquivos do cliente para os funcionários de vendas da empresa. Enquanto isso, outro administrador usa o Editor de Política de Grupo para criar uma política (Política B) que desabilita o redirecionamento de arquivos do cliente para os funcionários de

vendas. Quando os funcionários de vendas fazem logon nos desktops virtuais, a Política B é aplicada e a Política A é ignorada. O motivo é que a Política B foi processada no nível do domínio e a Política A foi processada no nível do GPO do site Virtual Apps and Desktops.

No entanto, quando um usuário inicia uma sessão ICA® ou Remote Desktop Protocol (RDP), as configurações de sessão Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou usando a Configuração do Host da Sessão da Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão de cliente RDP. Os exemplos de configurações de conexão de cliente RDP são Papel de parede da área de trabalho, animação de menu e Visualizar conteúdo da janela ao arrastar.

Ao usar várias políticas, você pode priorizar políticas que contêm configurações conflitantes. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

Fluxo de trabalho para políticas Citrix

O processo para configurar políticas é o seguinte:

1. Crie a política.
2. Configure as configurações da política.
3. Atribua a política a objetos de máquina e usuário.
4. Priorize a política.
5. Verifique a política efetiva executando o assistente de Modelagem de Política de Grupo Citrix.

> **Observação:**
>
> Você abre o assistente de Modelagem de Política de Grupo Citrix navegando até a guia **Policies > Modeling** e clicando em **Launch Modeling Wizard** na barra de ações. A guia **Modeling** está disponível no Web Studio por solicitação do cliente.

navegar políticas e configurações Citrix

No Editor de Política de Grupo Local, as políticas e configurações aparecem em duas categorias: Configuração do Computador e Configuração do Usuário. Cada categoria tem um nó de Políticas Citrix. Consulte a documentação da Microsoft para obter detalhes sobre como navegar e usar este snap-in.

No Web Studio, as configurações de política são classificadas em categorias com base na funcionalidade ou recurso que afetam. Por exemplo, a seção **Gerenciamento de Perfil** inclui configurações de política para Gerenciamento de Perfil.

- As configurações de computador (configurações de política aplicadas a máquinas) definem o comportamento dos desktops virtuais e são aplicadas quando um desktop virtual é iniciado. Essas configurações são aplicadas mesmo quando não há sessões de usuário ativas no desktop virtual.
- As configurações de usuário definem a experiência do usuário ao se conectar usando ICA. As políticas de usuário são aplicadas quando um usuário se conecta ou reconecta usando ICA. As políticas de usuário não são aplicadas se um usuário se conecta usando RDP ou faz logon diretamente no console.

  Para acessar políticas, configurações ou modelos, selecione **Políticas** no painel esquerdo do Web Studio.

  - A guia **Políticas** lista todas as políticas. Ao selecionar uma política, as guias na parte inferior exibem:
    - Visão geral - Lista nome, prioridade, status ativado/desativado e descrição
    - Configurações - Lista todas as configurações configuradas
    - Atribuído a - Lista os objetos de usuário e máquina aos quais a política está atribuída. Para obter mais informações, consulte Criar políticas.
  - A guia **Modelos** lista os modelos fornecidos pela Citrix e os modelos personalizados que você criou. Ao selecionar um modelo, as guias na parte inferior exibem:
    - Descrição (por que você pode querer usar o modelo)
    - Configurações (lista de configurações configuradas). Para obter mais informações, consulte Modelos de política.
  - A guia **Comparação** permite comparar as configurações em uma política ou modelo com as configurações em outras políticas ou modelos. Por exemplo, você pode querer verificar os valores das configurações para garantir a conformidade com as melhores práticas. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

  Para pesquisar uma configuração em uma política ou modelo:

  a. Selecione a política ou o modelo.

b. Selecione **Editar política** ou **Editar modelo** na barra de ações.

c. Na página **Configurações**, digite o nome da configuração no campo de **pesquisa**:

   Você pode refinar sua pesquisa selecionando:

   - Uma versão específica do produto
   - Uma categoria (por exemplo, Largura de banda)
   - Palavras-chave no nome da configuração
   - A caixa de seleção **Ver somente selecionados**
   - Para pesquisar apenas as configurações que foram adicionadas à política selecionada.

Para uma pesquisa não filtrada, selecione **Todas as Configurações**.

- Para pesquisar uma configuração dentro de uma política:

  a. Selecione a política.

  b. Selecione a guia **Configurações** e digite o nome da configuração.

Você pode refinar sua pesquisa selecionando uma versão específica do produto ou selecionando uma categoria. Para uma pesquisa não filtrada, selecione **Todas as Configurações**.

Uma política, uma vez criada, é independente do modelo usado. Você pode usar o campo **Descrição** em uma nova política para rastrear o modelo de origem usado.

No Editor de Política de Grupo, as configurações de computador e usuário devem ser aplicadas separadamente, mesmo que criadas a partir de um modelo que inclua ambos os tipos de configurações. Neste exemplo, a escolha de usar a Experiência de Usuário de Alta Definição na Configuração do Computador:

- O modo Gráficos Legados é uma configuração de Computador que é usada em uma política criada a partir deste modelo.
- As configurações de Usuário, esmaecidas, não são usadas em uma política criada a partir deste modelo.

Editor de Política de Grupo Local(/en-us/citrix-virtual-apps-desktops/2407/media/group-policy-editor-template-example.png)

Modelos de política

> **Observação:**

> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> Modelos são coleções de configurações que são recomendadas para serem usadas na criação de políticas para alcançar resultados específicos. Por exemplo, para criar políticas para fornecer uma experiência de usuário de alta definição aos usuários finais, as configurações definidas no modelo Very High Definition User Experience podem ser usadas como referência e ponto de partida para a criação de tais políticas.

Modelos não são políticas. Modelos são documentação suplementar para as configurações de política do Citrix. Eles demonstram as funcionalidades coletivas de certas configurações relacionadas ao usuário.

O uso de modelos é opcional. Os administradores podem criar políticas sem usar modelos. Os modelos são úteis para administradores que têm uma ideia de alto nível sobre como um site deve ser configurado, mas não têm certeza de quais configurações usar para alcançar a configuração desejada.

Os administradores podem criar os modelos usando um modelo existente, uma política existente ou do zero.

ADMX/ADML

Os modelos de política de grupo do Citrix descritos aqui não têm nada a ver com os modelos de política do Windows. Os modelos descritos aqui e os modelos de política do Windows são dois conceitos diferentes. Os modelos de política de grupo do Citrix não são arquivos ADMX.

Modelos Citrix integrados

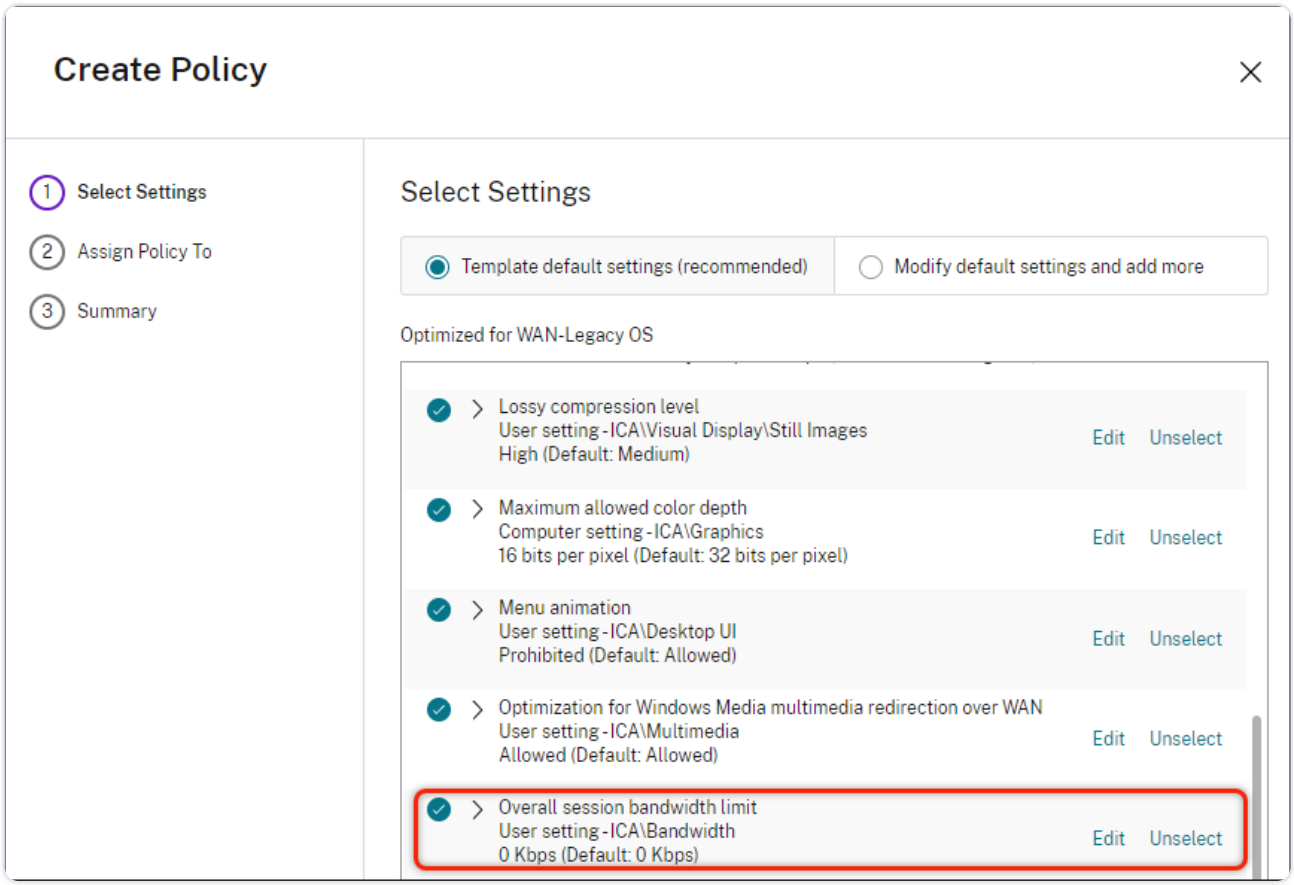
Os seguintes modelos de política estão disponíveis:

- **Experiência de Usuário de Altíssima Definição**. Este modelo impõe configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde múltiplas políticas são processadas em ordem de precedência.
- **Alta Escalabilidade de Servidor**. Aplique este modelo para economizar recursos do servidor. Este modelo equilibra a experiência do usuário e a escalabilidade do servidor. Ele oferece uma boa experiência do usuário enquanto aumenta o número de usuários que você pode hospedar

em um único servidor. Este modelo não usa um codec de vídeo para compressão de gráficos e impede a renderização multimídia do lado do servidor.

- **Alta Escalabilidade de Servidor - SO Legado**. Este modelo de Alta Escalabilidade de Servidor se aplica apenas a VDAs executando Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo depende do modo gráfico Legado, que é mais eficiente para esses sistemas operacionais.
- **Otimizado para NetScaler SD-WAN.** Aplique este modelo para usuários que trabalham em filiais com NetScaler SD-WAN para otimizar a entrega de Citrix Virtual Desktops. (NetScaler SD-WAN é o novo nome para CloudBridge).
- **Otimizado para WAN**. Este modelo é destinado a trabalhadores de tarefas em filiais que usam uma conexão WAN compartilhada ou locais remotos com conexões de baixa largura de banda acessando aplicativos com interfaces de usuário graficamente simples e pouco conteúdo multimídia. Este modelo troca a experiência de reprodução de vídeo e alguma escalabilidade do servidor por eficiência de largura de banda otimizada.
- **Otimizado para WAN-SO Legado**. Este modelo *Otimizado para WAN* se aplica apenas a VDAs executando Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo depende do modo gráfico Legado, que é mais eficiente para esses sistemas operacionais.
- **Segurança e Controle**. Use este modelo em ambientes com baixa tolerância a riscos, para minimizar os recursos habilitados por padrão no Citrix Virtual Apps and Desktops. Este modelo inclui configurações que desabilitam o acesso a impressão, área de transferência, dispositivos periféricos, mapeamento de unidade, redirecionamento de porta e aceleração Flash em dispositivos de usuário. A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade de usuários por servidor.

Embora recomendemos o uso dos modelos Citrix integrados com suas configurações padrão, existem configurações que não possuem um valor recomendado específico. Por exemplo, **Limite geral de largura de banda da sessão**, incluído nos modelos Otimizado para WAN. Neste caso, o modelo expõe a configuração para que o administrador entenda que essa configuração provavelmente se aplica ao cenário.



Se você estiver trabalhando com uma implantação (gerenciamento de políticas e VDAs) anterior ao XenApp e XenDesktop 7.6 FP3, e precisar dos modelos Alta Escalabilidade de Servidor e Otimizado para WAN, use as versões de SO Legado desses modelos quando aplicável.

> **Observação:**
>
> A Citrix cria e atualiza modelos integrados. Você não pode modificar ou excluir esses modelos.

Criar e gerenciar modelos usando o Web Studio

Para criar um modelo com base em um modelo:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e, em seguida, selecione o modelo a partir do qual você criará o modelo.
3. Selecione a guia **Criar Modelo**. A tela **Selecionar Configurações** é exibida.
4. Selecione e configure as configurações de política a serem incluídas no modelo.
5. Clique em **Avançar**. A tela **Resumo** é exibida.

6. Insira um nome para o modelo.
7. Clique em **Concluir**. O novo modelo aparece na guia **Modelos**.

Para criar um modelo com base em uma política:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Políticas** e, em seguida, selecione a política a partir da qual você criará o modelo.
3. Clique na guia **Mais**.
4. Selecione **Salvar como Modelo**. A tela **Selecionar Configurações** é exibida.
5. Selecione e configure quaisquer novas configurações de política para incluir no modelo.
6. Clique em **Avançar**. A tela **Resumo** é exibida.
7. Insira um nome e uma descrição para o modelo e, em seguida, clique em **Concluir**.

Modelos e administração delegada

Os modelos no Web Studio são armazenados no banco de dados do site, ao contrário dos modelos no Citrix Studio, que são armazenados como arquivos na pasta de perfil de usuário do administrador atual com uma extensão `.gpt`. Os modelos do Citrix Studio criados por um administrador não são visíveis para outros administradores ou para o mesmo administrador em uma máquina diferente. Os modelos do Web Studio são visíveis para todos os administradores, sujeitos a permissões e administração delegada.

Criar políticas

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

> Antes de criar uma política, decida qual grupo de usuários ou dispositivos ela pode afetar. Você pode querer criar uma política baseada na função de trabalho do usuário, tipo de

> conexão, dispositivo do usuário ou localização geográfica. Você também pode usar os mesmos critérios que usa para as políticas de grupo do Windows Active Directory.

Se você já criou uma política que se aplica a um grupo, considere editar essa política em vez de criar outra. Após editar a política, configure as configurações apropriadas. Evite criar uma política apenas para habilitar uma configuração específica ou para excluir a política de se aplicar a determinados usuários.

Ao criar uma política, você pode baseá-la nas configurações de um modelo de política e personalizar as configurações conforme necessário. Você também pode criá-la sem usar um modelo e adicionar todas as configurações de que precisa.

No Web Studio, as novas políticas criadas são definidas como Desabilitadas, a menos que a caixa de seleção **Habilitar política** seja explicitamente marcada.

Durante a criação da política e ao configurar as definições, o sistema oferece uma opção para visualizar o tipo de definição. Você pode visualizar os seguintes tipos de definições:

- Todas as configurações - Visualizar todas as aplicáveis a todas as versões do VDA
- Somente configurações atuais - Visualizar configurações específicas da versão atual do VDA
- Somente configurações legadas - Visualizar configurações aplicáveis apenas às versões VDA descontinuadas

Para visualizar as configurações ao configurá-las:

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Na guia **Políticas**, clique em **Criar Política**.
3. Na tabela **Selecionar Configurações**, clique na lista suspensa ao lado de **Configurações**.
4. Selecione uma das seguintes opções na lista suspensa:

- Todas as configurações - Visualizar todas as configurações para todas as versões do VDA
- Somente configurações atuais - Exibir configurações apenas para as versões atuais do VDA
- Somente configurações herdadas - Exibir configurações apenas para as versões VDA obsoletas

1. A tabela **Configurações** lista as configurações disponíveis com base na etapa anterior.

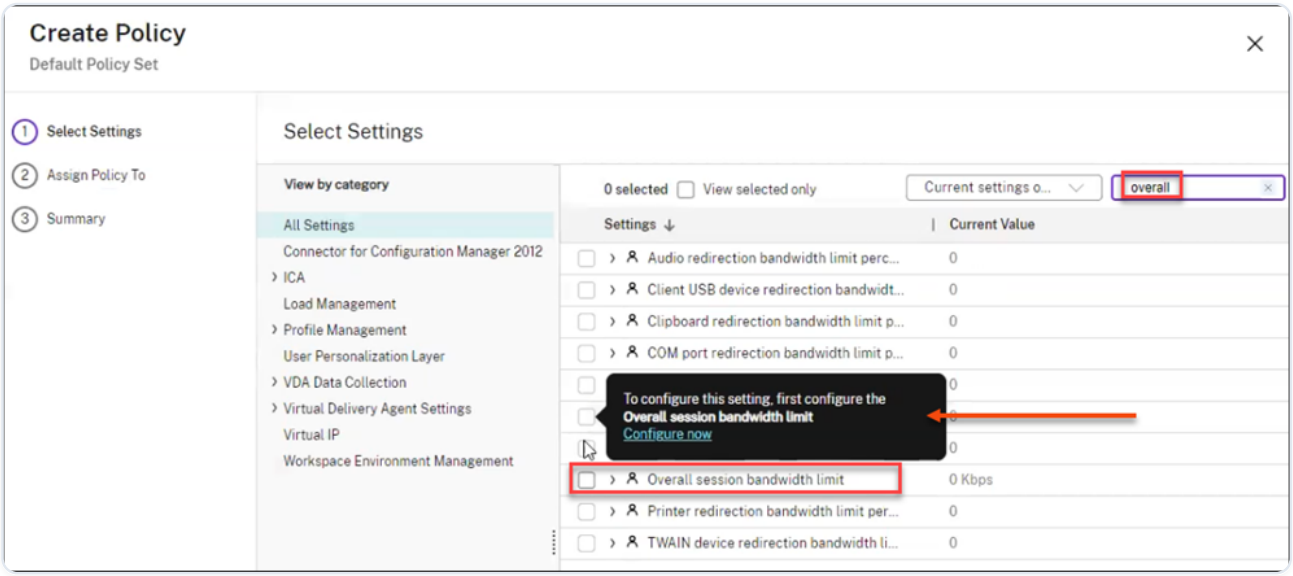
Configurações de política

As configurações de política podem ser habilitadas, desabilitadas ou não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

As configurações de política são aprimoradas para fornecer clareza entre políticas dependentes. Esse recurso garante que a política pai seja configurada primeiro para que as configurações da política filha entrem em vigor quando configuradas.

Para configurar as configurações de política:

1. Na página **Criar Política**, em **Selecionar Configurações**, procure por "geral". Todas as políticas (pai e filhas) relacionadas a **Limite geral de largura de banda da sessão** são listadas.
2. Ao passar o mouse sobre uma política filha, uma dica de ferramenta informa que a política filha não pode ser configurada até que a política pai **Limite geral de largura de banda da sessão** seja configurada.
3. Configure as configurações da política pai e, em seguida, configure as configurações da política filha e clique em **Salvar**.
4. As colunas **Configurações** e **Valor Atual** mostram os valores configurados na tabela **Criar/ Editar política**. A tabela mostra a opção **Editar** para você modificar as configurações configuradas.



Nota:

- As políticas filhas não podem ser selecionadas até que a política pai seja configurada.
- Se a política pai for desmarcada, uma mensagem pop-up informa que as políticas filhas associadas também serão desmarcadas ou desselecionadas.

A tabela a seguir fornece a lista de políticas pai, juntamente com as políticas dependentes ou filhas correspondentes.

POLÍTICA PAI	POLÍTICAS FILHAS DEPENDENTES
Limite geral de largura de banda da sessão	Porcentagem de limite de largura de banda de redirecionamento de áudio
	Porcentagem de limite de largura de banda de redirecionamento da área de transferência
	Porcentagem de limite de largura de banda de redirecionamento de porta COM
	Porcentagem de limite de largura de banda de redirecionamento de arquivo
	Porcentagem de limite de largura de banda de aceleração multimídia HDX™ MediaStream
	Porcentagem de limite de largura de banda de redirecionamento de porta LPT
	Porcentagem de limite de largura de banda de redirecionamento de impressora
	Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente
	Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN
Permitir redirecionamento de conteúdo bidirecional	URLs permitidas para serem redirecionadas para o Cliente

POLÍTICA PAI	POLÍTICAS FILHAS DEPENDENTES
	URLs permitidas para serem redirecionadas para o VDA
Uso da CPU	Prioridade de processo excluída do uso da CPU
Modo gráfico legado	Nível de compressão progressiva
Habilitar marca d'água da sessão	Texto personalizado da marca d'água
	Estilo da marca d'água da sessão
	Transparência da marca d'água
Transporte adaptável HDX	Modo tolerante a perdas para áudio

Algumas configurações de política podem estar em um dos seguintes estados:

- Permitido ou Proibido permite ou impede a ação controlada pela configuração. Às vezes, os usuários são permitidos ou impedidos de gerenciar a ação da configuração em uma sessão. Por exemplo, se a configuração de animação de menu for definida como Permitido, os usuários poderão controlar as animações de menu em seu ambiente cliente.
- Ativado ou Desativado liga ou desliga a configuração. Se você desativar uma configuração, ela não será ativada em políticas de classificação inferior.

Além disso, algumas configurações controlam a eficácia de configurações dependentes. Por exemplo, o redirecionamento de unidade cliente controla se os usuários têm permissão para acessar as unidades em seus dispositivos. Tanto esta configuração quanto a configuração de **Unidades de rede cliente** devem ser adicionadas à política para permitir que os usuários acessem suas unidades de rede. Se a configuração de **Redirecionamento de unidade cliente** estiver desativada, os usuários não poderão acessar suas unidades de rede, mesmo que a configuração de **Unidades de rede cliente** esteja ativada.

Em geral, as alterações nas configurações de política que afetam as máquinas entram em vigor quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon. As alterações nas configurações de política que afetam os usuários entram em vigor na próxima vez que os usuários fizerem logon. Se você estiver usando o Active Directory, as configurações de política serão atualizadas quando o Active Directory reavaliar as políticas em intervalos de 90 minutos. E as

configurações de política são aplicadas quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon.

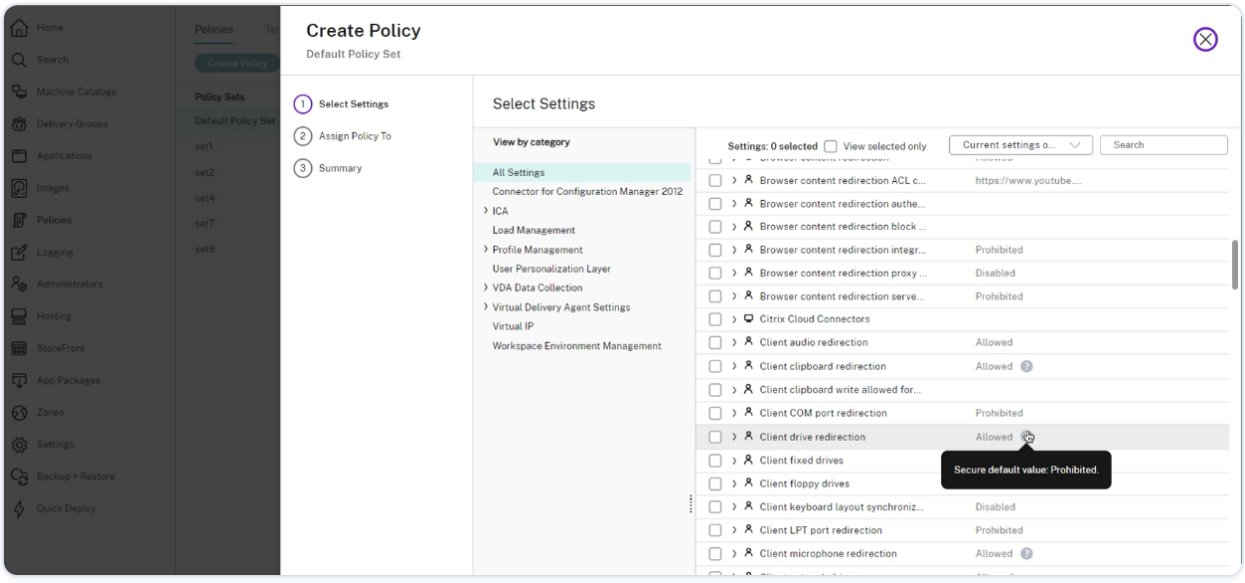
Para algumas configurações de política, você pode inserir ou selecionar um valor ao adicionar a configuração a uma política. Você pode limitar a configuração da configuração selecionando Usar valor padrão. Essa seleção desativa a configuração da configuração e permite que apenas o valor padrão da configuração seja usado quando a política é aplicada. Essa seleção é independente do valor que foi inserido antes de selecionar Usar valor padrão.

Se a configuração padrão segura estiver ativada, durante a instalação do VDA, a prioridade das configurações de política será afetada da seguinte forma:

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

Para ver a configuração padrão segura para uma política:

1. Faça logon no Web Studio.
2. Na navegação à esquerda, clique em **Políticas**.
3. Na guia **Políticas**, clique em **Criar Política**.
4. Na tabela **Selecionar Configurações**, ao passar o mouse sobre as configurações que têm **Permitido ?** como seu valor atual, o **Valor padrão seguro: Proibido** é exibido.



Como melhores práticas:

- Atribua políticas a grupos em vez de usuários individuais. Se você atribuir políticas a grupos, as atribuições serão atualizadas automaticamente quando você adicionar ou remover usuários do grupo.
- Não ative configurações conflitantes ou sobrepostas na Configuração do Host da Sessão da Área de Trabalho Remota. Às vezes, a Configuração do Host da Sessão da Área de Trabalho Remota oferece funcionalidade semelhante às configurações de política do Citrix. Quando possível, mantenha todas as configurações consistentes (ativadas ou desativadas) para facilitar a solução de problemas.
- Desative 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, ou especificar atribuições mas desativá-las, a política será aplicada a **todas** as conexões.

> **Observação:**
>
> As atribuições de política também são conhecidas como filtros de política. Para obter informações adicionais, consulte os seguintes tópicos:
>
> - Criar, modificar ou excluir um filtro para uma política
> - Como os filtros são aplicados?

A tabela a seguir lista as atribuições disponíveis:

NOME DA ATRIBUIÇÃO	APLICA UMA POLÍTICA COM BASE EM
Controle de Acesso	Condições de controle de acesso através das quais um cliente está se conectando. *Tipo de conexão* - Se a política deve ser aplicada a conexões feitas com ou sem o NetScaler® Gateway. *Nome do farm do NetScaler*

NOME DA ATRIBUIÇÃO	APLICA UMA POLÍTICA COM BASE EM
	Gateway - Nome do servidor virtual do NetScaler Gateway. *Condição de acesso* - Nome da política de análise de ponto de extremidade ou política de sessão a ser usada.
NetScaler SD-WAN	Se uma sessão de usuário é iniciada através do NetScaler SD-WAN. **Nota:** Você pode adicionar apenas uma atribuição de NetScaler SD-WAN a uma política.
Endereço IP do Cliente	Endereço IP do dispositivo do usuário usado para se conectar à sessão: Exemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; Exemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nome do Cliente	Nome do dispositivo do usuário. Correspondência exata: ClientABCName. Usando curinga: Client*Name.
Grupo de Entrega	Associação ao 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. **Nota:** As opções de filtro de área de trabalho privada e área de trabalho compartilhada estão disponíveis apenas para Citrix Virtual Apps and Desktops 7.x. Para obter mais informações, consulte CTX219153.
Unidade Organizacional (OU)	Unidade organizacional.
Tag	Tags. **Nota:** Aplique esta política a todas as máquinas marcadas. As tags de aplicativo não estão incluídas.
Usuário ou Grupo	Nome de usuário ou grupo.

Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas por ordem de prioridade e várias instâncias de qualquer configuração são comparadas. Cada configuração é aplicada de acordo com a classificação de prioridade da política. Qualquer configuração de política desabilitada tem precedência sobre uma configuração de classificação inferior que esteja habilitada. As configurações de política que não são configuradas são ignoradas.

> **Importante:**

> Ao configurar políticas do Active Directory e do Citrix usando o Console de Gerenciamento de Política de Grupo, as atribuições e configurações podem não ser aplicadas conforme o esperado. Para obter mais informações, consulte CTX127461

> Uma política chamada "Não Filtrada" é fornecida por padrão.

- Se você usar o Web Studio para gerenciar políticas Citrix, as configurações adicionadas à política Não Filtrada serão aplicadas a todos os servidores, áreas de trabalho e conexões em um Site.
- Se você usar o Editor de Política de Grupo Local para gerenciar políticas Citrix, as configurações adicionadas à política Não Filtrada serão aplicadas a todos os Sites e conexões. Os Sites e as conexões devem estar dentro do escopo dos Objetos de Política de Grupo (GPOs) que incluem a política. Por exemplo, a OU de Vendas inclui um GPO chamado Vendas-EUA que inclui todos os membros da equipe de vendas dos EUA. O GPO Vendas-EUA é configurado com uma política Não Filtrada que inclui várias configurações de política de usuário. Quando o gerente de Vendas dos EUA faz logon no Site, as configurações da política Não Filtrada 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 for definido como Permitir (o padrão), a política será aplicada apenas a conexões que correspondem aos critérios de atribuição. Se o modo for definido como Negar, 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 do mesmo tipo com modos diferentes** - Em políticas com duas atribuições do mesmo tipo, uma definida como Permitir e outra como Negar, a atribuição

definida como Negar tem precedência, desde que a conexão satisfaça ambas as atribuições. Por exemplo:

A Política 1 inclui as seguintes atribuições:

- A Atribuição A especifica o grupo de Vendas. O modo está definido como Permitir.
- A Atribuição B especifica a conta do gerente de Vendas. O modo está definido como Negar.

Como o modo para a Atribuição B está definido como Negar, a política não é aplicada quando o gerente de Vendas faz logon no Site, mesmo que o usuário seja membro do grupo de Vendas.

- **Exemplo: Atribuições de tipos diferentes com modos semelhantes** - Em políticas com duas ou mais atribuições de tipos diferentes, definidas como Permitir, 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:

  - A Atribuição C é uma atribuição de Usuário que especifica o grupo de Vendas. O modo está definido como Permitir.
  - A Atribuição D é uma atribuição de Endereço IP do Cliente que especifica 10.8.169.* (a rede corporativa). O modo está definido como Permitir.

  Quando o gerente de Vendas faz logon no Site do escritório, a política é aplicada porque a conexão satisfaz ambas as atribuições.

  A Política 3 inclui as seguintes atribuições:

  - A Atribuição E é uma atribuição de Usuário que especifica o grupo de Vendas. O modo está definido como Permitir.
  - A Atribuição F é uma atribuição de Controle de Acesso que especifica as condições de conexão do NetScaler Gateway. O modo está definido como Permitir.

  Quando o gerente de Vendas faz logon no Site do escritório, a política não é aplicada porque a conexão não satisfaz a Atribuição F.

Criar uma política com base em um modelo, usando o Web Studio

1. Faça logon no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e selecione um modelo.

3. Selecione **Criar Política a partir do Modelo** na barra de ações.
4. Por padrão, a nova política usa todas as configurações padrão do modelo. Neste caso, **Configurações padrão do modelo (recomendado)** está selecionado. Se você quiser alterar as configurações, selecione **Modificar configurações padrão e adicionar mais**, e então adicione ou remova configurações.
5. Especifique como aplicar a política selecionando uma das seguintes opções:
   - **Objetos de usuário e máquina selecionados**. Para aplicar a política a objetos de usuário e máquina selecionados e, em seguida, clique em **Atribuir** para selecionar os objetos de usuário e máquina aos quais a política deve ser aplicada.
   - **Todos os objetos no site**. Para aplicar a política a todos os objetos de usuário e máquina no site.
6. Insira um nome para a política. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

   A política é desabilitada por padrão; você pode habilitá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem logon. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

Criar uma política usando o Web Studio

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Políticas**.
3. Selecione **Criar Política** na barra de ações.
4. Adicione e configure as configurações da política.
5. Especifique como aplicar a política escolhendo uma das seguintes opções:
   - Atribua a objetos de usuário e máquina selecionados e, em seguida, selecione os objetos de usuário e máquina aos quais a política deve ser aplicada.
   - Atribua a todos os objetos em um site para aplicar a política a todos os objetos de usuário e máquina no Site.
6. Insira um nome para a política ou aceite o padrão. Considere nomear a política de acordo com quem ou o que ela afeta, por exemplo, Departamento de Contabilidade ou Usuários Remotos. Opcionalmente, adicione uma descrição.

A política é habilitada por padrão; você pode desativá-la. Habilitar a política permite que ela seja aplicada imediatamente aos usuários que fazem logon. Desabilitar impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, considere desabilitar a política até que esteja pronto para aplicá-la.

Criar e gerenciar políticas usando o Editor de Política de Grupo

No Editor de Política de Grupo, expanda **Configuração do Computador ou Configuração do Usuário**. Expanda o nó **Políticas** e selecione **Políticas Citrix**. Escolha a ação apropriada:

TAREFA	INSTRUÇÃO
Criar uma política	Na guia **Políticas**, clique em **Novo**.
Editar uma política existente	Na guia **Políticas**, selecione a política e clique em **Editar**.
Alterar a prioridade de uma política existente	Na guia **Políticas**, selecione a política e clique em **Superior** ou **Inferior**.
Exibir informações de resumo sobre uma política	Na guia **Políticas**, selecione a política e clique na guia **Resumo**.
Exibir e alterar as configurações da política	Na guia **Políticas**, selecione a política e clique na guia **Configurações**.
Visualizar e alterar filtros de política	Na guia **Políticas**, selecione a política e clique na guia **Filtros**. Ao adicionar mais de um filtro a uma política, todas as condições de filtro devem ser atendidas para que a política seja aplicada.
Habilitar ou desabilitar uma política	Na guia **Políticas**, selecione a política e, em seguida, selecione **Ações > Habilitar** ou **Ações > Desabilitar**.
Criar uma política a partir de um modelo existente	Na guia **Modelos**, selecione o modelo e clique em **Nova Política**.

Conjuntos de políticas

Conjuntos de políticas são objetos no Citrix Virtual Apps and Desktops™ que agregam políticas para permitir acesso simplificado e baseado em função, e gerenciamento fácil. Você pode criar conjuntos de políticas para espelhar divisões lógicas em sua equipe de administradores e empresa. Por exemplo, você pode criar um conjunto de políticas para cada região geográfica, unidade de negócios ou para um caso de uso específico. Uma vez criados, escopos e grupos de entrega são atribuídos a conjuntos de políticas para que apenas administradores autorizados possam gerenciar as políticas que se aplicam aos seus usuários e máquinas relevantes.

> **Observação:**

> Antes de habilitar os conjuntos de políticas, a Citrix® recomenda que você observe o seguinte:

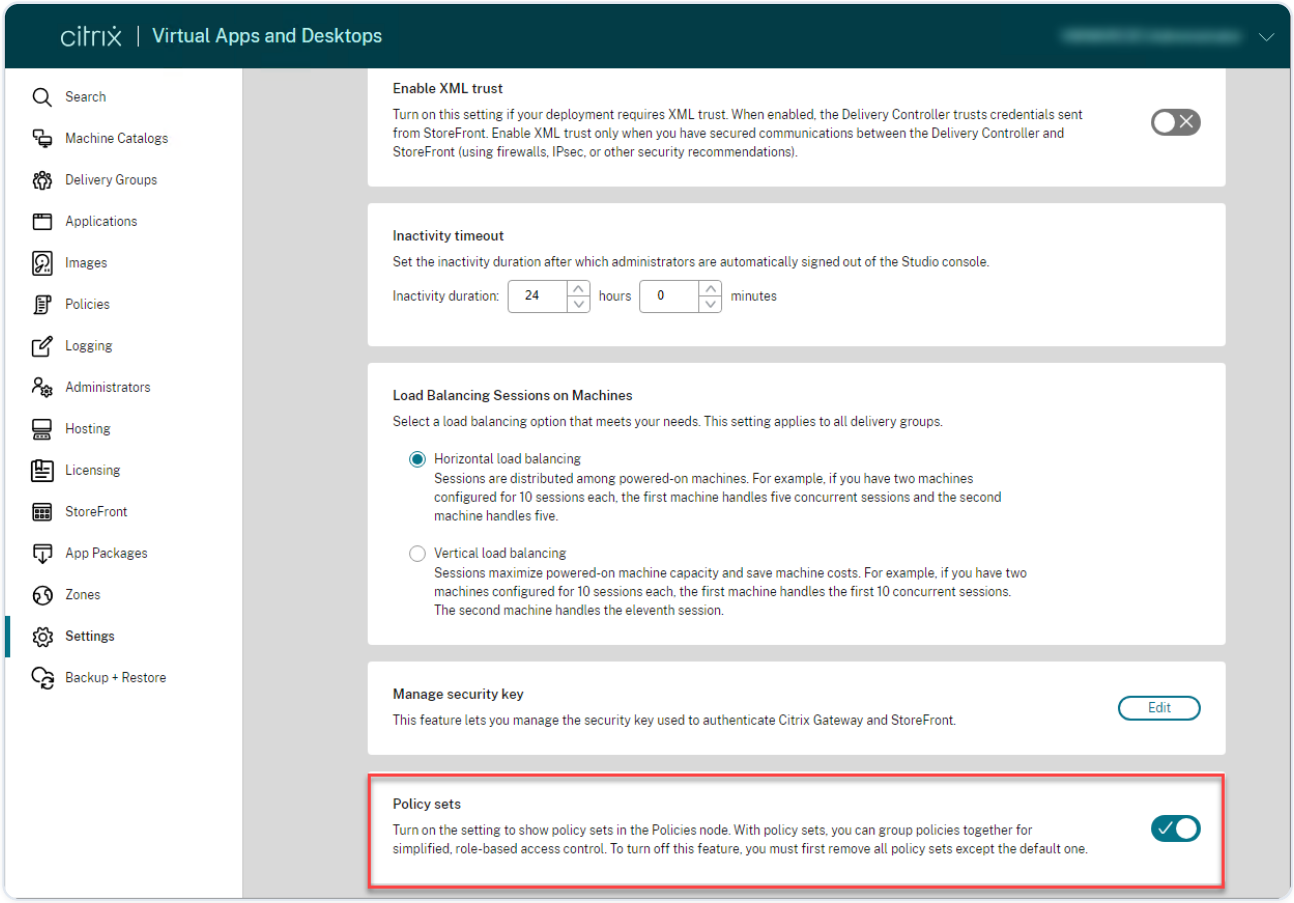
- Validações de política adicionais são adicionadas. Como resultado, fazer um upgrade no local pode levar à perda de dados da política se configurações de política inválidas estiverem presentes.
- Para detectar os dados inválidos, use a ferramenta de scanner GPO e faça as edições necessárias antes de fazer o upgrade. Para obter mais informações, consulte CTX676686.
- Para todos os upgrades futuros, a Citrix recomenda que você use o SDK mais recente. Usar um SDK mais antigo para atualizar políticas pode permitir a adição de dados inválidos às configurações da política, o que pode levar ao risco de perda de dados da política.

Benefícios

- Controle de acesso baseado em função para equipes de administradores distribuídas
- Fusões, aquisições e consolidações simplificadas
- Domínio de falha limitado
- Suporte multilocatário para políticas

Habilitar conjuntos de políticas

Na guia **Gerenciar** do Virtual Apps and Desktops, navegar para **Configurações** e ative a configuração **Conjuntos de políticas**.



Observação:

Você deve habilitar os 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 dentro do Citrix Studio.	Políticas, configurações, filtros e prioridades de políticas são configurados separadamente para cada conjunto de políticas.
Se você gerencia uma política, você deve gerenciar todas as políticas.	Administradores completos podem delegar a administradores de nível inferior a capacidade

ANTES DE APLICAR CONJUNTOS DE POLÍTICAS	DEPOIS DE APLICAR CONJUNTOS DE POLÍTICAS
	de gerenciar um conjunto de políticas específico individualmente.
As políticas em ambientes grandes e distribuídos tornam-se complexas e difíceis de gerenciar.	As políticas em ambientes grandes e distribuídos podem ser divididas e gerenciadas facilmente.

Como 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 conjunto de políticas atribuído recebem o conjunto de políticas padrão
- Um grupo de entrega pode ter apenas um conjunto de políticas atribuído a ele
- Vários grupos de entrega podem usar o mesmo conjunto de políticas
- Mesmo que os conjuntos de políticas sejam atribuídos a grupos de entrega, as políticas mantêm seus filtros

Para obter mais informações, consulte Como os filtros são aplicados?. Não há alteração na forma como as atribuições de política ou os filtros de política funcionam para conjuntos de políticas. Ou seja, eles funcionam da mesma forma que para as políticas.

Conjunto de políticas padrão

- Quando a configuração do conjunto de políticas é 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 de administradores crie um conjunto de políticas e o atribua a um grupo de entrega.
- Depois que um grupo de entrega tiver um conjunto de políticas diferente atribuído a ele, ele não receberá mais políticas do conjunto de políticas padrão

Criação de conjunto de políticas

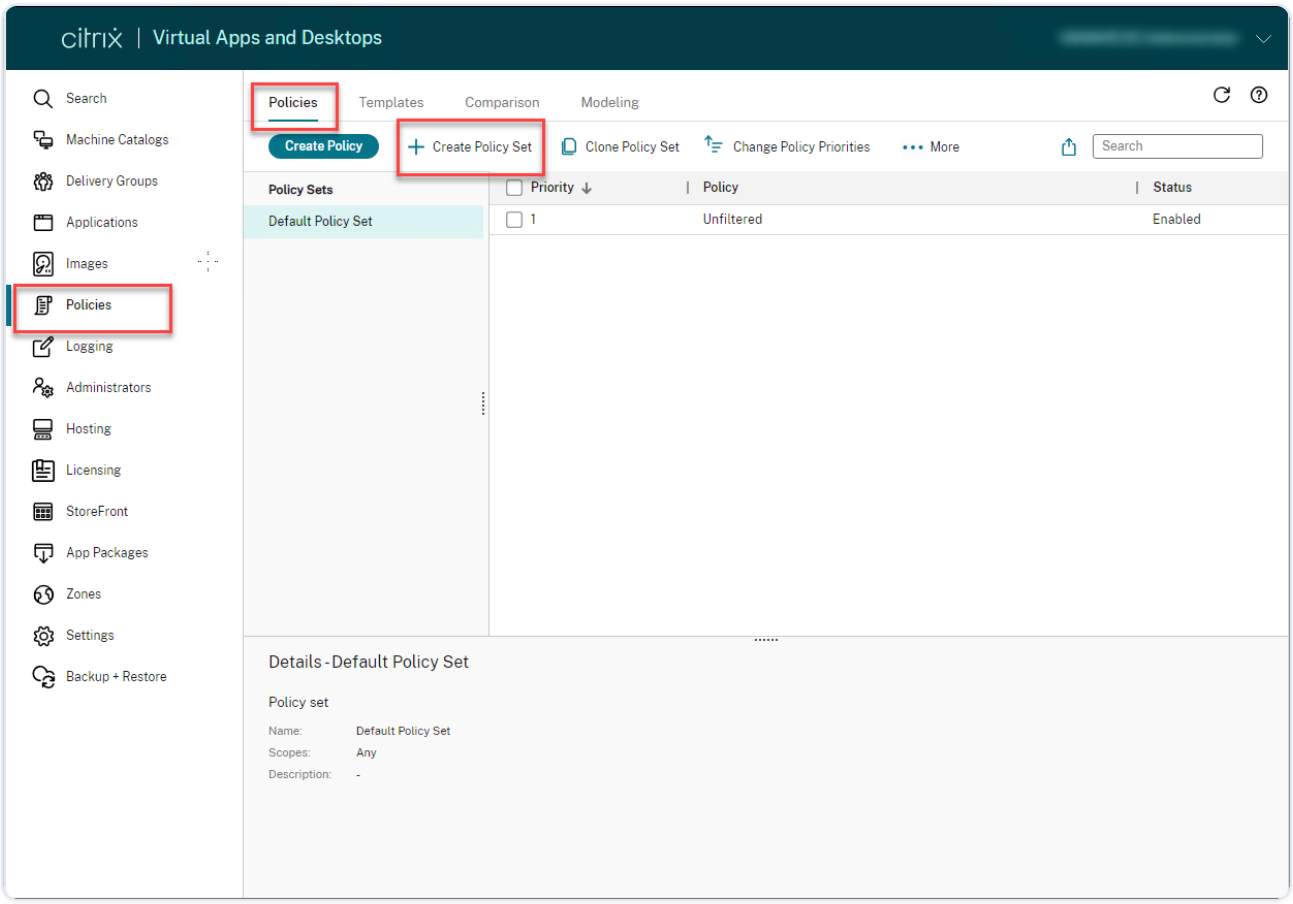
Os conjuntos de políticas podem ser criados das duas maneiras a seguir:

- Criar conjunto de políticas - esta ação cria um conjunto de políticas vazio

- Clonar conjunto de políticas - esta ação cria um conjunto de políticas com base em um conjunto de políticas existente

Criar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.



1. Selecione **Criar Conjunto de Políticas**. A guia **Introdução** é exibida.
2. Clique em **Avançar** ou clique na guia **Nome e Descrição**.
3. Insira o nome e a descrição do conjunto de políticas.
4. Clique em **Avançar** ou clique na guia **Atribuições**.
5. Selecione um ou mais grupos de entrega aos quais você deseja atribuir o conjunto de políticas.
6. Clique em **Avançar** ou clique na guia **Escopos**.
7. Selecione os escopos do conjunto de políticas.
8. Clique em **Criar**. O conjunto de políticas é criado com a atribuição e o escopo definidos.

Clonar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.

2. Selecione **Clonar Conjunto de Políticas**.
3. Modifique o nome do conjunto de políticas.
4. Modifique ou crie atribuições para o conjunto de políticas e clique em **Avançar**.
5. Selecione ou desmarque as políticas a serem incluídas no conjunto de políticas clonado.
6. Modifique o escopo da política.
7. Clique em **Criar**. O conjunto de políticas é criado.

Editar conjuntos de políticas

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Selecione **Editar Conjunto de Políticas**.
3. Modifique o nome do conjunto de políticas e clique em **Avançar**.
4. Modifique ou crie atribuições para o conjunto de políticas e clique em **Avançar**.
5. Modifique o escopo da política.
6. Clique em **Criar**.

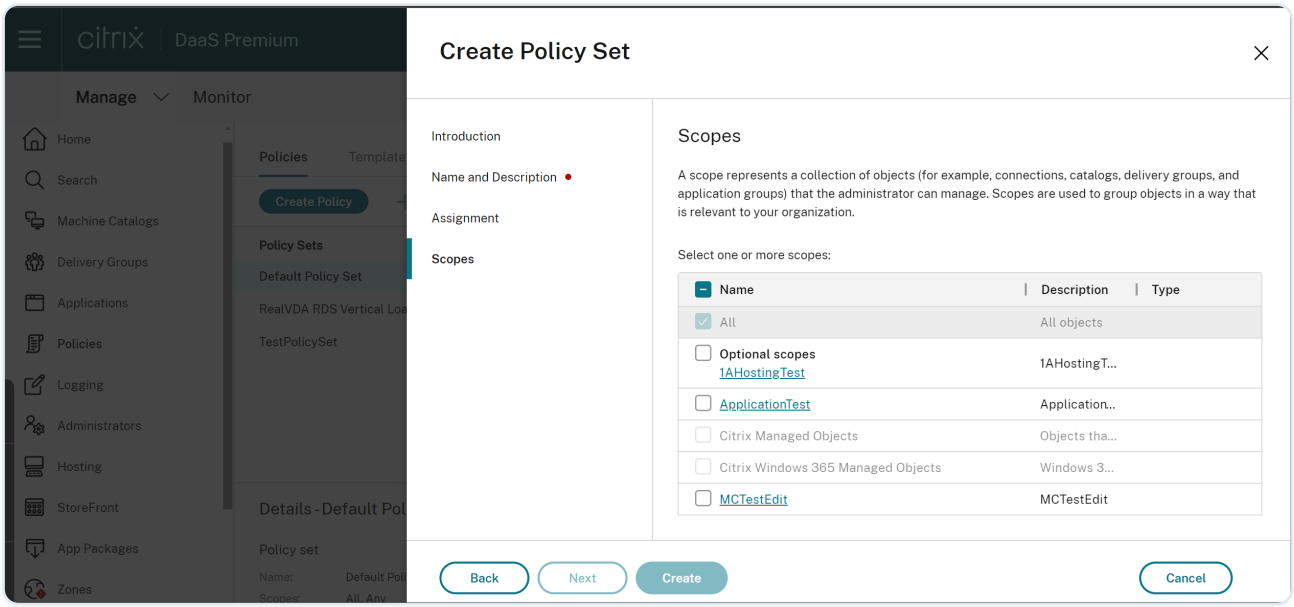
Atribuição de conjunto de políticas

Os conjuntos de políticas são atribuídos a 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 de conjunto de políticas

Os administradores podem definir o escopo do conjunto de políticas para que apenas administradores autorizados possam visualizá-lo ou editá-lo. Você pode configurar escopos quando o conjunto de políticas é criado ou editado.

Com a introdução dos Conjuntos de Políticas, você também pode criar e gerenciar a Política Citrix usando a API. Para obter mais informações, consulte Como criar um conjunto de políticas no Citrix DaaS.



Comparar, priorizar, modelar e solucionar problemas de políticas

Observação:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Você pode usar várias políticas para personalizar seu ambiente e atender às necessidades dos usuários com base em suas funções de trabalho, localizações geográficas ou tipos de conexão. Por exemplo, para segurança aprimorada, imponha restrições a grupos de usuários que interagem regularmente com dados confidenciais.

Você também pode criar uma política que impeça os usuários de salvar arquivos confidenciais em suas unidades de cliente locais. No entanto, se alguns usuários no grupo de usuários precisarem de acesso às suas unidades locais, você poderá criar outra política apenas para esses usuários. Em seguida, você classifica ou prioriza 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 efetiva quando as políticas entram em conflito.

Em geral, as políticas substituem configurações semelhantes configuradas para todo o Site, para Delivery Controllers específicos ou no dispositivo do usuário. A exceção a este princípio é a segurança. A configuração de criptografia mais alta em seu ambiente sempre substitui outras configurações e políticas. A configuração de criptografia mais alta inclui o sistema operacional e as configurações de sombreamento mais restritivas.

As políticas Citrix interagem com as políticas que você define em seu sistema operacional. Em um ambiente Citrix, as configurações Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou usando a Configuração do Host da Sessão da Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão de cliente do Protocolo de Área de Trabalho Remota (RDP). As configurações típicas de RDP incluem configurações como papel de parede da área de trabalho, animação de menu e visualização do conteúdo da janela ao arrastar.

Algumas configurações de política, como Secure ICA®, devem corresponder às configurações do sistema operacional. Se um nível de criptografia de prioridade mais alta for definido em outro lugar, as configurações da **política Secure ICA** que você especificar na política ou ao entregar aplicativos e desktops poderão ser substituídas.

Por exemplo, as configurações de criptografia que você especifica ao criar Grupos de Entrega devem estar no mesmo nível das configurações de criptografia que você especificou em todo o seu ambiente.

> **Observação:**
>
> No segundo salto de cenários de salto duplo, considere que um VDA de SO de sessão única se conecta a um VDA de SO de múltiplas sessões. Neste caso, as políticas Citrix atuam no VDA de SO de sessão única como se fosse o dispositivo do usuário. Por exemplo, considere que as políticas estão configuradas para armazenar imagens em cache no dispositivo do usuário. Neste exemplo, as imagens armazenadas em cache para o segundo salto em um cenário de salto duplo são armazenadas em cache na máquina VDA de SO de sessão única.

Usar o assistente de modelagem de política

A modelagem de política ajuda você a simular políticas habilitadas com filtros para fins de planejamento e teste. Somente políticas habilitadas com filtros são modeladas. Políticas desabilitadas nunca são aplicadas e políticas habilitadas sem filtros são sempre aplicadas.

Execute as seguintes etapas para abrir o assistente de **Modelagem de Política**:

1. Selecione **Políticas** na navegação à esquerda.
2. Selecione a guia **Modelagem**.
3. Selecione **Modelagem de Política** na barra de ações.
4. Leia a página **Introdução** e clique em **Avançar**.
5. Selecione usuários ou computadores. Você pode procurar por contêineres ou usuários ou computadores específicos. Clique em **Avançar**.
6. Escolha sua evidência de filtro. Opcionalmente, você pode ser mais granular com sua simulação inserindo detalhes adicionais, como **Grupo de entrega**, **Tags**, **Endereço IP do cliente** e assim por diante. Clique em **Avançar**.
7. Revise o resumo de suas seleções e clique em **Executar**.

Depois de clicar em **Executar**, o assistente gera um relatório dos resultados da modelagem. Ao visualizar este relatório, você pode:

- Selecione se deseja visualizar **Todas as configurações**, **Configurações do computador** ou **Configurações do usuário** no menu suspenso.
- Use a barra de pesquisa para procurar configurações específicas.
- Clique em uma configuração específica para ver os detalhes dessa configuração. Por exemplo, se todas as configurações de usuário não foram aplicadas para uma política específica, o painel **Detalhes** mostra o motivo pelo qual as configurações não foram aplicadas.
- Clique em **Exportar** para exportar os resultados da modelagem no formato JSON, formato HTML ou ambos.

Após executar a modelagem de política, mais opções ficam disponíveis para você. Você pode:

- **Exibir Relatório de Modelagem**: Isso abre o mesmo relatório de modelagem de cima para que você possa visualizá-lo novamente ou exportá-lo.
- **Executar Novamente a Modelagem de Política**: Isso permite que você execute novamente a modelagem de política com o mesmo conjunto de critérios selecionados anteriormente e gere

novos resultados de modelagem. Isso é útil se algumas políticas foram alteradas e você gostaria de ver como essas alterações afetam seu modelo atual.

- **Excluir Relatório de Modelagem**: Isso exclui o relatório de modelagem atual.

Comparar políticas e modelos

Você pode comparar as configurações em uma política ou modelo com as configurações das outras políticas ou modelos. Por exemplo, você pode precisar verificar os valores das configurações para manter a conformidade com as melhores práticas. Você também pode querer comparar as configurações em uma política ou modelo com as configurações padrão fornecidas pela Citrix.

1. Faça login no Web Studio e selecione **Políticas** no painel esquerdo.
2. Clique na guia **Comparação** e, em seguida, clique em **Selecionar**.
3. Escolha as políticas ou modelos a serem comparados. Para incluir valores padrão na comparação, selecione a caixa de seleção **Comparar com as configurações padrão**.
4. Depois de clicar em **Comparar**, as configurações configuradas são exibidas em colunas.
5. Para ver todas as configurações, selecione **Mostrar Todas as Configurações**. Para retornar à visualização padrão, selecione **Mostrar Configurações Comuns**.

Priorizar políticas

Priorizar políticas permite definir a precedência das políticas quando elas contêm configurações conflitantes. 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 qualquer configuração são comparadas. Cada configuração é aplicada de acordo com a classificação de prioridade da política.

Você prioriza as políticas atribuindo-lhes diferentes números de prioridade. Por padrão, as novas políticas recebem a prioridade mais baixa. Se as configurações da política entrarem em conflito, uma política com prioridade mais alta (um número de prioridade 1 é o mais alto) substitui uma política com prioridade mais baixa. As configurações são mescladas de acordo com a prioridade e a condição da configuração. Por exemplo, se a configuração está desabilitada ou habilitada. Qualquer configuração desabilitada substitui uma configuração de classificação inferior que esteja habilitada. As configurações de política que não são configuradas são ignoradas e não substituem as configurações de classificações inferiores.

1. Selecione **Políticas** no painel esquerdo. Certifique-se de selecionar a guia **Políticas**.

2. Na guia **Políticas**, selecione **Alterar Prioridades de Política** na barra de ações. A página **Alterar Prioridades de Política** é exibida.
3. Na lista de prioridades, use uma das seguintes maneiras para alterar a prioridade de uma política:
    - Arraste a política para a posição desejada.
    - Para movê-lo para cima ou para baixo em uma posição, clique no ícone de seta Para Cima ou Para Baixo, respectivamente.
    - Para movê-lo para o início ou fim da lista, clique no ícone de seta Início ou Fim, respectivamente.
    - Para alterar o número de prioridade, clique no ícone **Editar**, insira um número conforme necessário e, em seguida, clique em **Salvar**.
4. Clique em **Salvar**.

Exceções

Ao criar políticas para grupos de usuários, dispositivos de usuário ou máquinas, você pode descobrir que alguns membros do grupo exigem exceções a algumas configurações de política. Você pode criar exceções por meio de:

- Criar uma política apenas para os membros do grupo que precisam das exceções e, em seguida, classificar a política com uma prioridade maior do que a política para o grupo inteiro
- Usar o modo Negar para uma atribuição adicionada à política

Uma atribuição com o modo definido como Negar aplica uma política apenas a conexões que não correspondem aos critérios de atribuição. Por exemplo, uma política inclui as seguintes atribuições:

- A Atribuição A é uma atribuição de endereço IP de cliente que especifica o intervalo 208.77.88.*. O modo está definido como Permitir
- A Atribuição B é uma atribuição de usuário que especifica uma conta de usuário específica. O modo está definido como Negar.

A política é aplicada a todos os usuários que fazem logon no Site com endereços IP no intervalo especificado na Atribuição A. No entanto, a política não é aplicada ao usuário que faz logon no Site com a conta de usuário especificada na Atribuição B.

Determinar quais políticas se aplicam a uma conexão

Uma conexão pode não responder como esperado porque várias políticas se aplicam. Se uma política de prioridade mais alta se aplicar a uma conexão, ela poderá substituir as configurações que você configurou na política original. Você pode calcular o Conjunto Resultante de Política e determinar como as configurações finais da política são mescladas para uma conexão.

Você pode calcular o Conjunto Resultante de Política das seguintes maneiras:

- Use o Assistente de **Modelagem de Política de Grupo Citrix** 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:
  - Controlador de domínio
  - Usuários
  - Valores de evidência de atribuição de política Citrix
  - Configurações de ambiente simulado, como conexão de rede lenta O relatório que o assistente produz lista as políticas Citrix que entram em vigor no cenário. Como você faz logon no Controller como um usuário de domínio, o assistente calcula os resultados usando as configurações de política de site e os Objetos de Política de Grupo (GPOs) do Active Directory.
- Use **Resultados da Política de Grupo** para produzir um relatório descrevendo as políticas Citrix em vigor para um determinado usuário e controlador. A ferramenta Resultados da Política de Grupo ajuda você a avaliar o estado atual dos GPOs em seu ambiente e gera um relatório. O relatório gerado descreve como esses objetos, incluindo as políticas Citrix, estão sendo aplicados atualmente a um usuário e controlador específicos.

Você pode iniciar o Assistente de Modelagem de Política de Grupo Citrix no Web Studio. Ou, você pode iniciar a ferramenta Resultados da Política de Grupo através do Console de Gerenciamento de Política de Grupo no Windows.

As configurações de política de site criadas usando o Web Studio não são incluídas no Conjunto Resultante de Política nos seguintes casos:

- Se você executar o Assistente de Modelagem de Política de Grupo Citrix a partir do Console de Gerenciamento de Política de Grupo
- Se você executar a ferramenta Resultados da Política de Grupo a partir do Console de Gerenciamento de Política de Grupo

Para verificar se você obtém o Conjunto Resultante de Política mais abrangente, a Citrix recomenda iniciar o assistente de Modelagem de Política de Grupo Citrix a partir do Web Studio, a menos que você crie políticas usando apenas o Console de Gerenciamento de Política de Grupo.

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 onde uma política pode não se comportar como esperado. Ao executar o Assistente de Modelagem de Política de Grupo Citrix ou a ferramenta Resultados da Política de Grupo, você pode descobrir que nenhuma política é aplicada às conexões de usuário. Em tal cenário, as configurações de política não são aplicadas aos usuários que se conectam aos seus aplicativos e desktops sob condições que correspondem aos critérios de avaliação da política. Esta situação ocorre 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 estão desabilitadas.

Se você deseja aplicar configurações de política às conexões que atendem aos critérios especificados, certifique-se de que:

- As políticas que você deseja aplicar a essas conexões estão habilitadas.
- As políticas que você deseja aplicar têm as configurações apropriadas configuradas.

Configurações de política padrão

As tabelas a seguir listam as configurações de política, seus valores padrão e as versões do Virtual Delivery Agent (VDA) às quais se aplicam.

ICA®

NOME	CONFIGURAÇÃO PADRÃO	VDA
Transporte adaptável	Desativado. Usar quando preferido	VDA 7.13–7.15; VDA 7.16 até a versão atual
Redirecionamento da área de transferência do cliente	Permitido	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Formatos permitidos para gravação na área de transferência do cliente	Nenhum formato especificado	VDA 7.6 até a versão atual
Inícios de desktop	Proibido	VDA para SO multissessão 7 até a versão atual
Número da porta do listener ICA	1494	Todas as versões de VDA
Inicialização de programas não publicados durante a conexão do cliente	Proibido	VDA para SO multi-sessão 7 até o atual
Limitar o tamanho da transferência da área de transferência do cliente para a sessão	Desabilitado	VDA 2009
Limitar o tamanho da transferência da área de transferência da sessão para o cliente	Desabilitado	VDA 2009
Modo tolerante a perdas	Permitido	VDA 2003. Observação: O modo de tolerância a perdas ainda não está disponível. Esta versão do VDA o suporta quando ele se tornar disponível.
Limites de tolerância a perdas	Quando o modo tolerante a perdas estiver disponível: Perda de pacote: 5%, Latência: 300 ms (RTT)	VDA 2003 até o atual
Protocolo Rendezvous	Desabilitado	Aplica-se apenas a sessões HDX estabelecidas via Citrix Cloud.

NOME	CONFIGURAÇÃO PADRÃO	VDA
Restringir gravação na área de transferência do cliente	Proibido	VDA 7.6 até o atual
Restringir gravação na área de transferência da sessão	Proibido	VDA 7.6 até o atual
Formatos permitidos para gravação na área de transferência da sessão	Nenhum formato especificado	VDA 7.6 até o atual
Alternância do modo tablet	Ativado	VDA 7.16 até o atual; para VDA 7.14 e 7.15 LTSR, configure esta definição usando o registro.
Lista de permissões de canal virtual	Ativado	VDA 2109 até o atual
Coleta de métricas de sessão	Permitido	7.42 até o atual

ICA/Entrega do Adobe Flash/Redirecionamento do Flash

NOME	CONFIGURAÇÃO PADRÃO	VDA
Prevenção de fallback de vídeo Flash	Não configurado	VDA 7.6 FP3 até o atual
Erro de prevenção de fallback de vídeo Flash *.swf	VDA 7.6 FP3 até o atual	

ICA/Áudio

NOME	CONFIGURAÇÃO PADRÃO	VDA
Áudio Adaptável	Ativado	Aplica-se a sessões de SO de sessão única e SO de múltiplas sessões de VDAs usando Citrix Virtual Apps and Desktops™ 2109 ou posterior.

NOME	CONFIGURAÇÃO PADRÃO	VDA
Áudio sobre transporte UDP em tempo real	Permitido	Todas as versões de VDA
Plug N Play de áudio	Permitido	VDA para SO de múltiplas sessões 7 até o atual
Qualidade do áudio	Alta - áudio de alta definição	Todas as versões de VDA
Redirecionamento de áudio do cliente	Permitido	Todas as versões de VDA
Redirecionamento de microfone do cliente	Permitido	Todas as versões de VDA
Modo tolerante a perdas para áudio	Proibido	Versões de VDA 2402 e superiores

ICA/Reconexão automática do cliente

NOME	CONFIGURAÇÃO PADRÃO	VDA
Reconexão automática do cliente	Permitido	Todas as versões de VDA
Autenticação de reconexão automática do cliente	Não exigir autenticação	Todas as versões de VDA
Registro de reconexão automática do cliente	Não registrar eventos de reconexão automática	Todas as versões de VDA
Tempo limite de reconexão automática do cliente	120 segundos	VDA 7.13 até a versão atual
Nível de transparência da interface do usuário de reconexão	80%	VDA 7.13 até a versão atual

ICA/Largura de banda

NOME	CONFIGURAÇÃO PADRÃO	VDA
Limite de largura de banda de redirecionamento de áudio	0 Kbps	Todas as versões de VDA
Porcentagem de limite de largura de banda de redirecionamento de áudio	0	Todas as versões de VDA
Limite de largura de banda de redirecionamento de dispositivo USB do cliente	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente	0	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Limite de largura de banda de redirecionamento da área de transferência	0 Kbps	Todas as versões do VDA
Porcentagem de limite de largura de banda de redirecionamento da área de transferência	0	Todas as versões do VDA
Limite de largura de banda de redirecionamento da porta COM	0 Kbps	Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta configuração usando o registro
Porcentagem de limite de largura de banda de redirecionamento de porta COM	0	Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta configuração usando o registro
Limite de largura de banda de redirecionamento de arquivo	0 Kbps	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Porcentagem de limite de largura de banda de redirecionamento de arquivo	0	Todas as versões do VDA
Limite de largura de banda da aceleração multimídia HDX MediaStream	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 e VDA para SO de sessão única 7 até o VDA atual para SO multi-sessão e VDA para SO de sessão única
Porcentagem do limite de largura de banda da aceleração multimídia HDX MediaStream	0	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Limite de largura de banda de redirecionamento de porta LPT	0 Kbps	Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro
Porcentagem de limite de largura de banda de redirecionamento de porta LPT	0	Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta definição usando o registro
Limite geral de largura de banda da sessão	0 Kbps	Todas as versões do VDA
Limite de largura de banda de redirecionamento de impressora	0 Kbps	Todas as versões do VDA
Porcentagem de limite de largura de banda de redirecionamento de impressora	0	Todas as versões do VDA
Limite de largura de banda para redirecionamento de dispositivo TWAIN	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7

NOME	CONFIGURAÇÃO PADRÃO	VDA
		até o atual, VDA para SO de sessão única 7 até o atual
Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN	0	VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Redirecionamento de conteúdo bidirecional

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir redirecionamento de conteúdo bidirecional	Proibido	VDA 7.13 até o atual
URLs permitidas para serem redirecionadas para o cliente	vazio	VDA 7.13 até o atual
URLs permitidas para serem redirecionadas para o VDA	vazio	VDA 7.13 até o atual
Configuração de redirecionamento de conteúdo bidirecional	Desabilitado	VDA 2311 até o atual

ICA/Redirecionamento de conteúdo do navegador

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de conteúdo do navegador	Permitido	VDA 7.16 até o atual
Configuração de ACL de redirecionamento de conteúdo do navegador	`https://www.youtube.com/*`	VDA 7.16 até o atual
Suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador	Proibido	VDA 2106 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Configuração de proxy de redirecionamento de conteúdo do navegador	vazio	VDA 7.16 até o atual
Autenticação de proxy web de busca do servidor de redirecionamento de conteúdo do navegador	Proibido	VDA 2012 até o atual

Sensores ICA/Cliente

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir que aplicativos usem a localização física do dispositivo cliente	Proibido	VDA 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/IU da Área de Trabalho

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de Composição da Área de Trabalho	Desabilitado (7.6 FP3 até o atual); Habilitado (5.6 até 7.6 FP2)	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Qualidade gráfica do redirecionamento de composição da área de trabalho	Médio	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Papel de parede da área de trabalho	Permitido	Todas as versões do VDA
Animação de menu	Permitido	Todas as versões do VDA
Visualizar conteúdo da janela ao arrastar	Permitido	Todas as versões de VDA

ICA/Monitoramento do usuário final

NOME	CONFIGURAÇÃO PADRÃO	VDA
Cálculo de ida e volta do ICA	Ativado	Todas as versões de VDA
Intervalo de cálculo de ida e volta do ICA	15 segundos	Todas as versões de VDA
Cálculos de ida e volta do ICA para conexões ociosas	Desabilitado	Todas as versões de VDA

ICA/Experiência de área de trabalho aprimorada

NOME	CONFIGURAÇÃO PADRÃO	VDA
Experiência de Área de Trabalho Aprimorada	Permitido	VDA para SO multissessão 7 até o atual

Redirecionamento de ICA/Arquivo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conectar automaticamente unidades de cliente	Permitido	Todas as versões de VDA
Redirecionamento de unidade de cliente	Permitido	Todas as versões de VDA
Unidades fixas de cliente	Permitido	Todas as versões de VDA
Unidades de disquete de cliente	Permitido	Todas as versões de VDA
Unidades de rede de cliente	Permitido	Todas as versões de VDA
Unidades ópticas do cliente	Permitido	Todas as versões de VDA
Unidades removíveis do cliente	Permitido	Todas as versões de VDA
Redirecionamento do host para o cliente	Desabilitado	VDA para SO multissessão 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Preservar letras de unidade do cliente	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Acesso somente leitura à unidade do cliente	Desabilitado	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento de pasta especial	Permitido	Somente implantações do Web Interface; VDA para SO multi-sessão 7 até o atual
Usar gravações assíncronas	Desabilitado	Todas as versões de VDA

ICA/Gráficos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir compactação visualmente sem perdas	Desabilitado	VDA 7.6 até o atual
Limite de memória de exibição	65.536 Kb	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Preferência de degradação do modo de exibição	Degradar profundidade de cor primeiro	Todas as versões de VDA
Visualização dinâmica de janelas	Ativado	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Indicador de status gráfico	Desabilitado	VDA 7.16 até o atual
Cache de imagem	Ativado	VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Modo gráfico legado	Desabilitado	VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual
Profundidade máxima de cor permitida	32 bits por pixel	Todas as versões do VDA
Notificar usuário quando o modo de exibição for degradado	Desabilitado	VDA para SO de múltiplas sessões 7 até o atual
Otimizar para carga de trabalho de gráficos 3D	Desabilitado	VDA 7.17 até o atual
Enfileiramento e descarte	Ativado	Todas as versões do VDA
Compartilhamento de tela	Desabilitado	VDA 2112
Usar codec de vídeo para compressão	Usar codec de vídeo quando preferencial	VDA 7.6 FP3 até o atual
Usar codificação de hardware para codec de vídeo	Ativado	VDA 7.11 até o atual

ICA/Gráficos/Cache

NOME	CONFIGURAÇÃO PADRÃO	VDA
Limite de cache persistente	3.000.000 bps	VDA para SO multissessão 7 até o atual

ICA/Gráficos/Framehawk

NOME	CONFIGURAÇÃO PADRÃO	VDA
Canal de exibição Framehawk	Desabilitado	VDA 7.6 FP2 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Intervalo de portas do canal de exibição Framehawk	3224,3324	VDA 7.6 FP2 até o atual

ICA/Manter ativo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Tempo limite de keep alive do ICA	60 segundos	Todas as versões VDA
Keep alives do ICA	Não enviar mensagens de keep alive do ICA	Todas as versões VDA

ICA/Teclado e IME

NOME	CONFIGURAÇÃO PADRÃO	VDA
Sincronização de Layout de Teclado do Cliente e Melhoria de IME	Desabilitado	Aplica-se apenas ao 1912 LTSR CU2 e posterior.
Habilitar Mapeamento de Layout de Teclado Unicode	Permitido (2407 até o atual); Proibido (versões anteriores)	Aplica-se apenas ao 1912 LTSR CU2 e posterior.
Ocultar Caixa de Mensagem Pop-up de Troca de Layout de Teclado	Proibido	Aplica-se apenas ao 1912 LTSR CU2 e posterior.

ICA/Acesso a Aplicativos Locais

NOME	CONFIGURAÇÃO PADRÃO	VDA
Permitir Acesso a Aplicativos Locais	Proibido	VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual
Lista de bloqueio de redirecionamento de URL	Nenhum site especificado	VDA para SO de múltiplas sessões 7 até o atual, VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
		para SO de sessão única 7 até o atual
Lista de permissão de redirecionamento de URL	Nenhum site especificado	VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Experiência móvel

NOME	CONFIGURAÇÃO PADRÃO	VDA
Exibição automática do teclado	Proibido	VDA 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual
Iniciar área de trabalho otimizada para toque	Permitido	VDA 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual. Esta configuração está desabilitada e não disponível para máquinas Windows 10 e Windows Server 2016.
Remover a caixa de combinação	Proibido	VDA 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Multimídia

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de vídeo HTML5	Proibido	VDA 7.12 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Limitar qualidade de vídeo	Não configurado	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento do Microsoft Teams	Permitido	VDA para SO multi-sessão 1906 até o atual, VDA para SO de sessão única 1906 até o atual.
Conferência multimídia	Permitido	Todas as versões de VDA
Otimização para redirecionamento multimídia do Windows Media via WAN	Permitido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Usar GPU para otimizar o redirecionamento multimídia do Windows Media via WAN	Proibido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Prevenção de fallback do Windows Media	Não configurado	VDA 7.6 FP3 até o atual
Busca de conteúdo do lado do cliente do Windows Media	Permitido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Redirecionamento do Windows Media	Permitido	Todas as versões de VDA
Tamanho do buffer de redirecionamento do Windows Media	5 segundos	VDA 5, 5.5, 5.6 FP1 até o atual
Uso do tamanho do buffer de redirecionamento do Windows Media	Desabilitado	VDA 5, 5.5, 5.6 FP1 até o atual

Conexões ICA/Multi-Stream

NOME	CONFIGURAÇÃO PADRÃO	VDA
Áudio sobre UDP	Permitido	VDA para SO multi-sessão 7 até o atual
Intervalo de portas UDP de áudio	16500, 16509	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Política Multi-Porta	A porta primária (2598) tem alta prioridade	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Configuração de computador Multi-Stream	Desabilitado	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Configuração de usuário Multi-Stream	Desabilitado	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Configuração de atribuição de fluxo de canal virtual Multi-Stream	Consulte Configuração de atribuição de canal virtual Multi-Stream para atribuições de fluxo padrão	VDA 2003

ICA/Redirecionamento de Porta

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conectar automaticamente portas COM do cliente	Desabilitado	Todas as versões do VDA; para VDA 7.0 a 7.8, configure esta configuração usando o registro
Conectar automaticamente portas LPT do cliente	Desabilitado	Todas as versões do VDA; para VDA 7.0 a 7.8, configure

NOME	CONFIGURAÇÃO PADRÃO	VDA
		esta configuração usando o registro
Redirecionamento de porta COM do cliente	Proibido	Todas as versões VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo
Redirecionamento da porta LPT do cliente	Proibido	Todas as versões VDA; para VDA 7.0 a 7.8, configure esta definição usando o registo

ICA/Impressão

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de impressora do cliente	Permitido	Todas as versões VDA
Impressora predefinida	Definir a impressora predefinida como a impressora principal do cliente	Todas as versões VDA
Atribuições de impressora	A impressora atual do utilizador é usada como impressora predefinida para a sessão	Todas as versões VDA
Preferência de registo de eventos de criação automática de impressora	Registrar erros e avisos	Todas as versões de VDA
Impressoras de sessão	Nenhuma impressora especificada	Todas as versões de VDA
Aguardar a criação de impressoras (desktop)	Desabilitado	Todas as versões de VDA

ICA/Impressão/Impressoras Cliente

NOME	CONFIGURAÇÃO PADRÃO	VDA
Criar automaticamente impressoras cliente	Criar automaticamente todas as impressoras cliente	Todas as versões de VDA
Criar automaticamente impressora universal genérica	Desabilitado	Todas as versões de VDA
Nomes de impressoras cliente	Nomes de impressoras padrão	VDA 5.6
Conexões diretas a servidores de impressão	Ativado	Todas as versões de VDA
Mapeamento e compatibilidade de driver de impressora	Nenhuma regra é especificada	Todas as versões de VDA
Retenção de propriedades da impressora	Mantido no perfil somente se não salvo no cliente	Todas as versões de VDA
Impressoras cliente retidas e restauradas	Permitido	VDA 5, 5,5, 5.6 FP1

ICA/Impressão/Drivers

NOME	CONFIGURAÇÃO PADRÃO	VDA
Instalação automática de drivers de impressora embutidos	Ativado	Todas as versões de VDA
Preferência de driver universal	EMF; XPS; PCL5c; PCL4; PS	Todas as versões do VDA
Uso do driver de impressão universal	Usar impressão universal somente se o driver solicitado não estiver disponível	Todas as versões do VDA

ICA/Impressão/Servidor de Impressão Universal

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar Servidor de Impressão Universal	Desabilitado	Todas as versões do VDA
Porta do fluxo de dados de impressão (CGP) do Servidor de Impressão Universal	7229	Todas as versões do VDA
Limite de largura de banda de entrada do fluxo de impressão (kbps) do Servidor de Impressão Universal	0	Todas as versões do VDA
Porta do serviço web (HTTP/SOAP) do Servidor de Impressão Universal	8080	Todas as versões de VDA
Servidores de Impressão Universal para balanceamento de carga	Versões de VDA 7.9 até a atual	
Limite de servidor de impressão universal fora de serviço	180 (segundos)	Versões de VDA 7.9 até a atual

ICA/Impressão/Impressão Universal

NOME	CONFIGURAÇÃO PADRÃO	VDA
Modo de processamento EMF de impressão universal	Enviar diretamente para a impressora	Todas as versões de VDA
Limite de compactação de imagem de impressão universal	Melhor qualidade (compressão sem perdas)	Todas as versões de VDA
Padrões de otimização de impressão universal	Compressão de Imagem: Qualidade de imagem desejada = Qualidade padrão, Habilitar compressão	Todas as versões de VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
	pesada = Falso; Cache de Imagens e Fontes: Permitir cache de imagens incorporadas = Verdadeiro; Permitir que não administradores modifiquem essas configurações = Falso;	
Preferência de visualização de impressão universal	Não usar visualização de impressão para impressoras universais genéricas ou criadas automaticamente	Todas as versões de VDA
Limite de qualidade de impressão universal	Sem limite	Todas as versões de VDA

ICA/Segurança

NOME	CONFIGURAÇÃO PADRÃO	VDA
Nível mínimo de criptografia SecureICA	Básico	VDA para SO multi-sessão 7 até o atual

ICA/Limites do Servidor

NOME	CONFIGURAÇÃO PADRÃO	VDA
Intervalo do temporizador de inatividade do servidor	0 milissegundos	VDA para SO multi-sessão 7 até o atual

Limites de ICA/Sessão

NOME	CONFIGURAÇÃO PADRÃO	VDA
Temporizador de sessão desconectada	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Temporizador de sessão desconectada do Acesso Remoto ao PC	Desabilitado	VDA para SO de sessão única 7 até o atual
Intervalo do temporizador de sessão desconectada	1.440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Temporizador de conexão de sessão	Desabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Intervalo do temporizador de conexão de sessão	1.440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Temporizador de inatividade da sessão	Ativado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual
Intervalo do temporizador de inatividade da sessão	1.440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sessão única 7 até o atual

ICA/Confiabilidade da Sessão

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conexões de confiabilidade da sessão	Permitido	Todas as versões do VDA
Número da porta de confiabilidade da sessão	2598	Todas as versões do VDA
Tempo limite de confiabilidade da sessão	180 segundos	Todas as versões do VDA

ICA/Controle de Fuso Horário

NOME	CONFIGURAÇÃO PADRÃO	VDA
Estimar hora local para clientes legados	Ativado	VDA para SO multi-sessão 7 até o atual
Restaurar fuso horário do SO de sessão única na desconexão ou logoff da sessão	Ativado	Versão atual do VDA
Usar hora local do cliente	Usar fuso horário do servidor	Todas as versões do VDA

Dispositivos ICA/TWAIN

NOME	CONFIGURAÇÃO PADRÃO	VDA
Redirecionamento de dispositivo TWAIN do cliente	Permitido	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Nível de compactação TWAIN	Médio	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

Dispositivos ICA/USB

NOME	CONFIGURAÇÃO PADRÃO	VDA
Regras de otimização de dispositivo USB do cliente	Ativado (VDA 7.6 FP3 até o atual); Desativado (VDA 7.11 até o atual); Por padrão, nenhuma regra é especificada	VDA 7.6 FP3 até o atual
Redirecionamento de dispositivo USB do cliente	Proibido	Todas as versões do VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Regras de redirecionamento de dispositivo USB do cliente	Nenhuma regra é especificada	Todas as versões do VDA
Redirecionamento de dispositivo USB Plug and Play do cliente	Permitido	VDA para SO multiusuário 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Exibição Visual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Profundidade de cor preferida para gráficos simples	24 bits por pixel	VDA 7.6 FP3 até o atual
Taxa de quadros alvo	30 quadros por segundo	Todas as versões de VDA
Qualidade visual	Médio	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

ICA/Exibição Visual/Imagens em Movimento

NOME	CONFIGURAÇÃO PADRÃO	VDA
Qualidade mínima da imagem	Normal	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Compressão de imagem em movimento	Ativado	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Nível de compressão progressiva	Nenhum	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Valor limite de compressão progressiva	2.147.483.647 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Taxa de quadros mínima alvo	10 quadros por segundo	VDA 5.5, 5.6 FP1, VDA para SO de múltiplas sessões 7 até o atual, VDA para SO de sessão única 7 até o atual

Observação:

A política de **Taxa de quadros mínima alvo** foi descontinuada.

ICA/Exibição Visual/Imagens Estáticas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Compressão de cor adicional	Desabilitado	Todas as versões de VDA
Limite de compressão de cor adicional	8.192 Kbps	Todas as versões de VDA
Compressão pesada	Desabilitado	Todas as versões de VDA
Nível de compressão com perdas	Médio	Todas as versões de VDA
Valor limite de compressão com perdas	2,147,483,647 Kbps	Todas as versões de VDA

ICA/WebSockets

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conexões WebSockets	Proibido	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Número da porta WebSockets	8008	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Lista de servidores de origem confiáveis do WebSockets	O curinga, *, é usado para confiar em todos os URLs do Receiver for Web	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

Gerenciamento de Carga

NOME	CONFIGURAÇÃO PADRÃO	VDA
Tolerância de logon simultâneo	2	VDA para SO multi-sessão 7 até o atual
Uso da CPU	Desabilitado	VDA para SO de Múltiplas Sessões 7 até o atual
Prioridade de processo excluída do uso da CPU	Abaixo do Normal ou Baixo	VDA para SO de Múltiplas Sessões 7 até o atual
Uso de disco	Desabilitado	VDA para SO de Múltiplas Sessões 7 até o atual
Número máximo de sessões	250	VDA para SO de Múltiplas Sessões 7 até o atual
Uso de memória	Desabilitado	VDA para SO de Múltiplas Sessões 7 até o atual
Carga base de uso de memória	Carga zero: 768 MB	VDA para SO de Múltiplas Sessões 7 até o atual

Gerenciamento de Perfil/Configurações avançadas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Desabilitar configuração automática	Desabilitado	Todas as versões de VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Fazer logoff do usuário se um problema for encontrado	Desabilitado	Todas as versões de VDA
Número de tentativas ao acessar arquivos bloqueados	5	Todas as versões de VDA
Processar arquivos de cookie da Internet no logoff	Desabilitado	Todas as versões de VDA

Gerenciamento de Perfil/Configurações básicas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Gravação ativa	Desabilitado	Todas as versões de VDA
Habilitar Gerenciamento de Perfil	Desabilitado	Todas as versões de VDA
Grupos excluídos	Desabilitado. Membros de todos os grupos de usuários são processados.	Todas as versões de VDA
Suporte a perfil offline	Desabilitado	Todas as versões de VDA
Caminho para o armazenamento do usuário	Windows	Todas as versões de VDA
Processar logons de administradores locais	Desabilitado	Todas as versões de VDA
Grupos processados	Desativado. Membros de todos os grupos de usuários são processados.	Todas as versões de VDA

Gerenciamento de Perfil/Configurações de Plataforma Cruzada

NOME	CONFIGURAÇÃO PADRÃO	VDA
Grupos de usuários de configurações de plataforma cruzada	Desativado. Todos os grupos de usuários especificados em Grupos processados são processados	Todas as versões de VDA
Habilitar configurações de plataforma cruzada	Desabilitado	Todas as versões de VDA
Caminho para definições de plataforma cruzada	Desativado. Nenhum caminho é especificado.	Todas as versões de VDA
Caminho para o armazenamento de configurações multiplataforma	Desativado. Windows\PM_CM é usado.	Todas as versões de VDA
Fonte para criar configurações multiplataforma	Desabilitado	Todas as versões de VDA

Gerenciamento de Perfil/Sistema de Arquivos/Exclusões

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de exclusão - diretórios	Desativado. Todas as pastas no perfil do usuário são sincronizadas.	Todas as versões de VDA
Lista de exclusão - arquivos	Desativado. Todos os arquivos no perfil do usuário são sincronizados.	Todas as versões de VDA

Gerenciamento de Perfil/Sistema de Arquivos/Sincronização

NOME	CONFIGURAÇÃO PADRÃO	VDA
Diretórios para sincronizar	Desativado. Apenas pastas não excluídas são sincronizadas.	Todas as versões VDA
Arquivos para sincronizar	Desativado. Apenas arquivos não excluídos são sincronizados.	Todas as versões VDA
Pastas para espelhar	Desativado. Nenhuma pasta é espelhada.	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta

NOME	CONFIGURAÇÃO PADRÃO	VDA
Conceder acesso de administrador	Desabilitado	Todas as versões VDA
Incluir nome de domínio	Desabilitado	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/AppData(Roaming)

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do AppData(Roaming)	Desabilitado. Nenhuma localização é especificada.	Todas as versões VDA
Configurações de redirecionamento para AppData(Roaming)	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho do AppData(Roaming)	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Contatos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Contatos	Desabilitado. Nenhuma localização é especificada.	Todas as versões VDA
Configurações de redirecionamento para Contatos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Contatos**	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Área de Trabalho

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho da Área de Trabalho	Desativado. Nenhuma localização é especificada.	Todas as versões VDA
Configurações de redirecionamento para Desktop	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho da Área de Trabalho**	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Documentos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Documentos	Desativado. Nenhuma localização é especificada.	Todas as versões VDA
Configurações de redirecionamento para Documentos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho dos Documentos**	Todas as versões VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Downloads

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Downloads	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Downloads	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Downloads**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Favoritos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Favoritos	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Favoritos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Favoritos**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Links

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho dos Links	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Links	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Links**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Música

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho da Música	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Música	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Música**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Imagens

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho das Imagens	Desativado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Imagens	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Imagens**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Jogos Salvos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho de Jogos Salvos	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Jogos Salvos	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Jogos Salvos**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Pesquisas

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho de Pesquisas	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Pesquisas	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Pesquisas**	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Menu Iniciar

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do Menu Iniciar	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para o Menu Iniciar	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da política de caminho do Menu Iniciar	Todas as versões de VDA

Gerenciamento de Perfil/Redirecionamento de Pasta/Vídeo

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do Vídeo	Desabilitado. Nenhuma localização é especificada.	Todas as versões de VDA
Configurações de redirecionamento para Vídeo	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho do Vídeo**	Todas as versões de VDA

Configurações de Gerenciamento de Perfil/Log

NOME	CONFIGURAÇÃO PADRÃO	VDA
Ações do Active Directory	Desabilitado	Todas as versões de VDA
Informações comuns	Desabilitado	Todas as versões de VDA
Avisos comuns	Desabilitado	Todas as versões de VDA
Habilitar registro em log	Desabilitado	Todas as versões de VDA
Ações do sistema de arquivos	Desabilitado	Todas as versões de VDA
Notificações do sistema de arquivos	Desabilitado	Todas as versões de VDA
Logoff	Desabilitado	Todas as versões de VDA
Logon	Desabilitado	Todas as versões de VDA
Tamanho máximo do arquivo de log	1048576	Todas as versões de VDA
Caminho para o arquivo de log	Desabilitado. Os arquivos de log são salvos no local padrão; %SystemRoot% \System32\Logfiles\UserProfileManager.	Todas as versões de VDA
Informações personalizadas do usuário	Desabilitado	Todas as versões de VDA
Valores da política no logon e logoff	Desabilitado	Todas as versões de VDA
Ações do Registro	Desabilitado	Todas as versões de VDA
Diferenças do Registro no logoff	Desabilitado	Todas as versões de VDA

Gerenciamento de perfil/Manipulação de perfil

NOME	CONFIGURAÇÃO PADRÃO	VDA
Atraso antes de excluir perfis em cache	0	Todas as versões de VDA
Excluir perfis armazenados em cache localmente no logoff	Desabilitado	Todas as versões de VDA
Tratamento de conflitos de perfil local	Usar perfil local	Todas as versões de VDA
Migração de perfis existentes	Local e roaming	Todas as versões de VDA
Caminho para o perfil de modelo	Desabilitado. Novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.	Todas as versões de VDA
O perfil de modelo substitui o perfil local	Desabilitado	Todas as versões de VDA
O perfil de modelo substitui o perfil de roaming	Desabilitado	Todas as versões de VDA
Perfil de modelo usado como um perfil obrigatório Citrix® para todos os logons	Desabilitado	Todas as versões de VDA

Gerenciamento de Perfil/Registro

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de exclusão	Desativado. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff.	Todas as versões de VDA

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de inclusão	Desativado. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff.	Todas as versões de VDA

Gerenciamento de Perfil/Perfis de usuário transmitidos

NOME	CONFIGURAÇÃO PADRÃO	VDA
Sempre armazenar em cache	Desabilitado	Todas as versões de VDA
Tamanho do cache sempre	0 Mb	Todas as versões de VDA
Streaming de perfil	Desabilitado	Todas as versões de VDA
Grupos de perfil de usuário transmitidos	Desabilitado. Todos os perfis de usuário dentro de uma OU são processados normalmente.	Todas as versões de VDA
Tempo limite para arquivos de bloqueio de área pendentes (dias)	1 dia	Todas as versões de VDA

Receiver

NOME	CONFIGURAÇÃO PADRÃO	VDA
Lista de contas do StoreFront™	Nenhuma loja especificada	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual

Camada de personalização do usuário

NOME	CONFIGURAÇÃO PADRÃO	VDA
Caminho do Repositório da Camada de Usuário	Desabilitado. Nenhum caminho especificado.	VDA 19.12 e versões posteriores

NOME	CONFIGURAÇÃO PADRÃO	VDA
Tamanho da Camada de Usuário em GB	10 GB. Uma camada de usuário é um disco de provisionamento dinâmico que se expande até o tamanho definido. As camadas de usuário nunca diminuem de tamanho.	VDA 19.12 ou versões posteriores

Agente de Entrega Virtual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Máscara de rede IPv6 de registro do Controller	Nenhuma máscara de rede é especificada	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Porta de registro do Controller	80	Todas as versões do VDA
SIDs do Controller	Nenhum SID é especificado	Todas as versões de VDA
Controladores	Nenhum controlador é especificado	Todas as versões de VDA
Habilitar atualização automática de controladores	Ativado	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
Usar apenas registro de controlador IPv6	Desabilitado	VDA para SO multi-sessão 7 até o atual, VDA para SO de sessão única 7 até o atual
GUID do Site	Nenhum GUID é especificado	Todas as versões de VDA

Virtual Delivery Agent/HDX 3D Pro

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar sem perdas	Ativado	VDA 5.5, 5.6 FP1

NOME	CONFIGURAÇÃO PADRÃO	VDA
Configurações de qualidade do HDX 3D Pro	VDA 5.5, 5.6 FP1	

Virtual Delivery Agent/Monitoramento

NOME	CONFIGURAÇÃO PADRÃO	VDA
Habilitar monitoramento de processo	Desabilitado	VDA 7.11 até o atual
Habilitar monitoramento de recursos	Ativado	VDA 7.11 até o atual

IP virtual

NOME	CONFIGURAÇÃO PADRÃO	VDA
Suporte a loopback de IP Virtual	Desabilitado	VDA 7.6 até o atual
Lista de programas de loopback virtual de IP Virtual	Nenhum	VDA 7.6 até o atual

Referência de configurações de política

As políticas incluem configurações que são aplicadas quando a política é imposta. As descrições nesta seção também indicam se mais configurações são necessárias para habilitar um recurso ou se são semelhantes a uma configuração.

Referência rápida

As tabelas a seguir listam as configurações que você pode configurar em uma política. Encontre a tarefa que você deseja concluir na coluna da esquerda e, em seguida, localize a configuração correspondente na coluna da direita.

Uma lista completa de todas as configurações de política está disponível nos formatos .CHM (HTML Compilado) e .CSV. Esses arquivos estão disponíveis na pasta `\program files\citrix\grouppolicy` no servidor onde o broker (controlador de entrega) está instalado. Você também pode baixar a versão mais recente das configurações de política clicando aqui.

Áudio

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar se o uso de vários dispositivos de áudio é permitido	Plug N Play de áudio
Controlar se a entrada de áudio de microfones no dispositivo do usuário é permitida	Redirecionamento de microfone do cliente
Controlar a qualidade do áudio no dispositivo do usuário	Qualidade do áudio
Controlar o mapeamento de áudio para alto-falantes no dispositivo do usuário	Redirecionamento de áudio do cliente

Largura de banda para dispositivos de usuário

PARA LIMITAR A LARGURA DE BANDA USADA PARA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Mapeamento de áudio do cliente	Limite de largura de banda de redirecionamento de áudio ou porcentagem do limite de largura de banda de redirecionamento de áudio
Recortar e colar usando uma área de transferência local	Limite de largura de banda de redirecionamento da área de transferência ou porcentagem do limite de largura de banda de redirecionamento da área de transferência
Acesso em uma sessão a unidades de cliente locais	Limite de largura de banda de redirecionamento de arquivo ou porcentagem do limite de largura de banda de redirecionamento de arquivo
Aceleração Multimídia HDX™ MediaStream	Limite de largura de banda da Aceleração Multimídia HDX MediaStream ou porcentagem do limite de largura de banda da Aceleração Multimídia HDX MediaStream
Sessão do cliente	Limite geral de largura de banda da sessão

PARA LIMITAR A LARGURA DE BANDA USADA PARA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Impressão	Limite de largura de banda de redirecionamento de impressora ou porcentagem do limite de largura de banda de redirecionamento de impressora
Dispositivos TWAIN (como uma câmera ou scanner)	Limite de largura de banda de redirecionamento de dispositivo TWAIN ou porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN
Dispositivos USB	Limite de largura de banda de redirecionamento de dispositivo USB do cliente ou porcentagem do limite de largura de banda de redirecionamento de dispositivo USB do cliente

Redirecionamento de unidades de cliente e dispositivos de usuário

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se as unidades no dispositivo do usuário são conectadas quando os usuários fazem logon no servidor ou não	Conectar automaticamente unidades cliente
Controla a transferência de dados de recortar e colar entre o servidor e a área de transferência local	Redirecionamento da área de transferência do cliente
Controla como as unidades são mapeadas do dispositivo do usuário	Redirecionamento de unidade cliente
Controla se os discos rígidos locais dos usuários estão disponíveis em uma sessão	Unidades fixas do cliente e redirecionamento de unidade cliente
Controla se as unidades de disquete locais dos usuários estão disponíveis em uma sessão	Unidades de disquete do cliente e redirecionamento de unidade cliente
Controla se as unidades de rede dos usuários estão disponíveis em uma sessão	Unidades de rede do cliente e redirecionamento de unidade cliente

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se as unidades de CD, DVD ou Blu-ray locais dos usuários estão disponíveis em uma sessão	Unidades ópticas do cliente e Redirecionamento de unidade do cliente
Controla se as unidades removíveis locais dos usuários estão disponíveis em uma sessão	Unidades removíveis do cliente e Redirecionamento de unidade do cliente
Controla se os dispositivos TWAIN dos usuários, como scanners e câmeras, estão disponíveis em uma sessão e controla a compactação das transferências de dados de imagem	Redirecionamento de dispositivo TWAIN do cliente; Redirecionamento de compactação TWAIN
Controla se os dispositivos USB estão disponíveis em uma sessão	Redirecionamento de dispositivo USB do cliente e Regras de redirecionamento de dispositivo USB do cliente
Melhora a velocidade de gravação e cópia de arquivos para um disco cliente em uma WAN	Usar gravações assíncronas

Redirecionamento de conteúdo

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controla se deve usar o redirecionamento de conteúdo do servidor para o dispositivo do usuário	Redirecionamento do host para o cliente

UI da Área de Trabalho

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar se o papel de parede da área de trabalho é usado nas sessões dos usuários ou não	Papel de parede da área de trabalho
Visualizar o conteúdo da janela enquanto uma janela é arrastada	Visualizar o conteúdo da janela ao arrastar

Gráficos e multimídia

Importante:

A política do Flash permanece apenas para permitir que clientes com VDAs mais antigos usem controladores mais recentes (por exemplo, controladores da versão 1912) e ainda usem o Flash. Esta versão do VDA não oferece suporte ao Flash.

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar o número máximo de quadros por segundo enviados para dispositivos de usuário a partir de desktops virtuais	Taxa de quadros de destino
Controlar a qualidade visual das imagens exibidas no dispositivo do usuário	Qualidade visual
Controlar se os sites podem exibir conteúdo Flash quando acessados em sessões	Lista de URLs de busca de conteúdo do lado do servidor Flash; Lista de compatibilidade de URLs Flash; Configuração de política de prevenção de fallback de vídeo Flash; Erro de prevenção de fallback de vídeo Flash *.swf
Controlar a compactação de vídeo renderizado no servidor	Usar codec de vídeo para compactação; Usar codificação de hardware para codec de vídeo
Controlar a entrega de conteúdo web multimídia HTML5 aos usuários	Redirecionamento de vídeo HTML5

Priorizar o tráfego de rede Multi-Stream

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Especificar portas para tráfego ICA® em várias conexões e estabelecer prioridades de rede	Política Multi-Porta

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Habilitar suporte para conexões multi-stream entre servidores e dispositivos de usuário	Multi-Stream (configurações de computador e usuário)

Imprimir

PARA ESTA TAREFA	USE ESTA CONFIGURAÇÃO DE POLÍTICA
Controlar a criação de impressoras cliente no dispositivo do usuário	Criar automaticamente impressoras cliente e Redirecionamento de impressora cliente
Controlar o local onde as propriedades da impressora são armazenadas	Retenção de propriedades da impressora
Controlar se o cliente ou o servidor processa as solicitações de impressão	Conexões diretas a servidores de impressão
Controlar se os usuários podem acessar impressoras conectadas aos seus dispositivos de usuário	Redirecionamento de impressora cliente
Controlar a instalação de drivers nativos do Windows ao criar automaticamente impressoras cliente e de rede	Instalação automática de drivers de impressora incluídos
Controlar quando usar o Driver de Impressora Universal	Uso do driver de impressão universal
Escolher uma impressora com base nas informações da sessão de usuário em roaming	Impressora padrão
Balancear carga e definir limite de failover para Servidores de Impressão Universal	Servidores de Impressão Universal para balanceamento de carga; limite de fora de serviço dos Servidores de Impressão Universal

Observação:

As políticas não podem ser usadas para habilitar um protetor de tela em uma sessão de área de trabalho ou aplicativo. Para usuários que exigem protetores de tela, o protetor de tela pode ser implementado no dispositivo do usuário.

Configurações de política ICA®

Observação:

Esta página fornece descrições e valores de configuração suportados para as configurações de política ICA. Para obter mais informações sobre como trabalhar com políticas, consulte a seção Trabalhar com políticas.

Transporte adaptável

Esta configuração permite ou impede o transporte de dados via EDT como primário e via TCP como fallback.

Por padrão, o transporte adaptável está ativado (**Preferencial**), e o EDT é usado quando possível, com fallback para TCP. Você pode alterar sua configuração conforme necessário:

- **Preferencial**. O transporte adaptável via EDT é usado quando possível, com fallback para TCP.
- **Modo de diagnóstico**. O EDT é forçado e o fallback para TCP é desativado. Recomendamos esta configuração apenas para solução de problemas.
- **Desativado**. O TCP é forçado e o EDT é desativado.

Para obter mais informações, consulte Transporte adaptável.

Configuração de arrastar e soltar

Esta configuração permite ou impede o arrastar e soltar de arquivos entre o cliente e aplicativos ou desktops virtuais. Por padrão, a política de arrastar e soltar está desativada. Você pode ativar esta política se necessário.

Tempo limite de espera para inicialização de aplicativo

Esta configuração especifica o valor do tempo limite de espera em milissegundos para que uma sessão aguarde o início do primeiro aplicativo. Se o início do aplicativo exceder este período de tempo, a sessão é encerrada.

Você pode escolher o tempo padrão (10.000 milissegundos) ou especificar um número em milissegundos.

Redirecionamento da área de transferência do cliente

Esta configuração permite ou impede que a área de transferência no dispositivo do usuário seja mapeada para a área de transferência no servidor.

Por padrão, o redirecionamento da área de transferência é permitido.

Para evitar a transferência de dados de copiar e colar entre uma sessão e a área de transferência local, selecione **Proibir**. Os usuários ainda podem copiar e colar dados entre aplicativos em execução nas sessões.

Depois de permitir esta configuração, configure a largura de banda máxima permitida que a área de transferência pode consumir em uma conexão de cliente. Use as configurações **Limite de largura de banda de redirecionamento da área de transferência** ou **Porcentagem do limite de largura de banda de redirecionamento da área de transferência**.

Formatos permitidos para gravação na área de transferência do cliente

Quando a configuração **Restringir gravação na área de transferência do cliente** está **Habilitada**, os dados da área de transferência do host não podem ser compartilhados com o endpoint do cliente. Você pode usar esta configuração para permitir que formatos de dados específicos sejam compartilhados com a área de transferência do endpoint do cliente. Para usar esta configuração, habilite-a e adicione os formatos específicos a serem permitidos.

Os seguintes formatos de área de transferência são definidos pelo sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE

- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Os seguintes formatos personalizados são predefinidos em XenApp e XenDesktop e Citrix Virtual Apps and Desktops™:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

O formato HTML está desabilitado por padrão. Para habilitar este recurso:

- Verifique se **Redirecionamento da área de transferência do cliente** está definido como **Permitido**.
- Verifique se **Restringir gravação da área de transferência do cliente** está definido como **Habilitado**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja que sejam suportados) em **Formatos permitidos para gravação da área de transferência do cliente**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos a serem registrados no sistema. Os nomes dos formatos diferenciam maiúsculas de minúsculas.

Essa configuração não se aplica se a política **Redirecionamento da área de transferência do cliente** estiver definida como **Proibido** ou se a política **Restringir gravação da área de transferência do cliente** estiver definida como **Desabilitado**.

> **Observação:**
>
> Habilitar o suporte à cópia da área de transferência no formato HTML (CF_HTML) copia quaisquer scripts da origem do conteúdo copiado para o destino. Verifique se você confia na origem antes de prosseguir com a cópia. Se você copiar conteúdo contendo scripts, eles estarão ativos somente se você salvar o arquivo de destino como um arquivo HTML e executá-lo.

Limitar o tamanho da transferência da área de transferência do cliente para a sessão

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de um endpoint cliente para uma sessão virtual durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, habilite a configuração **Limitar o tamanho da transferência da área de transferência do cliente para a sessão**. Em seguida, no campo **Limite de Tamanho**, insira um valor em kilobytes para definir o tamanho da transferência de dados entre a área de transferência local e uma sessão.

Por padrão, esta configuração está desabilitada e não há limite para transferências do cliente para a sessão.

HDX™ Direct

O HDX Direct permite que o cliente estabeleça automaticamente uma conexão direta com o host da sessão quando a comunicação direta estiver disponível. As conexões são estabelecidas de forma segura usando criptografia em nível de rede.

Modo HDX Direct

O HDX Direct pode ser usado para estabelecer conexões diretas com hosts de sessão para clientes internos e externos. Essa configuração determina se o HDX Direct está disponível apenas para clientes internos ou para clientes internos e externos.

Quando definido como **Somente interno**, o HDX Direct tenta estabelecer conexões diretas apenas para clientes na rede interna.

Quando definido como **Interno** e **externo**, o HDX Direct tenta estabelecer conexões diretas para clientes internos e externos.

Por padrão, o HDX Direct é configurado apenas para clientes internos.

Intervalo de portas do HDX Direct

O intervalo de portas que são usadas pelo HDX Direct para conexões de usuários externos. Por padrão, o HDX Direct usa o intervalo de portas: 55000–55250.

Limitar o tamanho da transferência da área de transferência da sessão para o cliente

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de uma sessão virtual para um endpoint cliente durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, habilite a configuração **Limitar o tamanho da transferência da área de transferência da sessão para o cliente**. Em seguida, no campo **Limite de tamanho**, insira um valor em kilobytes para definir o tamanho da transferência de dados entre uma sessão e a área de transferência local.

Por padrão, esta configuração está desabilitada e não há limite para transferências da sessão para o cliente.

Restringir gravação da área de transferência do cliente

Se esta configuração estiver **Habilitada**, os dados da área de transferência do host não podem ser compartilhados com o endpoint do cliente. Você pode permitir formatos específicos habilitando a configuração **Formatos permitidos para gravação da área de transferência do cliente**.

Por padrão, esta configuração está **Desabilitada**.

Restringir gravação da área de transferência da sessão

Quando esta configuração está **Habilitada**, os dados da área de transferência do cliente não podem ser compartilhados com os aplicativos da sessão. Você pode permitir formatos específicos habilitando a configuração **Formatos permitidos para gravação da área de transferência da sessão**.

Por padrão, esta configuração está **Desabilitada**.

Formatos permitidos para gravação da área de transferência da sessão

Quando a configuração **Restringir gravação da área de transferência da sessão** está **Habilitada**, os dados da área de transferência do cliente não podem ser compartilhados com os

aplicativos da sessão. Você pode usar esta configuração para permitir que formatos de dados específicos sejam compartilhados com a área de transferência da sessão.

Os seguintes formatos de área de transferência são definidos pelo sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Os seguintes formatos personalizados são predefinidos em XenApp and XenDesktop e Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT

- CFX_OfficeDrawingShape
- CFX_BIFF8

O formato HTML está desabilitado por padrão. Para habilitar este recurso:

- Verifique se **Redirecionamento da área de transferência do cliente** está definido como **Permitido**.
- Verifique se **Restringir gravação da área de transferência da sessão** está definido como **Habilitado**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja que sejam suportados) em **Formatos permitidos para gravação da área de transferência da sessão**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos a serem registrados no sistema. Os nomes dos formatos diferenciam maiúsculas de minúsculas.

Esta configuração não se aplica se a política de **Redirecionamento da área de transferência do cliente** estiver definida como **Proibido** ou a política de **Restringir gravação da área de transferência da sessão** estiver definida como **Desabilitado**.

> **Observação:**
>
> Habilitar o suporte à cópia da área de transferência no formato HTML (CF_HTML) copia quaisquer scripts da origem do conteúdo copiado para o destino. Verifique se você confia na origem antes de prosseguir com a cópia. Se você copiar conteúdo contendo scripts, eles estarão ativos apenas se você salvar o arquivo de destino como um arquivo HTML e executá-lo.

Inicialização da área de trabalho

Esta configuração permite ou impede conexões a uma sessão nesse VDA usando uma conexão ICA por usuários não administrativos em um grupo de Usuários de Acesso Direto do VDA.

Por padrão, usuários não administrativos não podem se conectar a essas sessões.

Esta configuração não afeta usuários não administrativos em um grupo de Usuários de Acesso Direto VDA que estão usando uma conexão RDP. Esses usuários podem se conectar ao VDA quando esta configuração está ativada ou desativada. Esta configuração não afeta usuários não

administrativos que não estão em um grupo de Usuários de Acesso Direto VDA. Esses usuários não podem se conectar ao VDA quando esta configuração está ativada ou desativada.

Redirecionamento FIDO2

Esta configuração ativa ou desativa o redirecionamento FIDO2. O redirecionamento FIDO2 permite que os usuários aproveitem os componentes FIDO2 do endpoint local em uma máquina virtual. Os usuários podem autenticar a sessão virtual por meio de chaves de segurança FIDO2 ou biometria integrada em dispositivos que possuem TPM 2.0 e Windows Hello.

Quando esta configuração está **Permitida**, os usuários podem fazer a autenticação FIDO2 usando os recursos do endpoint local. Por padrão, esta configuração está **Permitida**.

Tempo limite de conexão do listener ICA

Esta configuração especifica o tempo máximo de espera para que uma conexão usando o protocolo ICA seja concluída.

Por padrão, o tempo máximo de espera é de 120.000 milissegundos, ou dois minutos.

Número da porta do listener ICA

Esta configuração especifica o número da porta TCP/IP usado pelo protocolo ICA no servidor.

Por padrão, o número da porta é definido como 1494.

Os números de porta válidos devem estar no intervalo de 0 a 65535 e não devem entrar em conflito com outros números de porta conhecidos. Se você alterar o número da porta, reinicie o servidor para que o novo valor entre em vigor. Se você alterar o número da porta no servidor, também deverá alterá-lo em cada aplicativo ou plug-in Citrix Workspace™ que se conecta ao servidor.

Teclado e Editor de Método de Entrada (IME)

Esta configuração ativa ou desativa o seguinte:

- Sincronização dinâmica do layout do teclado
- Editor de Método de Entrada (IME)
- Mapeamento de layout de teclado Unicode
- Oculta ou mostra a mensagem da caixa de diálogo de notificação de troca de layout do teclado

1. No Web Studio, selecione **Teclado e IME**.

2. Selecione **Sincronização do layout do teclado do cliente e melhoria do IME** para controlar a sincronização dinâmica do layout do teclado e os recursos genéricos do Editor de Método de Entrada (IME) do cliente no VDA. Você pode configurar:

   Desabilitado - sincronização dinâmica do layout do teclado e Editor de Método de Entrada (IME) genérico do cliente.

   Suportar sincronização dinâmica do layout do teclado do cliente - habilita a sincronização dinâmica do layout do teclado.

   Suportar sincronização dinâmica do layout do teclado do cliente e melhoria do IME - habilita tanto a sincronização dinâmica do layout do teclado quanto o Editor de Método de Entrada (IME) genérico do cliente.
3. Selecione **Habilitar mapeamento de layout de teclado Unicode** para habilitar ou desabilitar o mapeamento de teclado Unicode.
4. Selecione **Ocultar caixa de mensagem pop-up de troca de layout do teclado** para controlar se uma mensagem aparece ou não, indicando que o layout do teclado está sincronizando quando o usuário altera o layout do teclado do cliente. Se você impedir que a mensagem apareça, os usuários devem esperar alguns momentos antes de digitar para evitar a entrada incorreta de caracteres.

Configurações padrão:

- **Sincronização do layout do teclado do cliente e melhoria do IME**
  - Desabilitado no Windows Server 2016 e Windows Server 2019.
  - Suporta sincronização dinâmica do layout do teclado do cliente e melhoria do IME no Windows Server 2012 e Windows 2010.
- **Desabilitar mapeamento de layout de teclado Unicode**
- **Mostrar caixa de mensagem pop-up de troca de layout do teclado**

Esta política substitui as configurações de registro listadas na seção **Descrição** das configurações de política.

Atraso na inicialização do verificador de logoff

Esta configuração especifica a duração para atrasar a inicialização do verificador de logoff. Use esta política para definir o tempo (em segundos) que uma sessão de cliente aguarda antes de desconectar a sessão.

Esta configuração também aumenta o tempo que um usuário leva para fazer logoff do servidor.

Modo tolerante a perdas

> **Importante:**
>
> - O recurso requer no mínimo o aplicativo Citrix Workspace 2002 para Windows. Esta versão do VDA o suporta quando ele se torna disponível.
> - O modo tolerante a perdas para gráficos é suportado no Citrix Gateway e no Citrix Gateway Service. Este modo está disponível apenas com conexões diretas.

> Esta configuração habilita ou desabilita o modo tolerante a perdas para gráficos.

Por padrão, o modo tolerante a perdas para gráficos é **Permitido**.

Quando permitido, o modo é ativado quando a perda de pacotes e a latência estão acima de um limite. Você pode definir os limites usando a política de limites tolerantes a perdas.

Limites tolerantes a perdas

Quando o modo tolerante a perdas estiver disponível, esta configuração especifica os limites das métricas de rede nos quais a sessão muda para o modo tolerante a perdas para gráficos.

Os limites padrão são:

- Perda de pacotes: 5%
- Latência: 300 ms (RTT)

Para obter mais informações, consulte modo tolerante a perdas.

Modo tolerante a perdas para áudio

Esta configuração habilita ou desabilita o modo tolerante a perdas para áudio.

Quando habilitado, o áudio é enviado através do modo tolerante a perdas.

Por padrão, o modo tolerante a perdas para áudio é **Proibido**.

Para habilitar a política, edite o registro da política de modo tolerante a perdas para áudio para **Permitido**.

O transporte EDT é necessário para habilitar o modo tolerante a perdas para áudio.

Protocolo Rendezvous

Esta configuração altera como as sessões HDX são proxy quando se usa o Citrix Gateway Service. Quando habilitado, o tráfego HDX não flui mais através do Citrix Cloud Connector. Em vez disso, o VDA estabelece uma conexão de saída diretamente com o Citrix Gateway Service (melhorando a escalabilidade do Cloud Connector).

> **Importante:**
>
> Um alternador de recursos no Citrix Cloud™ e uma configuração de política HDX controlam este recurso. O alternador de recursos do Citrix Cloud é habilitado por padrão, enquanto a configuração HDX é desabilitada por padrão. A configuração HDX afeta apenas as sessões HDX estabelecidas através do Citrix Gateway Service. Esta configuração não afeta as sessões estabelecidas diretamente entre o cliente e o VDA ou através de um Citrix Gateway local.

> Para obter informações, consulte protocolo Rendezvous.

Configuração de proxy Rendezvous

Esta configuração permite configurar um proxy explícito para uso com o protocolo Rendezvous. Se estiver usando um proxy transparente, esta configuração não precisa ser habilitada.

Por padrão, esta configuração está desabilitada.

Quando desabilitado, o VDA não roteia o tráfego de saída através de nenhum proxy não transparente ao tentar estabelecer uma conexão Rendezvous com o Gateway Service.

Quando habilitado, o VDA tenta estabelecer uma conexão Rendezvous com o Gateway Service através do proxy definido nesta configuração.

O VDA suporta o uso de proxies HTTP e SOCKS5 para conexões Rendezvous. Para configurar o VDA para usar um proxy para a conexão Rendezvous, você deve habilitar esta configuração. Além disso, especifique o endereço do proxy ou o caminho para o arquivo PAC. Por exemplo:

- Endereço do proxy: `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path>/<filename>.pac`

A versão 2103 do VDA é a versão mínima suportada para configuração de proxy com um arquivo PAC. Para obter mais informações sobre o esquema de arquivo PAC para proxies SOCKS5, consulte Configuração de proxy.

Observação:

Somente proxies SOCKS5 suportam transporte de dados via EDT. Para um proxy HTTP, use TCP como protocolo de transporte para ICA.

Para obter mais informações, consulte Protocolo Rendezvous.

Início de programas não publicados durante a conexão do cliente

Essa configuração especifica se deve permitir o início de aplicativos iniciais via RDP no servidor.

Por padrão, o início de aplicativos iniciais via RDP no servidor não é permitido.

Coleta de métricas de sessão

Essa configuração permite que a Citrix colete métricas de sessão de usuário e máquina entre o VDA e o Workspace para melhorar a experiência do usuário.

A Citrix coleta dados como sistema operacional, tempo de atividade, informações do sistema do computador, detalhes do controlador de vídeo, versão do VDA, tipo de implantação e status de ingresso no domínio. Além disso, você pode coletar algumas configurações de sessão, juntamente com dados de desempenho e confiabilidade, para auxiliar nos esforços de melhoria do produto. Para obter mais informações sobre nosso Programa de Melhoria da Experiência do Cliente, consulte:

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/pt-br/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/pt-br/mac-vda/configure/session/supportability-service>`

Por padrão, essa configuração está habilitada.

Configurações de política de alternância do modo tablet

A alternância do modo tablet otimiza a aparência e o comportamento dos aplicativos da Loja, aplicativos Win32 e do shell do Windows no VDA. Isso é feito alternando automaticamente a área de trabalho virtual para o modo Tablet ao conectar-se de dispositivos de formato pequeno, como telefones e tablets, ou qualquer dispositivo habilitado para toque.

Se esta política estiver desabilitada, o VDA estará no modo definido pelo usuário e manterá o mesmo modo durante todo o tempo, independentemente do tipo de cliente.

Configurações de política de reconexão automática do cliente

A seção **Reconexão Automática do Cliente** contém configurações de política para controlar a reconexão automática de sessões.

Reconexão automática do cliente

Esta configuração permite ou impede a reconexão automática pelo mesmo cliente após uma conexão ter sido interrompida.

Para Citrix Receiver para Windows 4.7 e posterior e Citrix Workspace app 1808 e posterior, a reconexão automática do cliente usa apenas as configurações de política do Citrix Studio. As atualizações dessas políticas no Studio sincronizam a reconexão automática do cliente do servidor para o cliente. Com versões mais antigas do Citrix Receiver para Windows, para configurar a reconexão automática do cliente, use uma política do Studio e altere o registro ou o arquivo default.ica.

Permitir a reconexão automática do cliente permite que os usuários retomem o trabalho de onde foram interrompidos quando uma conexão foi quebrada. A reconexão automática detecta conexões quebradas e, em seguida, reconecta os usuários às suas sessões.

Se o cookie do aplicativo Citrix Workspace™ contendo a chave para o ID da sessão e as credenciais não for usado, a reconexão automática poderá resultar no início de uma nova sessão. Ou seja, em vez de reconectar a uma sessão existente. O cookie não é usado se tiver expirado. Por exemplo, o cookie pode expirar devido a um atraso na reconexão, ou se as credenciais precisarem ser reinseridas. Se os usuários se desconectarem intencionalmente, a reconexão automática do cliente não será acionada.

Uma janela de sessão fica esmaecida quando uma reconexão está em andamento. Um cronômetro de contagem regressiva exibe o tempo restante antes que a sessão seja reconectada. Quando uma sessão expira, ela é desconectada.

Para sessões de aplicativo, quando a reconexão automática é permitida, um cronômetro de contagem regressiva aparece na área de notificação. Este cronômetro especifica o tempo restante antes que a sessão seja reconectada. O aplicativo Citrix Workspace tenta reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de usuário, quando a reconexão automática é permitida, o aplicativo Citrix Workspace tenta 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, este período é de dois minutos. Para alterar este período, edite a política.

Por padrão, a reconexão automática do cliente é permitida. Você pode desativá-la definindo a política como **Proibida**.

Autenticação de reconexão automática do cliente

Esta configuração especifica se a autenticação é necessária para reconexões automáticas do cliente.

Quando um usuário faz login inicialmente, as credenciais são criptografadas, armazenadas na memória e um cookie é criado contendo a chave de criptografia. O cookie é enviado para o aplicativo Citrix Workspace. Quando esta configuração é configurada, os cookies não são usados. Em vez disso, uma caixa de diálogo é exibida para os usuários solicitando credenciais quando o aplicativo Citrix Workspace tenta reconectar automaticamente.

Por padrão, a autenticação não é necessária.

Registro de reconexão automática do cliente

Essa configuração habilita ou desabilita o registro de reconexões automáticas do cliente no log de eventos.

Quando o registro está habilitado, o Log do Sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Um site não fornece um log combinado de eventos de reconexão para todos os servidores.

Por padrão, o registro está desabilitado.

Tempo limite de reconexão automática do cliente

Por padrão, o tempo limite de reconexão automática do cliente é definido como 120 segundos; o valor máximo configurável para um tempo limite de reconexão automática do cliente é de 300 segundos. Use esta política para definir o valor do tempo limite.

Nível de transparência da interface do usuário de reconexão

Essa configuração permite especificar o nível de opacidade aplicado à janela da sessão do XenApp ou XenDesktop® durante o tempo de reconexão de confiabilidade da sessão.

Por padrão, a transparência da interface do usuário de reconexão é definida como 80%.

Configurações de política de áudio

A seção **Áudio** inclui configurações de política que permitem que os dispositivos do usuário enviem e recebam áudio em sessões sem reduzir o desempenho.

Áudio Adaptável

Esta configuração habilita ou desabilita o áudio adaptável. Ao habilitar esta política, as configurações de qualidade de áudio são ajustadas dinamicamente para fornecer a melhor experiência do usuário. Esta configuração se aplica a sessões de SO de sessão única e SO de múltiplas sessões de VDAs usando Citrix Virtual Apps and Desktops™ 2109 ou posterior.

Quando esta configuração é proibida, a política de qualidade de áudio é aplicada. Para obter mais informações, consulte Qualidade de áudio.

Por padrão, a política de áudio adaptável está habilitada.

Áudio sobre transporte em tempo real UDP

Esta configuração permite ou impede a transmissão e o recebimento de áudio entre o VDA e o dispositivo do usuário via RTP usando o User Datagram Protocol (UDP). Quando esta configuração é desabilitada, o áudio é enviado e recebido via TCP.

Por padrão, o áudio sobre UDP é permitido.

Plug N Play de áudio

Esta configuração permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som.

Por padrão, o uso de vários dispositivos de áudio é permitido.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Qualidade do áudio

Esta configuração especifica o nível de qualidade do som recebido nas sessões do usuário.

Por padrão, a qualidade do som é definida como Alta - áudio de alta definição.

Para controlar a qualidade do som, escolha uma das seguintes opções:

- Selecione Baixa - para conexões de baixa velocidade para conexões de baixa largura de banda. Os sons enviados para o dispositivo do usuário são compactados em até 16 Kbps. Essa compactação resulta em uma redução significativa na qualidade do som. Mas também permite um desempenho razoável para uma conexão de baixa largura de banda.
- Selecione Médio - otimizado para fala para fornecer aplicativos de Voz sobre Protocolo de Internet. Essa configuração entrega aplicativos de mídia em conexões de rede desafiadoras com linhas inferiores a 512 Kbps, ou congestionamento significativo e perda de pacotes. Este codec oferece tempo de codificação rápido, tornando-o ideal para uso com softphones e aplicativos de Comunicações Unificadas quando você precisa de processamento de mídia no lado do servidor.

  O áudio enviado para o dispositivo do usuário é compactado em até 64 Kbps. Essa compactação resulta em uma redução moderada na qualidade do áudio reproduzido no dispositivo do usuário, ao mesmo tempo em que oferece baixa latência e consome pouca largura de banda. Se a qualidade da Voz sobre Protocolo de Internet for insatisfatória, certifique-se de que a configuração da política de Transporte em Tempo Real de Áudio sobre UDP esteja definida como Permitido.

  Agora, o Transporte em Tempo Real (RTP) sobre UDP é suportado apenas quando esta qualidade de áudio é selecionada. Use esta qualidade de áudio mesmo para entregar aplicativos de mídia para conexões de rede desafiadoras, como linhas de baixa velocidade (inferiores a 512 Kbps). Além disso, quando há congestionamento e perda de pacotes na rede.
- Selecione Alta - áudio de alta definição para conexões onde a largura de banda é abundante e a qualidade do som é importante. Os clientes podem reproduzir o som em sua taxa nativa. Os sons são compactados em um nível de alta qualidade, mantendo a qualidade de CD, e usando até 112 Kbps de largura de banda. A transmissão dessa quantidade de dados pode resultar em aumento do uso da CPU e congestionamento da rede.

A largura de banda é consumida apenas enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo de largura de banda dobra.

Para especificar a quantidade máxima de largura de banda, configure as configurações de **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem de limite de largura de banda de redirecionamento de áudio**.

Redirecionamento de áudio do cliente

Essa configuração especifica se os aplicativos hospedados no servidor podem reproduzir sons por meio de um dispositivo de som instalado no dispositivo do usuário. Essa configuração também especifica se os usuários podem gravar entrada de áudio.

Por padrão, o redirecionamento de áudio é permitido.

Depois de permitir essa configuração, você pode limitar a largura de banda consumida pela reprodução ou gravação de áudio. A restrição desse consumo pelo áudio pode melhorar o desempenho do aplicativo, mas também pode degradar a qualidade do áudio. O consumo ocorre apenas enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, esse consumo dobra. Para especificar a quantidade máxima de largura de banda, configure as configurações de **Limite de largura de banda de redirecionamento de áudio** ou **Porcentagem de limite de largura de banda de redirecionamento de áudio**.

Em máquinas com Windows Multi-session OS, certifique-se de que a configuração **Audio Plug N Play** esteja habilitada para suportar vários dispositivos de áudio.

Importante: Proibir o redirecionamento de áudio do cliente desabilita toda a funcionalidade de áudio HDX™.

Redirecionamento de microfone do cliente

Essa configuração habilita ou desabilita o redirecionamento do microfone do cliente. Quando habilitado, os usuários podem usar microfones para gravar entrada de áudio em uma sessão.

Por padrão, o redirecionamento de microfone é permitido.

Por segurança, os usuários são alertados quando servidores não confiáveis por seus dispositivos tentam acessar microfones. Os usuários podem optar por aceitar ou não aceitar o acesso. Os usuários podem desabilitar o alerta no aplicativo Citrix Workspace™.

Em máquinas com Windows Multi-session OS, certifique-se de que a configuração Audio Plug N Play esteja Habilitada para suportar vários dispositivos de áudio.

Se a configuração de **Redirecionamento de áudio do cliente** estiver desabilitada no dispositivo do usuário, esta regra não terá efeito.

Configurações de política de largura de banda

A seção **Largura de banda** inclui configurações de política para evitar problemas de desempenho relacionados ao uso da largura de banda da sessão do cliente.

Importante: O uso dessas configurações de política com as configurações da **política Multi-Stream** pode produzir resultados inesperados. Se você usar as configurações Multi-Stream em uma política, certifique-se de que essas configurações de política de limite de largura de banda não estejam incluídas.

Limite de largura de banda de redirecionamento de áudio

Esta configuração especifica a largura de banda máxima permitida para reprodução ou gravação de áudio em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de áudio

Esta configuração especifica o limite máximo de largura de banda permitido para reprodução ou gravação de áudio como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de áudio**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para as sessões do cliente.

Limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB para e do cliente. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de dispositivo USB do cliente**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente

Esta configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB de e para o cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de dispositivo USB do cliente**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta configuração, também deverá configurar a configuração **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Limite de largura de banda de redirecionamento da área de transferência

Esta configuração especifica a largura de banda máxima permitida para a transferência de dados entre uma sessão e a área de transferência local. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento da área de transferência**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento da área de transferência

Esta configuração especifica a largura de banda máxima permitida para a transferência de dados entre uma sessão e a área de transferência local como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento da área de transferência**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta configuração, também deverá configurar a configuração **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Limite de largura de banda de redirecionamento de porta COM

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta configuração usando o registro; consulte Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica a largura de banda máxima permitida em kilobits por segundo para acessar uma porta COM em uma conexão de cliente. Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de porta COM**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de porta COM

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registo; consulte Configurar as definições de Redirecionamento de Porta COM e Porta LPT usando o registo.

Esta definição especifica a largura de banda máxima permitida para aceder a portas COM numa ligação de cliente como uma percentagem da largura de banda total da sessão.

Por predefinição, nenhum máximo (zero) é especificado

Se introduzir um valor para esta definição e um valor para a definição **limite de largura de banda de redirecionamento de porta COM**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se configurar esta definição, também deve configurar a definição **limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente

Limite de largura de banda de redirecionamento de ficheiros

Esta definição especifica a largura de banda máxima permitida para aceder a uma unidade de cliente numa sessão de utilizador. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por predefinição, nenhum máximo (zero) é especificado.

Se introduzir um valor para esta definição e um valor para a definição **percentagem do limite de largura de banda de redirecionamento de ficheiros**, a definição mais restritiva (o valor mais baixo) entra em vigor.

Porcentagem de limite de largura de banda de redirecionamento de arquivo

Esta definição especifica o limite máximo de largura de banda permitido para aceder a unidades de cliente como uma percentagem da largura de banda total da sessão.

Por predefinição, nenhum máximo (zero) é especificado.

Se introduzir um valor para esta definição e um valor para a definição **limite de largura de banda de redirecionamento de ficheiros**, a definição mais restritiva (o valor mais baixo) é aplicada.

Se configurar esta definição, também deve configurar a definição **limite de largura de banda geral da sessão**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Limite de largura de banda de aceleração multimédia HDX™ MediaStream

Esta definição especifica o limite máximo de largura de banda permitido para a entrega de áudio e vídeo em streaming usando a Aceleração Multimédia HDX MediaStream. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) terá efeito.

Porcentagem do limite de largura de banda da aceleração multimídia HDX MediaStream

Esta configuração especifica a largura de banda máxima permitida para a entrega de áudio e vídeo por streaming usando a aceleração multimídia HDX MediaStream como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit**, a configuração mais restritiva (o valor mais baixo) terá efeito.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Limite de largura de banda de redirecionamento de porta LPT

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as definições de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica a largura de banda máxima permitida para trabalhos de impressão usando uma porta LPT em uma única sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **LPT port redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de porta LPT

Nota: Para o Virtual Delivery Agent 7.0 a 7.8, configure esta definição usando o registro; consulte Configurar as definições de redirecionamento de porta COM e porta LPT usando o registro.

Esta configuração especifica o limite de largura de banda para trabalhos de impressão usando uma porta LPT em uma única sessão de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de porta LPT**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para as sessões do cliente.

Limite geral de largura de banda da sessão

Esta configuração especifica a quantidade total de largura de banda disponível, em kilobits por segundo, para as sessões do usuário.

O limite máximo de largura de banda aplicável é de 20 Mbps (20.000 Kbps). Por padrão, nenhum máximo (zero) é especificado.

Limitar a quantidade de largura de banda consumida por uma conexão de cliente pode melhorar o desempenho quando outros aplicativos fora da conexão de cliente estão competindo por largura de banda limitada.

Limite de largura de banda de redirecionamento de impressora

Esta configuração especifica a largura de banda máxima permitida para acessar impressoras cliente em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Porcentagem do limite de largura de banda de redirecionamento de impressora**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem de limite de largura de banda de redirecionamento de impressora

Esta configuração especifica a largura de banda máxima permitida para acessar impressoras cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **Limite de largura de banda de redirecionamento de impressora**, a configuração mais restritiva (com o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Limite geral de largura de banda da sessão**, que especifica a quantidade total de largura de banda disponível para as sessões do cliente.

Limite de largura de banda de redirecionamento de dispositivo TWAIN

Esta configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN a partir de aplicativos publicados. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **TWAIN device redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN

Esta configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN de aplicativos publicados como uma porcentagem da largura de banda total da sessão.

Por padrão, nenhum máximo (zero) é especificado.

Se você inserir um valor para esta configuração e um valor para a configuração **TWAIN device redirection bandwidth limit**, a configuração mais restritiva (com o valor mais baixo) será aplicada.

Se você configurar esta definição, também deverá configurar a definição **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões de cliente.

Configurações de política de redirecionamento de conteúdo bidirecional

A seção **Redirecionamento de Conteúdo Bidirecional** possui configurações de política para habilitar ou desabilitar o redirecionamento de URL do cliente para o VDA e do VDA para o cliente.

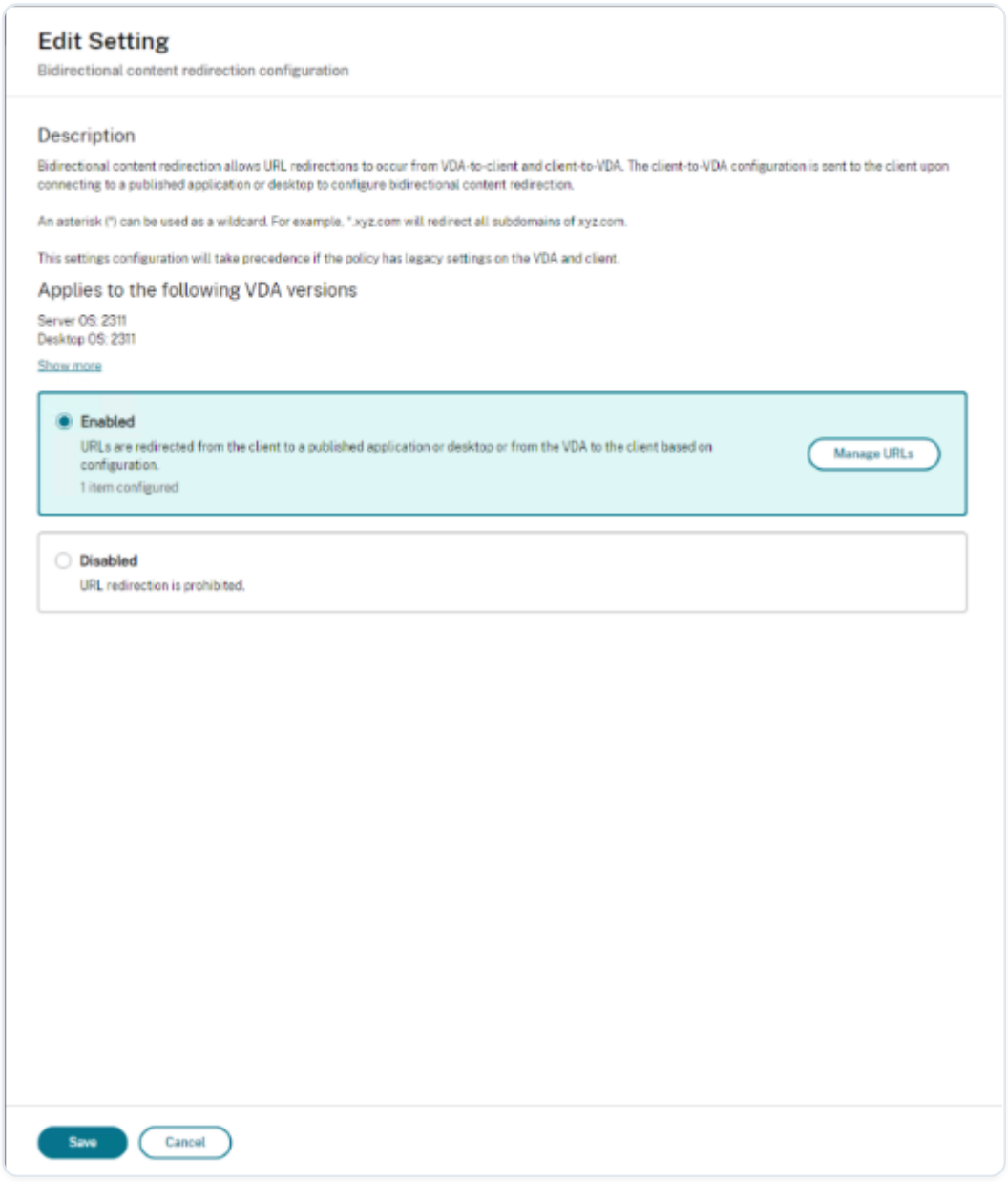
As políticas de servidor são definidas no Web Studio. A partir da versão 2311 do aplicativo Citrix Workspace™, esta configuração substitui as três configurações legadas a seguir no Web Studio que estão obsoletas:

- Permitir redirecionamento de conteúdo bidirecional
- URLs permitidas para serem redirecionadas para o VDA
- URLs permitidas para serem redirecionadas para o Cliente

Também substitui as três configurações de Objeto de Política de Grupo (GPO) locais a seguir em clientes Windows:

- Redirecionamento de conteúdo bidirecional
- Substituições de redirecionamento de conteúdo bidirecional
- Redirecionamento OAuth

Se esta configuração estiver habilitada, as configurações de cliente para VDA são enviadas ao cliente ao conectar-se a um aplicativo ou desktop publicado para configurar o redirecionamento de conteúdo bidirecional.



Se esta configuração estiver configurada, ela terá precedência sobre as configurações legadas no Web Studio e no cliente. A Citrix® recomenda usar apenas as novas configurações de política e excluir quaisquer configurações legadas para evitar comportamentos inesperados.

As políticas de cliente não devem ser definidas se o VDA e o DDC estiverem executando a versão 2311 ou posterior. Caso contrário, as políticas de cliente são definidas a partir do modelo administrativo do Objeto de Política de Grupo do aplicativo Citrix Workspace.

A Citrix oferece redirecionamento de host para cliente e Acesso a Aplicativos Locais para redirecionamento de cliente para URL. No entanto, a Citrix recomenda que você use o redirecionamento de conteúdo bidirecional para clientes Windows ingressados no domínio.

A Citrix recomenda usar a nova interface de usuário no Web Studio para configurar o recurso em vez do Desktop Studio.

Redirecionamento de curinga

O redirecionamento de conteúdo bidirecional suporta o uso de curingas ao definir as URLs a serem redirecionadas. Para mais detalhes e para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de Configuração. No Web Studio, defina a URL curinga editando a string JSON como um valor na chave `url` no array `hostToClientUrls` ou no array `clientToHostUrls`.

> **Observação:**
>
> - Não defina a mesma URL em `hostToClientUrls` e `clientToHostUrls` para evitar loops infinitos.
> - Domínios de nível superior não são suportados. Por exemplo, `<https://www.citrix.*>` ou `<http://www.citrix.co*>` não é redirecionado.

Configuração de redirecionamento de conteúdo bidirecional

Defina esta política como `Enabled` para começar a configurar o recurso e clique em **Gerenciar URLs**. Defina as seguintes configurações:

- **Redirecionamento VDA para cliente**
- **Redirecionamento cliente para VDA**

REDIRECIONAMENTO VDA PARA CLIENTE

Para redirecionar URLs do VDA para o cliente, insira uma URL por linha. Curingas são permitidos. O redirecionamento OAuth permite que você use o navegador no endpoint do cliente para realizar a autenticação e enviar o token de volta para o VDA.

Benefícios:

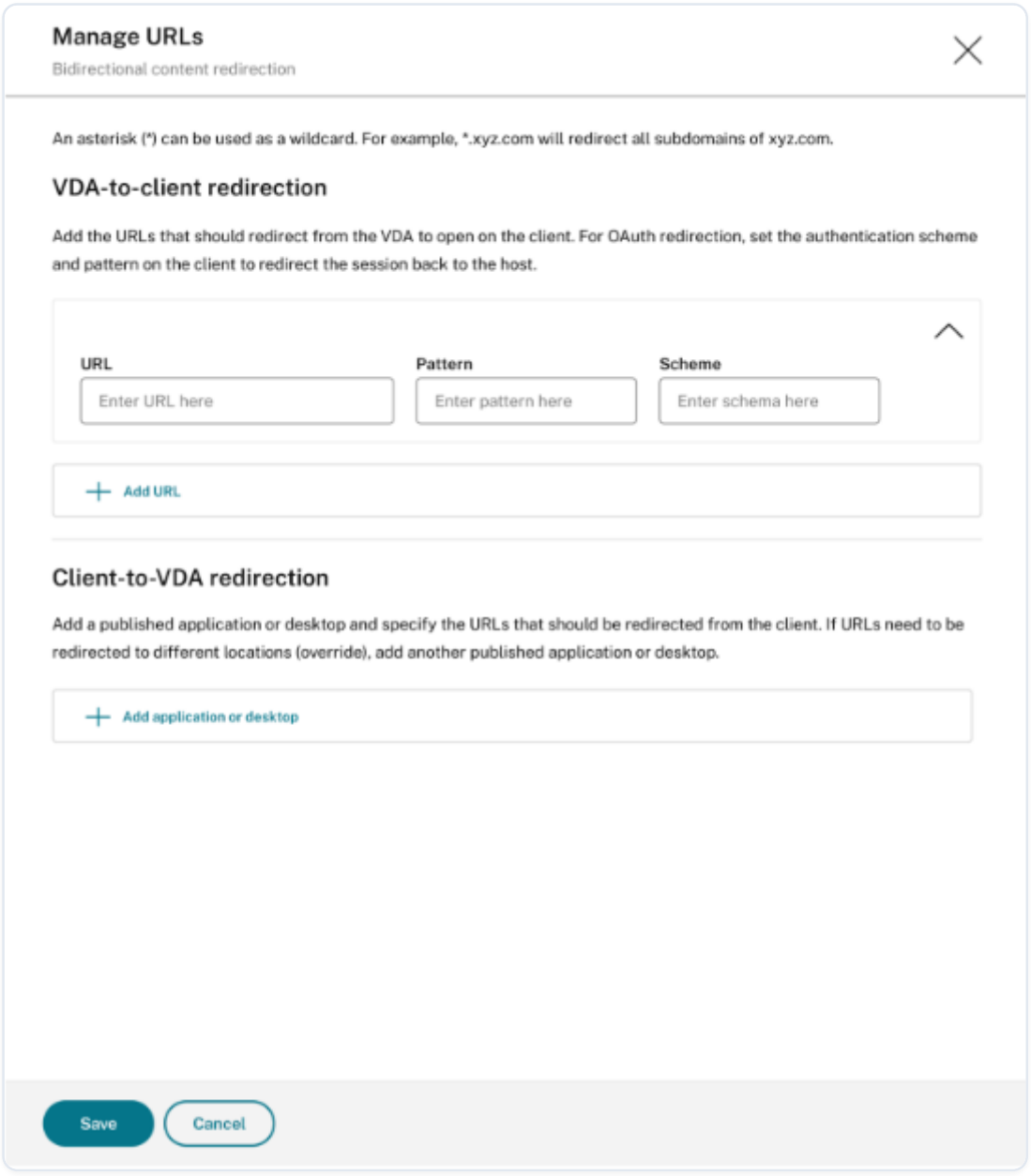
- Você pode evitar armazenar essas credenciais no ambiente hospedado.
- Você pode usar recursos biométricos que estão disponíveis no endpoint e não no VDA.

Configurações:

Para configurar o redirecionamento VDA para cliente para a URL, especifique o seguinte:

- **URL** (Obrigatório) Adicione a URL que deve ser redirecionada do VDA para abrir no cliente. Para **Redirecionamento OAuth**, defina o esquema de autenticação e o padrão no cliente para redirecionar a sessão de volta ao host.

- **Padrão**: (Opcional) Expressão regular de URL que, quando redirecionada para o cliente através do redirecionamento de URL VDA para Cliente, é rastreada como se um fluxo de autenticação OAuth tivesse começado, e quando o fluxo é concluído (detectado pelo esquema resultante ou padrão de URL de redirecionamento sendo aberto), essa URL resultante é redirecionada de volta para o VDA host que iniciou esse fluxo.
- **Esquema**: (Opcional) Se o **Esquema** for especificado, a URL de término deverá ter o formato: `<scheme>`:// `<something>`. Considere que o Esquema não foi especificado (vazio). Nesse caso, o padrão de URL resultante original é extraído do Padrão por meio de um grupo de captura de expressão regular (deve ser especificado no Padrão), e a URL original é reescrita para usar uma URL de redirecionamento `citrix-oauth-redir://`. Quando o fluxo é concluído, a URL de redirecionamento original é então redirecionada de volta para o Host (VDA). Neste caso, qualquer servidor de autorização OAuth deve ser configurado para permitir URLs de redirecionamento `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.



Observação:

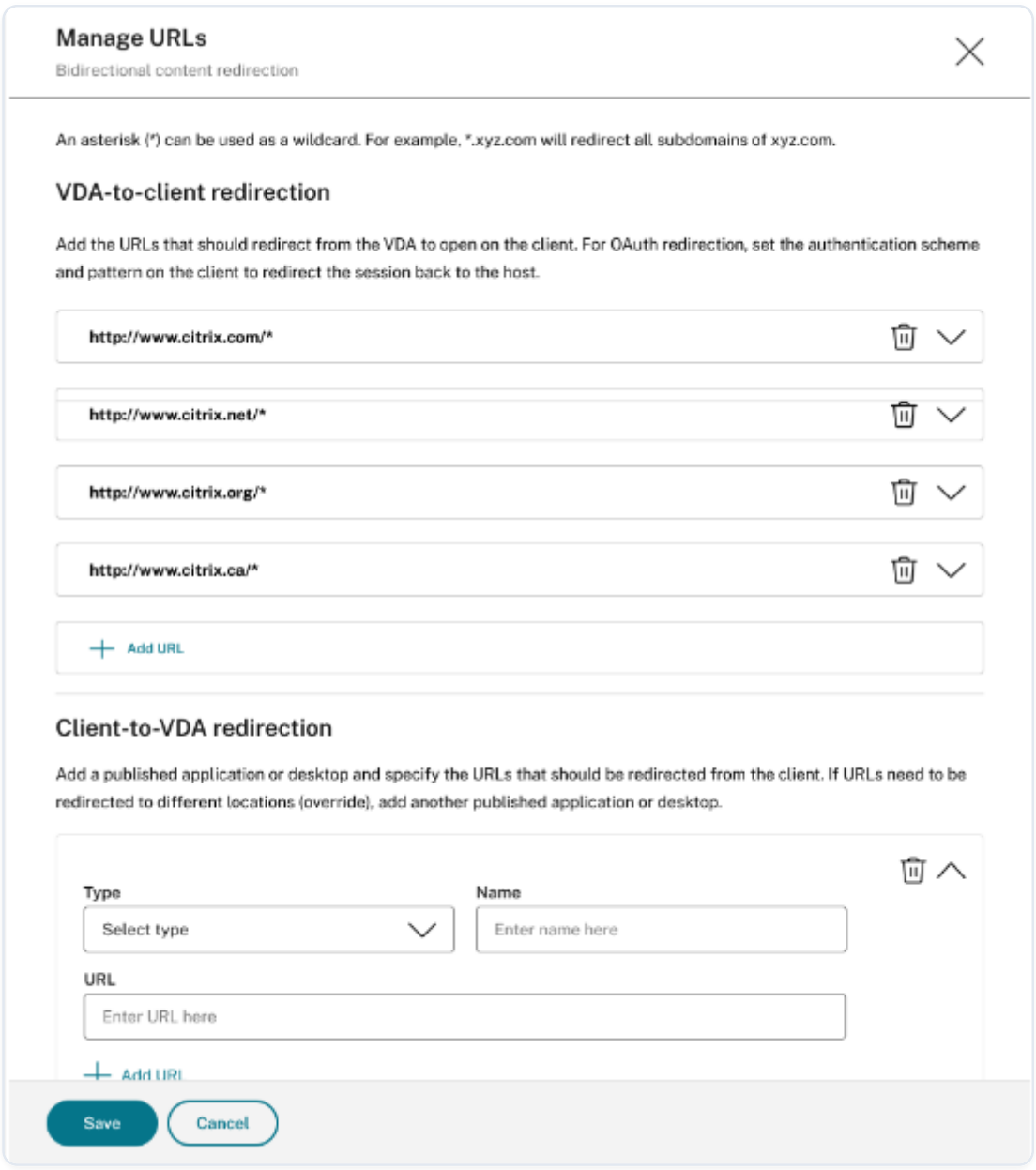
Embora tanto o **Padrão** quanto o **Esquema** sejam opcionais, se o **Padrão** for especificado, você também deve especificar o **Esquema**.

REDIRECIONAMENTO DE CLIENTE PARA VDA

Para redirecionar URLs do cliente para o VDA, conclua as seguintes etapas:

1. Configure o destino para as URLs do cliente.
2. Selecione Aplicativo Publicado ou Área de Trabalho Publicada.
3. Especifique o nome desse recurso.

4. Adicione todas as URLs que devem ser redirecionadas para esse recurso. Você pode substituir este recurso padrão adicionando um novo aplicativo ou área de trabalho e, em seguida, especificando as URLs a serem redirecionadas para esse recurso.



DESKTOP STUDIO

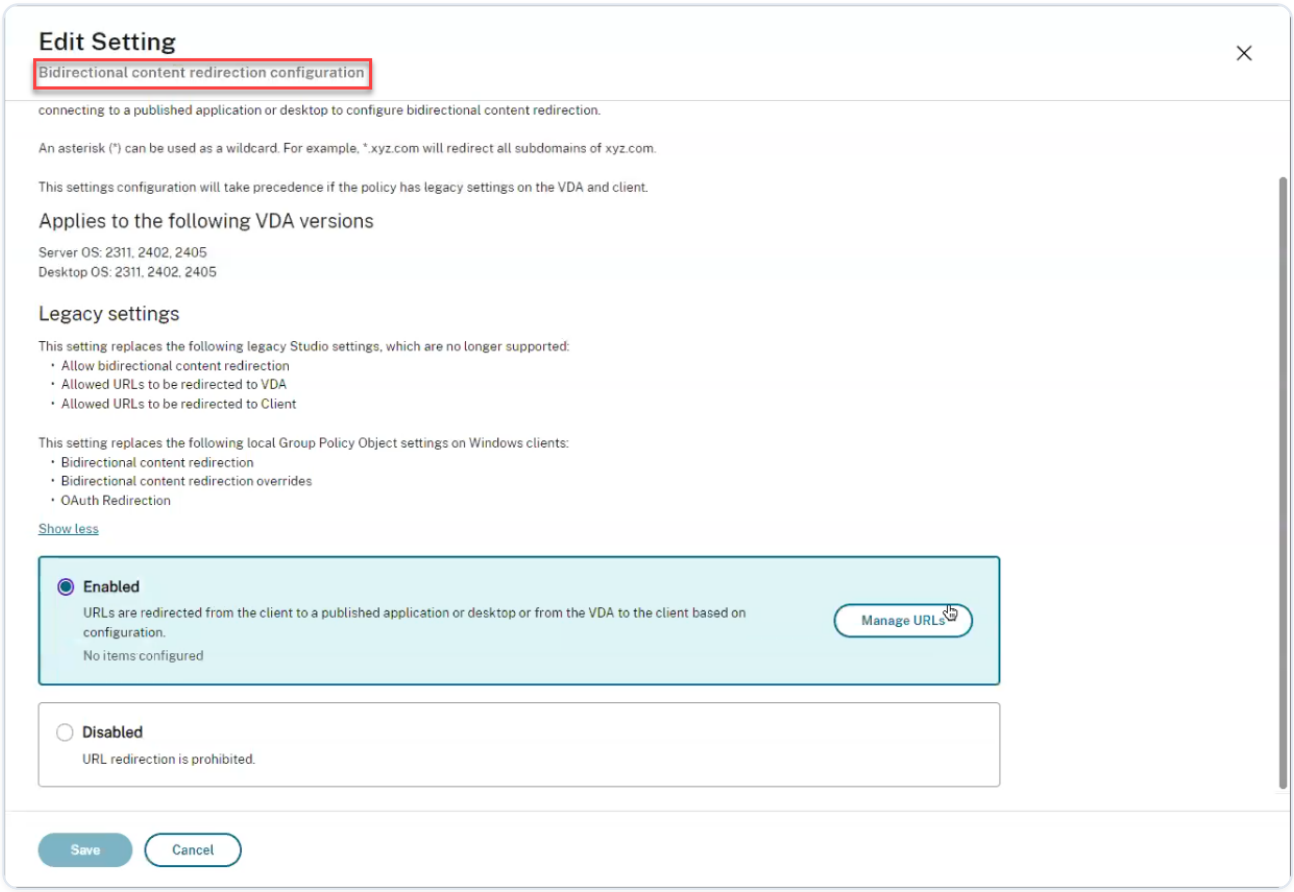
Observação:

A Citrix recomenda usar o Web Studio para configurar este recurso a partir da versão 2402 do Citrix Virtual Apps and Desktops™.

Para configurar o redirecionamento de conteúdo bidirecional para 2311, crie uma string JSON com o seguinte formato:

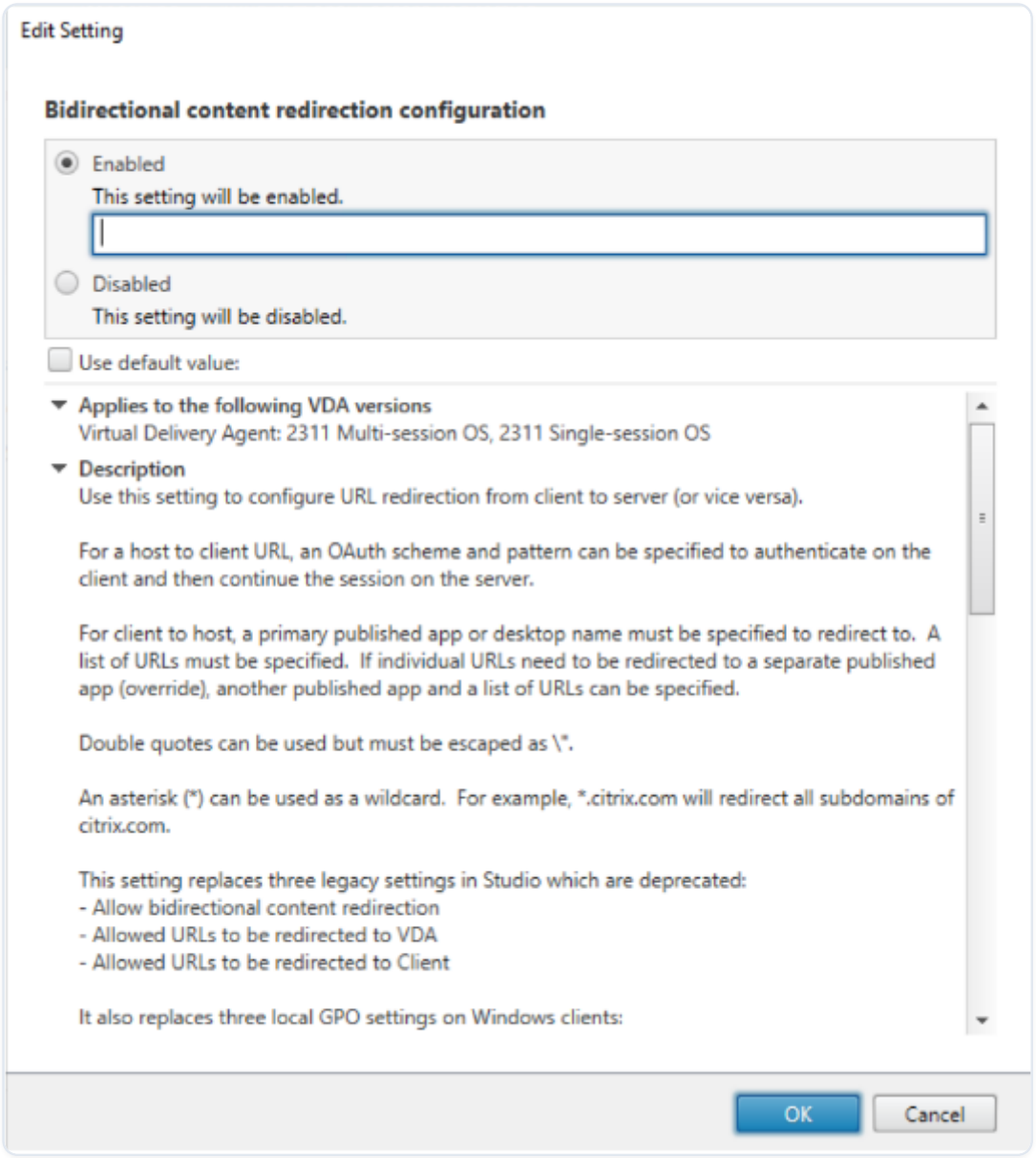
```
{
  "version": 1,
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



Os seguintes parâmetros devem ser definidos:

- **version**: (Obrigatório) Defina como 1.
- Para redirecionamento de URL de VDA para cliente, crie um único `hostToClientConfig`.
- **hostToClientUrls**: (Obrigatório) Lista de URLs a serem redirecionadas do host (VDA) para o cliente. Curingas são permitidos. Se '*' for especificado, então `clientToHostConfig` deve ser especificado com `publishedAppOrDesktopNameType`, um `publishedAppOrDesktopName` vazio e um `clientToHostUrls` vazio.



Redirecionamento OAuth

O redirecionamento OAuth permite que você use o navegador do endpoint do cliente para autenticar e envie o token de volta para o VDA.

Benefícios:

- Você pode evitar armazenar essas credenciais no ambiente hospedado.
- Você pode usar recursos biométricos que estão disponíveis no endpoint e não no VDA.

Para configurar o redirecionamento OAuth para a URL, especifique os seguintes parâmetros:

- **oAuthRedirectionPattern**: (Opcional) Expressão regular de URL que, quando redirecionada para o cliente via redirecionamento de URL VDA-para-Cliente, é rastreada como se um fluxo de autenticação OAuth tivesse começado, e quando o fluxo é concluído (detectado pelo

esquema resultante ou padrão de URL de redirecionamento sendo aberto), essa URL resultante é redirecionada de volta para o VDA host que iniciou esse fluxo.

- **oAuthScheme**: (Opcional) Se um Esquema for especificado, a URL de terminação deve estar no formato: `<scheme>`:// `<something>`. Considere que o Esquema não foi especificado (vazio). Nesse caso, o padrão de URL resultante original é extraído do Padrão por meio de um grupo de captura de expressão regular (deve ser especificado no Padrão), e a URL original é reescrita para usar uma URL de redirecionamento `citrix-oauth-redir://`. Quando o fluxo é concluído, a URL de redirecionamento original é então redirecionada de volta para o Host (VDA). Neste caso, qualquer servidor de Autorização OAuth deve ser configurado para permitir URLs de redirecionamento `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.

Para um redirecionamento de cliente para VDA, crie **clientToHostConfig** para cada recurso a ser redirecionado. Para cada recurso, inclua os seguintes parâmetros:

- **publishedAppOrDesktopNameType**: (Obrigatório) Um desktop publicado (“Desktop”) ou um aplicativo publicado (“Application”) configurado no Web Studio. Se o recurso não for válido, o redirecionamento não funcionará corretamente.
- **publishedAppOrDesktopName**: (Obrigatório) Nome do recurso conforme configurado no Web Studio.
- **clientToHostUrls**: (Obrigatório) Lista de URLs a serem redirecionadas do cliente para o host (VDA). curingas são permitidos.

Limitação conhecida

Ao iniciar um navegador usando o PowerShell com um esquema de URL personalizado (não HTTP ou HTTPS), as URLs personalizadas não são redirecionadas para o cliente.

Configurações de política de redirecionamento de conteúdo do navegador

A seção de redirecionamento de conteúdo do navegador inclui configurações de política para configurar esse recurso.

O redirecionamento de conteúdo do navegador controla e otimiza a forma como o Citrix Virtual Apps and Desktops™ entrega qualquer conteúdo de navegador da web (por exemplo, HTML5) aos usuários. Apenas a área visível do navegador onde o conteúdo é exibido é redirecionada.

O redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador são recursos independentes. As políticas de redirecionamento de vídeo HTML5 não são necessárias para que este recurso funcione. No entanto, o Serviço de Redirecionamento de Vídeo HTML5 do

Citrix HDX é usado para o redirecionamento de conteúdo do navegador. Para obter mais informações, consulte Redirecionamento de conteúdo do navegador.

> **Observação:**
>
> As configurações de política disponíveis no Web Studio podem ser substituídas por chaves de registro no VDA, mas as chaves de registro são opcionais.

TLS e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) em execução no VDA. Para conseguir esse redirecionamento e manter a integridade TLS da página da web, o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX gera dois certificados personalizados no armazenamento de certificados no VDA.

HdxVideo.js usa Secure Web sockets para se comunicar com WebSocketService.exe em execução no VDA. Este processo é executado no Sistema Local e realiza a terminação SSL e o mapeamento de sessão do usuário.

WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

Redirecionamento de conteúdo do navegador

Por padrão, o aplicativo Citrix Workspace™ tenta a busca e a renderização do cliente. A renderização do lado do servidor é tentada quando a busca e a renderização do cliente falham. Se você também habilitar a política de configuração de proxy de redirecionamento de conteúdo do navegador, o aplicativo Citrix Workspace tentará apenas a busca do servidor e a renderização do cliente.

Por padrão, esta configuração é Permitida.

Configuração de suporte à Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

O redirecionamento de conteúdo do navegador habilita a sobreposição que usa o esquema Negotiate para autenticação. Este aprimoramento fornece logon único a um servidor web configurado com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA.

Quando definido como **Permitido**, a sobreposição de redirecionamento de conteúdo do navegador obtém um tíquete Negotiate usando as credenciais do VDA do usuário. O usuário então se autentica no servidor web com um logon único.

Quando definido como **Proibido**, a sobreposição de redirecionamento de conteúdo do navegador não solicita um tíquete Negotiate do VDA. O usuário se autentica em um servidor web usando um método de autenticação básico. Este método de autenticação exige que os usuários insiram suas credenciais VDA cada vez que acessam o servidor web.

Por padrão, esta configuração é Proibida.

Configuração de autenticação de proxy web de busca de servidor de redirecionamento de conteúdo do navegador

Esta configuração roteia o tráfego HTTP originado em uma sobreposição através de um proxy web downstream. O proxy web downstream autoriza e autentica o tráfego HTTP usando as credenciais de domínio do usuário VDA através do esquema de autenticação Negotiate.

Você deve configurar o redirecionamento de conteúdo do navegador para o modo de busca de servidor no arquivo PAC usando a política de configuração de proxy de redirecionamento de conteúdo do navegador. No script PAC, forneça instruções para rotear o tráfego da sobreposição através de um proxy web downstream. Em seguida, configure o proxy web downstream para autenticar os usuários VDA através do esquema de autenticação Negotiate.

Quando definido como **Permitido**, o proxy web responde com um desafio 407 Negotiate, incluindo um cabeçalho **Proxy-autenticar: Negotiate**. O redirecionamento de conteúdo do navegador então obtém um tíquete de serviço Kerberos usando as credenciais de domínio do usuário VDA. Além disso, inclua o tíquete de serviço em solicitações posteriores ao proxy web.

Quando definido como **Proibido**, o redirecionamento de conteúdo do navegador faz proxy de todo o tráfego TCP entre a sobreposição e o proxy web sem interferir. A sobreposição usa credenciais de autenticação básicas ou quaisquer outras credenciais disponíveis para autenticar no proxy web.

Por padrão, esta configuração é Proibida.

Configurações da política de configuração de ACL (Lista de Controle de Acesso) de redirecionamento de conteúdo do navegador

Use esta configuração para configurar uma Lista de Controle de Acesso (ACL) de URLs que podem usar o redirecionamento de conteúdo do navegador ou que têm o acesso negado ao redirecionamento de conteúdo do navegador.

URLs autorizadas são as URLs na lista de permissões cujo conteúdo é redirecionado para o cliente.

O curinga `*` é permitido, mas não é permitido dentro do protocolo ou da parte do endereço de domínio da URL. No entanto, a partir do Citrix Virtual Apps and Desktops 7 2206, o curinga `*` é permitido dentro da parte do endereço de subdomínio da URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Não permitido: `http://*.*.com/`

Você pode obter uma granularidade melhor especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, apenas a página index.html será redirecionada.

Por padrão, esta configuração é definida como `https://www.youtube.com/*`

Para obter mais informações, consulte o artigo da Central de Conhecimento CTX238236.

> **Observação:**
>
> Você pode configurar a ACL para permitir que o BCR redirecione sites para o endpoint, e os sites de autenticação podem ser configurados para permitir Provedores de Identidade (IdP), como Okta e Duo, para autenticação usada na URL configurada.

Sites de autenticação de redirecionamento de conteúdo do navegador

Use esta configuração para configurar uma lista de URLs. Os sites redirecionados usando o redirecionamento de conteúdo do navegador usam a lista para autenticar um usuário. A configuração especifica as URLs para as quais o redirecionamento de conteúdo do navegador permanece ativo (redirecionado) ao navegar para fora de uma URL na lista de permissões.

Um cenário clássico é um site que depende de um Provedor de Identidade (IdP) para autenticação. Por exemplo, um site `www.xyz.com` deve ser redirecionado para o endpoint, mas um IdP de terceiros, como Okta (`www.xyz.okta.com`), lida com a parte da autenticação. O administrador usa a política de configuração de ACL de redirecionamento de conteúdo do navegador para adicionar `www.xyz.com` à lista de permissões. Em seguida, usa os sites de autenticação de redirecionamento de conteúdo do navegador para adicionar `www.xyz.okta.com` à lista de permissões.

Para obter mais informações, consulte o artigo da Central de Conhecimento CTX238236.

Configuração da lista de bloqueio de redirecionamento de conteúdo do navegador

Esta configuração funciona em conjunto com a configuração de ACL de redirecionamento de conteúdo do navegador. Considere que as URLs estão presentes na configuração de ACL de redirecionamento de conteúdo do navegador e na configuração da lista de bloqueio. Neste caso, a configuração da lista de bloqueio tem precedência e o conteúdo do navegador da URL não é redirecionado.

URLs não autorizadas: Especifica as URLs na lista de bloqueio cujo conteúdo do navegador não é redirecionado para o cliente, mas renderizado no servidor.

O curinga * é permitido, mas não é permitido dentro do protocolo ou da parte do endereço de domínio da URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Não permitido: `http://*.xyz.com/`

Você pode obter uma granularidade melhor especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, apenas index.html estará na lista de bloqueio.

Configuração de proxy de redirecionamento de conteúdo do navegador

Esta configuração fornece opções de configuração para as configurações de proxy no VDA para redirecionamento de conteúdo do navegador. Se ativado com um endereço de proxy e número de porta válidos, URL PAC / WPAD ou configuração Direta/Transparente, o aplicativo Citrix Workspace tenta apenas a busca no servidor e a renderização no cliente.

Se desativado ou não configurado e usando um valor padrão, o aplicativo Citrix Workspace tenta a busca no cliente e a renderização no cliente.

Por padrão, esta configuração é Proibida.

Padrão permitido para um proxy explícito:

`http://<hostname/ip address\>:\<port\>`

Exemplo:

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

Padrões permitidos para arquivos PAC/WPAD:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

Exemplo: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

Exemplo: `http://10.10.10.10/configuration/pac/wpad.dat`

Padrões permitidos para proxies diretos ou transparentes:

Digite a palavra **DIRECT** na caixa de texto da política.

Substituições de chave de registro de redirecionamento de conteúdo do navegador

> **Aviso:**

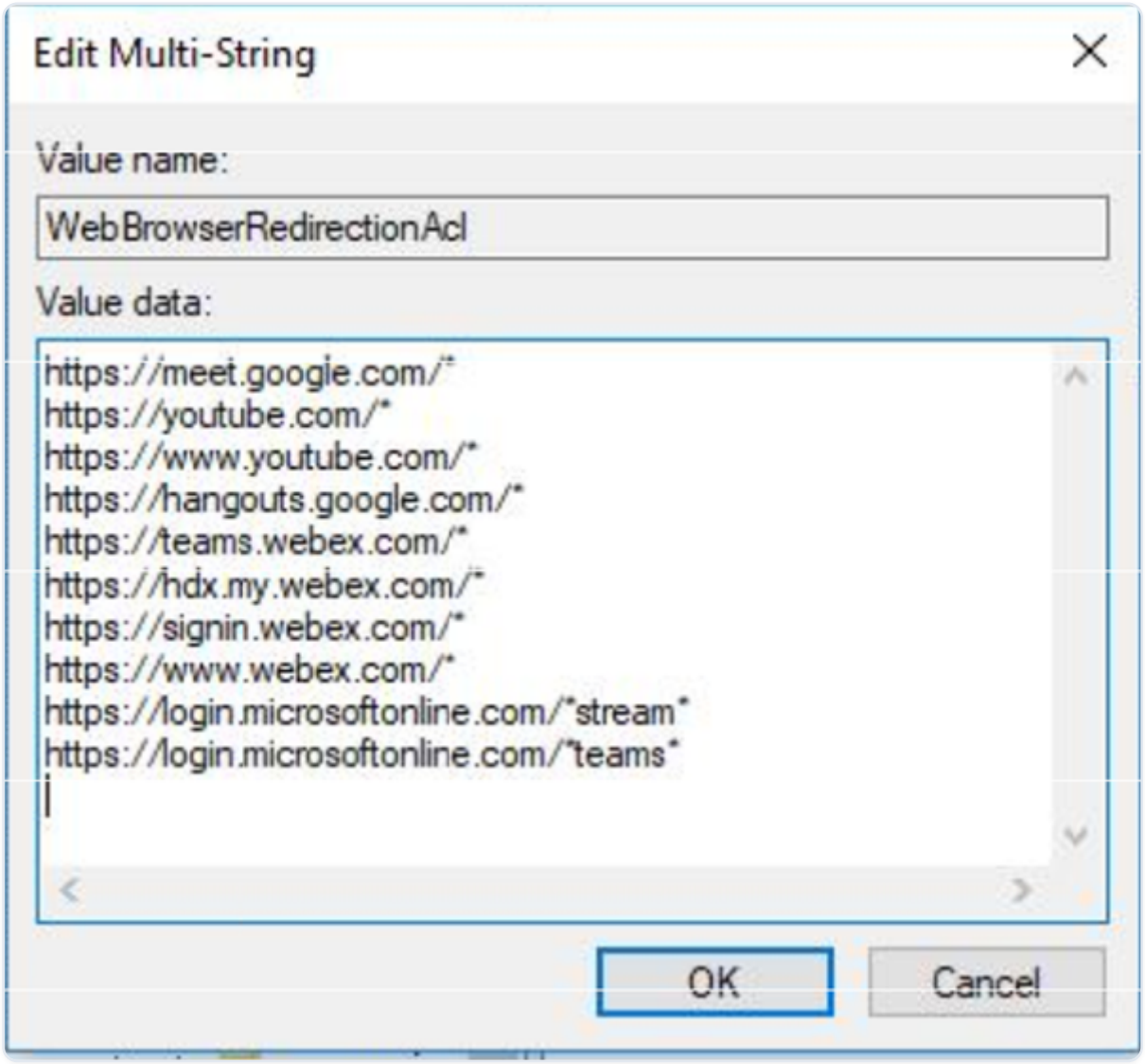
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> Opções de substituição de registros para configurações de política:

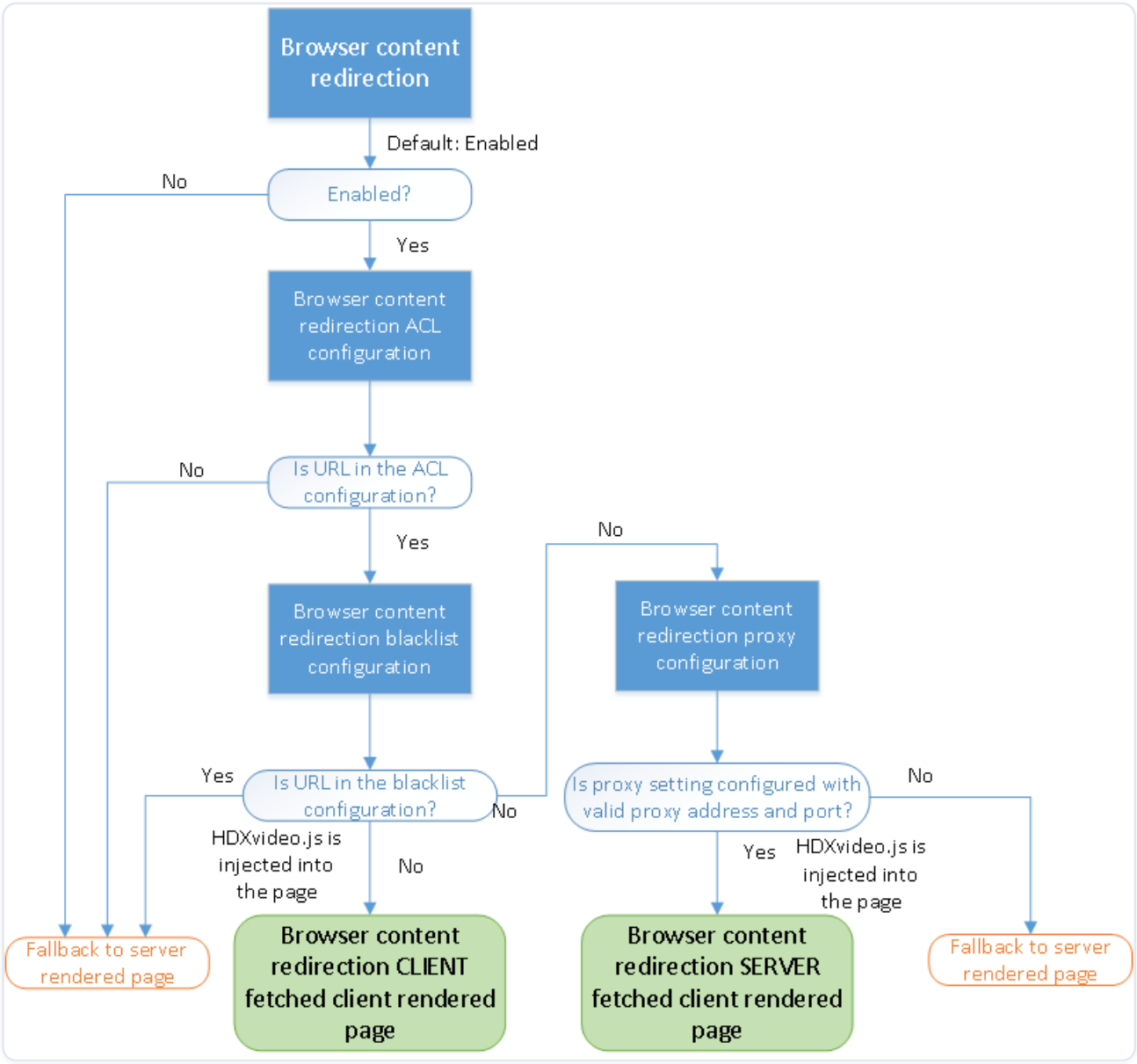
`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

NOME	TIPO	VALOR
WebBrowserRedirection	DWORD	1=Permitido, 0=Proibido
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` ou `http://10.10.10.10:8888`

NOME	TIPO	VALOR
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



Inserção de HDXVideo.js para redirecionamento de conteúdo do navegador



HdxVideo.js é injetado na página da web usando a extensão do Chrome de redirecionamento de conteúdo do navegador ou o Objeto Auxiliar do Navegador (BHO) do Internet Explorer. O BHO é um modelo de plug-in para o Internet Explorer. Ele fornece ganchos para APIs do navegador e permite que o plug-in acesse o Modelo de Objeto de Documento (DOM) da página para controlar a navegação.

O BHO decide se injeta o HdxVideo.js em uma determinada página. A decisão é baseada nas políticas administrativas mostradas no fluxograma anterior.

Depois que ele decide injetar o JavaScript e redirecionar o conteúdo do navegador para o cliente, a página da web fica em branco no navegador Internet Explorer no VDA. Definir **document.body.innerHTML** como vazio remove todo o corpo da página da web no VDA. A página está pronta para ser enviada ao cliente para ser exibida no navegador de sobreposição (Hdxbrowser.exe) no cliente.

Configurações de política de sensores do cliente

A seção **Sensores do Cliente** inclui configurações de política para controlar como as informações do sensor do dispositivo móvel são tratadas em uma sessão de usuário.

Permitir que aplicativos usem a localização física do dispositivo cliente

Esta configuração determina se os aplicativos em execução em uma sessão em um dispositivo móvel têm permissão para usar a localização física do dispositivo do usuário.

Por padrão, o uso de informações de localização é proibido

Quando esta configuração é proibida, as tentativas de um aplicativo de recuperar informações de localização retornam um valor de "permissão negada".

Quando esta configuração é permitida, um usuário pode proibir o uso de informações de localização negando uma solicitação do aplicativo Citrix Workspace™ para acessar a localização. Dispositivos Android e iOS solicitam na primeira vez que as informações de localização são solicitadas em cada sessão.

Ao desenvolver aplicativos hospedados que usam a configuração Permitir que aplicativos usem a localização física do dispositivo cliente, considere o seguinte:

- Certifique-se de que um aplicativo habilitado para localização não dependa da disponibilidade de informações de localização porque:
  - Um usuário pode não permitir o acesso às informações de localização.
  - A localização pode não estar disponível ou pode mudar enquanto o aplicativo está em execução.
  - Um usuário pode se conectar à sessão do aplicativo a partir de um dispositivo diferente que não oferece suporte a informações de localização.
- Um aplicativo habilitado para localização deve:
  - Ter o recurso de localização desativado por padrão.
  - Fornecer ao usuário uma opção para permitir ou desativar o recurso enquanto o aplicativo está em execução.
  - Forneça ao usuário uma opção para limpar os dados de localização que o aplicativo armazena em cache. (O aplicativo Citrix Workspace não armazena dados de localização em cache.)

- Um aplicativo habilitado para localização deve gerenciar a granularidade das informações de localização. Esse gerenciamento garante que os dados adquiridos sejam apropriados para a finalidade do aplicativo. Além disso, está em conformidade com os regulamentos em todas as jurisdições relevantes.
- Imponha uma conexão segura (por exemplo, usando TLS ou uma VPN) ao usar serviços de localização. Conecte o aplicativo Citrix Workspace a servidores confiáveis.
- Considere obter aconselhamento jurídico sobre o uso de serviços de localização.

Configurações de política da UI do desktop

A seção **Interface do Usuário da Área de Trabalho** inclui configurações de política que controlam efeitos visuais como papel de parede da área de trabalho, animações de menu e imagens de arrastar. Essas configurações de política ajudam a gerenciar a largura de banda usada em conexões de cliente. Você pode melhorar o desempenho do aplicativo em uma WAN limitando o uso da largura de banda.

> **Importante:**
>
> Não oferecemos suporte ao modo gráfico herdado e à Redireção de Composição da Área de Trabalho (DCR) nesta versão. Esta política é incluída apenas para compatibilidade com versões anteriores ao usar:
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Versões anteriores do VDA com Windows 7 e Windows 2008 R2.

Redirecionamento de Composição da Área de Trabalho

Essa configuração especifica se devem ser usados os recursos de processamento do seguinte para renderização gráfica local do DirectX, a fim de proporcionar aos usuários uma experiência de área de trabalho do Windows mais fluida:

- Unidade de processamento gráfico (GPU) no dispositivo do usuário
- Ou,
- Processador gráfico integrado (IGP) no dispositivo do usuário

Quando ativado, o **Redirecionamento de Composição da Área de Trabalho** oferece uma experiência Windows altamente responsiva, mantendo alta escalabilidade no servidor.

Por padrão, o **Redirecionamento de Composição da Área de Trabalho** está desativado.

Para desmarcar o **Redirecionamento de Composição da Área de Trabalho** e reduzir a largura de banda necessária nas sessões do usuário, selecione **Desativado** ao adicionar essa configuração a uma política.

Qualidade gráfica do Redirecionamento de Composição da Área de Trabalho

Essa configuração especifica a qualidade dos gráficos usados para o Redirecionamento de Composição da Área de Trabalho.

O padrão é Alto.

Escolha entre qualidade Alta, Média, Baixa ou Sem Perdas.

Papel de parede da área de trabalho

Essa configuração permite ou impede a exibição de papel de parede em sessões de usuário.

Por padrão, as sessões de usuário podem exibir papel de parede.

Para desmarcar o papel de parede da área de trabalho e reduzir a largura de banda necessária nas sessões de usuário, selecione **Proibido** ao adicionar essa configuração a uma política.

Animação de menu

Essa configuração permite ou impede a animação de menu em sessões de usuário.

Por padrão, a animação de menu é permitida.

A animação de menu é uma configuração de preferência pessoal da Microsoft para facilitar o acesso. Quando ativada, ela faz com que um menu apareça após um pequeno atraso, seja rolando ou esmaecendo. Um ícone de seta aparece na parte inferior do menu. O menu aparece quando você aponta para essa seta.

A animação de menu é ativada em uma área de trabalho se essa configuração de política estiver definida como **Permitido** e a configuração de preferência pessoal da Microsoft para animação de menu estiver ativada.

> **Observação:**

> As alterações na configuração de preferência pessoal da Microsoft para animação de menu afetam a área de trabalho. Considere que você configurou a área de trabalho para descartar as alterações quando a sessão termina. Nesse caso, um usuário que ativou as animações de menu pode não ter animação de menu em sessões subsequentes. Para usuários que exigem animação de menu, ative a configuração da Microsoft na imagem principal da área de trabalho ou garanta que a área de trabalho retenha as alterações do usuário.

Visualizar conteúdo da janela ao arrastar

Esta configuração permite ou impede a exibição do conteúdo da janela ao arrastar uma janela pela tela.

Por padrão, a visualização do conteúdo da janela é permitida.

Quando definido como **Permitido**, a janela inteira parece se mover quando você a arrasta. Quando definido como **Proibido**, apenas o contorno da janela parece se mover até que você a solte.

Configurações de política de monitoramento do usuário final

A seção **Monitoramento do Usuário Final** inclui configurações de política para medir o tráfego da sessão.

Cálculo de ida e volta do ICA®

Esta configuração determina se os cálculos de ida e volta do ICA são feitos para conexões ativas.

Por padrão, os cálculos para conexões ativas estão habilitados.

Por padrão, cada início de medição de ida e volta do ICA é atrasado. Esse atraso ocorre até que algum tráfego que indique interação do usuário aconteça. Esse atraso pode ser de duração indefinida e foi projetado para evitar que a medição de ida e volta do ICA seja a única razão para o tráfego do ICA.

Intervalo de cálculo de ida e volta do ICA

Esta configuração especifica a frequência, em segundos, com que os cálculos de ida e volta do ICA são realizados.

Por padrão, o tempo de ida e volta do ICA é calculado a cada 15 segundos.

Cálculos de ida e volta do ICA para conexões ociosas

Esta configuração determina se os cálculos de ida e volta do ICA são feitos para conexões ociosas.

Por padrão, os cálculos não são realizados para conexões ociosas.

Por padrão, cada início de medição de ida e volta do ICA é atrasado. Esse atraso ocorre até que algum tráfego que indique interação do usuário aconteça. Esse atraso pode ser de duração indefinida e foi projetado para evitar que a medição de ida e volta do ICA seja a única razão para o tráfego do ICA.

Configurações de política de Redirecionamento de Arquivos

A seção **Redirecionamento de Arquivos** inclui configurações de política relacionadas ao mapeamento de unidades cliente e otimização de unidades cliente.

Conectar automaticamente unidades cliente

Esta configuração permite ou impede a conexão automática de unidades cliente quando os usuários fazem logon.

Por padrão, a conexão automática é permitida.

Ao adicionar esta configuração a uma política, certifique-se de habilitar as configurações para os tipos de unidade que você deseja conectar automaticamente. Por exemplo, para permitir a conexão automática de unidades de CD-ROM dos usuários, configure esta configuração e a configuração **Unidades ópticas cliente**.

As seguintes configurações de política estão relacionadas:

- **Redirecionamento de unidade cliente**
- **Unidades de disquete cliente**
- **Unidades ópticas cliente**
- **Unidades fixas cliente**
- **Unidades de rede cliente**
- **Unidades removíveis cliente**

Redirecionamento de unidade cliente

Esta configuração habilita ou desabilita o redirecionamento de arquivos para e de unidades no dispositivo do usuário.

Por padrão, o redirecionamento de arquivos está habilitado.

> **Observação:**

> As configurações de política de redirecionamento de unidade cliente não se aplicam a unidades mapeadas para sessões usando redirecionamento USB genérico.

> Quando habilitado, os usuários podem salvar arquivos em todas as suas unidades cliente. Quando desabilitado, todo o redirecionamento de arquivos é impedido. Esta configuração é aplicável independentemente do estado das configurações individuais de redirecionamento de arquivos. As configurações individuais de redirecionamento de arquivos incluem Unidades de disquete do cliente e Unidades de rede do cliente.

As seguintes configurações de política estão relacionadas:

- **Unidades de disquete do cliente**
- **Unidades ópticas do cliente**
- **Unidades fixas do cliente**
- **Unidades de rede do cliente**
- **Unidades removíveis do cliente**

Unidades fixas do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades fixas no dispositivo do usuário.

Por padrão, o acesso a unidades fixas do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades fixas do cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente, independentemente do estado da configuração **Unidades fixas do cliente**.

Configure a configuração **Conectar automaticamente unidades cliente** para garantir que as unidades fixas sejam conectadas automaticamente quando os usuários fizerem logon.

Unidades de disquete do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades de disquete no dispositivo do usuário.

Por padrão, o acesso a unidades de disquete do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades de disquete do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente, independentemente do estado da configuração **Unidades de disquete do cliente**.

Para garantir que as unidades de disquete sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades de cliente automaticamente**.

Unidades de rede do cliente

Esta configuração permite ou impede que os usuários acessem e salvem arquivos em unidades de rede (remotas) através do dispositivo do usuário.

Por padrão, o acesso a unidades de rede do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades de rede do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Esta configuração é aplicável independentemente do estado da configuração **Unidades de rede do cliente**.

Para garantir que as unidades de rede sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades de cliente automaticamente**.

Unidades ópticas do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos nos seguintes locais:

- CD-ROM no dispositivo do usuário
- DVD-ROM no dispositivo do usuário
- Unidades BD-ROM no dispositivo do usuário.

Por padrão, o acesso a unidades ópticas do cliente é permitido.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja presente e definida como **Permitido**. Se essas configurações estiverem desabilitadas, as unidades ópticas do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Essa configuração é aplicável independentemente do estado da configuração **Unidades ópticas do cliente**.

Para garantir que as unidades ópticas sejam conectadas automaticamente quando os usuários fizerem logon, configure a configuração **Conectar unidades cliente automaticamente**.

Unidades removíveis do cliente

Esta configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades USB no dispositivo do usuário.

Por padrão, o acesso a unidades removíveis do cliente é permitido.

Ao adicionar esta configuração a uma política, verifique se a configuração **Redirecionamento de unidade cliente** está presente e definida como Permitido. Se essas configurações estiverem desabilitadas, as unidades removíveis do cliente não serão mapeadas e os usuários não poderão acessá-las manualmente. Essa configuração é aplicável independentemente do estado da configuração **Unidades removíveis do cliente**.

Configure a configuração **Conectar unidades cliente automaticamente** para garantir que as unidades removíveis sejam conectadas automaticamente quando os usuários fizerem logon.

Redirecionamento do host para o cliente

Esta configuração habilita ou desabilita associações de tipo de arquivo para URLs e alguns conteúdos de mídia a serem abertos no dispositivo do usuário. Quando desabilitado, o conteúdo é aberto no servidor.

Por padrão, a associação de tipo de arquivo está desabilitada.

Esses tipos de URL são abertos localmente quando você habilita esta configuração:

- HTTP
- HTTPS
- Real Player e QuickTime (RTSP)
- Real Player e QuickTime (RTSPU)
- Real Player legado (PNM)
- Microsoft Media Server (MMS)

Preservar letras de unidade do cliente

Esta configuração habilita ou desabilita o mapeamento de unidades do cliente para a mesma letra de unidade na sessão.

Por padrão, as letras de unidade do cliente não são preservadas.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido.

Acesso somente leitura à unidade do cliente

Esta configuração permite ou impede que usuários e aplicativos façam o seguinte:

- Criar arquivos em unidades de cliente mapeadas
- Alterar arquivos em unidades de cliente mapeadas
- Alterar pastas em unidades de cliente mapeadas

Por padrão, arquivos e pastas em unidades de cliente mapeadas podem ser alterados.

Se definido como Habilitado, arquivos e pastas são acessíveis com permissões somente leitura.

Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade do cliente** esteja presente e definida como Permitido.

Redirecionamento de pasta especial

Esta configuração permite ou impede que usuários do aplicativo Citrix Workspace™ e do Web Interface vejam suas pastas especiais locais de Documentos e Área de Trabalho a partir de uma sessão.

Por padrão, o redirecionamento de pasta especial é permitido.

Essa configuração impede que quaisquer objetos filtrados por meio de uma política tenham redirecionamento de pasta especial, independentemente das configurações existentes em outros locais. Quando essa configuração é proibida, quaisquer configurações relacionadas especificadas para StoreFront™, Web Interface ou Citrix Workspace app são ignoradas.

Para definir quais usuários podem ter redirecionamento de pasta especial, selecione **Permitido** e inclua essa configuração em uma política filtrada nos usuários que você deseja que tenham esse recurso. Essa configuração substitui todas as outras configurações de redirecionamento de pasta especial.

As configurações de política que impedem os usuários de acessar ou salvar arquivos em seus discos rígidos locais também impedem que o redirecionamento de pasta especial funcione. Essa situação ocorre porque o redirecionamento de pasta especial deve interagir com o dispositivo do usuário.

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Unidades fixas do cliente** esteja presente e definida como Permitido.

Políticas de transferência de arquivos

Por padrão, a transferência de arquivos está habilitada. Use o Web Studio para alterar essas políticas, localizadas em **User setting - ICA\File Redirection**. Considere o seguinte ao usar políticas de transferência de arquivos:

- **Transferência de arquivos para o aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários transfiram arquivos entre uma sessão do Citrix Virtual Apps and Desktops e seus dispositivos.
- **Carregar arquivo para o aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários carreguem arquivos de seus dispositivos para uma sessão do Citrix Virtual Apps and Desktops.
- **Baixar arquivo para o aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários baixem arquivos de uma sessão do Citrix Virtual Apps and Desktops para seus dispositivos.

> **Observação:**
>
> As políticas de transferência de arquivos são aplicáveis apenas para o aplicativo Citrix Workspace para HTML5 e para o aplicativo Citrix Workspace para Chrome OS.

Usar gravações assíncronas

Essa configuração habilita ou desabilita as gravações assíncronas em disco.

Por padrão, as gravações assíncronas estão desabilitadas.

As gravações assíncronas em disco podem melhorar a velocidade das transferências de arquivos e a gravação em discos de cliente em WANs, que são tipicamente caracterizadas por alta largura de banda e alta latência. No entanto, se houver uma falha de conexão ou de disco, o arquivo ou arquivos do cliente que estão sendo gravados podem terminar em um estado indefinido. Se esse estado indefinido ocorrer, uma janela pop-up informa o usuário sobre os arquivos afetados. O usuário pode então tomar medidas corretivas, como reiniciar uma transferência de arquivo interrompida na reconexão ou quando a falha do disco for corrigida.

A Citrix® recomenda habilitar gravações assíncronas em disco apenas para usuários que exigem conectividade remota com boa velocidade de acesso a arquivos e que possam recuperar facilmente arquivos ou dados perdidos se houver uma falha de conexão ou de disco.

Ao adicionar esta configuração a uma política, verifique se a configuração **Redirecionamento de unidade cliente** está presente e definida como Permitido. Se esta configuração estiver desabilitada, as gravações assíncronas não ocorrem.

Configurações de política de gráficos

A seção **Gráficos** inclui configurações de política para controlar como as imagens são tratadas nas sessões do usuário.

Permitir compressão visualmente sem perdas

Essa configuração permite que a compressão visualmente sem perdas seja usada em vez da compressão verdadeiramente sem perdas para gráficos. A compressão visualmente sem perdas melhora o desempenho em relação à verdadeiramente sem perdas, mas tem uma pequena perda que é imperceptível à vista. Essa configuração altera a forma como os valores da configuração Qualidade visual são usados.

Por padrão, essa configuração está desabilitada.

Indicador de status gráfico

Essa configuração configura o indicador de status gráfico para ser executado na sessão do usuário. Essa ferramenta permite que o usuário veja informações sobre o modo gráfico ativo. As informações incluem detalhes sobre codec de vídeo, codificação de hardware, qualidade de imagem e monitores em uso para a sessão. Com o indicador de status gráfico, o usuário também pode habilitar ou desabilitar o modo pixel-perfect.

As versões do Citrix Virtual Apps and Desktops™ 2103 e posteriores incluem um controle deslizante de qualidade de imagem para ajudar o usuário a encontrar o equilíbrio certo entre qualidade de imagem e interatividade.

As versões do Citrix Virtual Apps and Desktops 2109 e posteriores incluem funcionalidade para configurar um layout de exibição virtual por meio de uma interface de usuário iniciada usando o indicador de status gráfico.

O indicador de status gráfico substitui a ferramenta de indicador sem perdas de versões anteriores. Essa política habilita o indicador sem perdas para as versões 7.16 a 1809 do Citrix Virtual Apps and Desktops.

Compartilhamento de tela

Essa configuração permite que os usuários compartilhem suas sessões, incluindo conteúdo da tela, teclados e mouses, com outros usuários.

Por padrão, a configuração está desabilitada.

O VDA tenta usar portas do intervalo de portas TCP para trocar dados, começando com a porta mais baixa e incrementando a cada conexão subsequente. A porta lida com tráfego de entrada e saída.

Por padrão, o intervalo de portas TCP é definido como 52525-52625.

A porta usada para compartilhamento de tela deve ser adicionada à lista de exceções do firewall. Essa opção é mostrada como uma caixa de seleção ao instalar o VDA. Por padrão, essa opção não está marcada.

Limite de memória de exibição

Esta configuração especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão.

Por padrão, o limite de memória de exibição é de 65.536 kilobytes.

Especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão. Especifique um valor em kilobytes de 128 a 4.194.303. O valor máximo de 4.194.303 não limita a memória de exibição. Por padrão, a memória de exibição é de 65.536 kilobytes. Usar maior profundidade de cor e maior resolução para conexões requer mais memória. No modo gráfico legado, se o limite de memória for atingido, a exibição degrada de acordo com a configuração "Preferência de degradação do modo de exibição".

Para conexões que exigem maior profundidade de cor e maior resolução, aumente o limite. Calcule a memória máxima necessária usando a equação:

Profundidade da memória em bytes = (profundidade-de-cor-em-bits-por-pixel) / 8) x (resolução-vertical-em-pixels) x (resolução-horizontal-em-pixels).

Por exemplo, considere um cenário com profundidade de cor de 32, resolução vertical de 600 e resolução horizontal de 800. Neste caso, a memória máxima necessária é (32 / 8) x (600) x (800) = 1.920.000 bytes, o que resulta em um limite de memória de exibição de 1920 KB.

Profundidades de cor diferentes de 32 bits estão disponíveis apenas se a configuração da política de modo gráfico legado estiver ativada.

O HDX™ aloca apenas a quantidade de memória de exibição necessária para cada sessão. Assim, se apenas alguns usuários exigirem mais do que o padrão, não haverá impacto negativo na escalabilidade ao aumentar o limite de memória de exibição.

Preferência de degradação do modo de exibição

> **Observação:**
>
> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica apenas quando a configuração da política de modo gráfico legado está ativada.

> Quando o limite de memória de exibição da sessão é atingido, esta configuração especifica se a profundidade de cor ou a resolução degrada primeiro.

Por padrão, a profundidade de cor é degradada primeiro.

Quando o limite de memória da sessão é atingido, você pode reduzir a qualidade das imagens exibidas. Você pode reduzir essa qualidade escolhendo se a profundidade de cor ou a resolução é degradada primeiro. Quando a profundidade de cor é degradada primeiro, as imagens exibidas usam menos cores. Quando a resolução é degradada primeiro, as imagens exibidas usam menos pixels por polegada.

Para notificar os usuários quando a profundidade de cor ou a resolução for degradada, configure a configuração Notificar usuário quando o modo de exibição for degradado.

Visualização dinâmica de janelas

Esta configuração habilita ou desabilita a exibição de janelas contínuas em:

- Flip-
- Flip 3D
- Visualização da barra de tarefas
- Windows Peek

OPÇÃO DE VISUALIZAÇÃO DO WINDOWS AERO	DESCRIÇÃO
Visualização da Barra de Tarefas	Quando o usuário passa o mouse sobre o ícone da janela na barra de tarefas, uma imagem dessa janela aparece acima da barra de tarefas.
Windows Peek	Quando o usuário passa o mouse sobre uma imagem de visualização da barra de tarefas,

OPÇÃO DE VISUALIZAÇÃO DO WINDOWS AERO	DESCRIÇÃO
	uma imagem em tamanho real da janela aparece na tela.
Flip	Quando o usuário pressiona ALT+TAB, pequenos ícones de visualização são mostrados para cada janela aberta.
Flip 3D	Quando o usuário pressiona a tecla TAB+logotipo do Windows, imagens grandes das janelas abertas são exibidas em cascata na tela.

Por padrão, esta configuração está habilitada.

Cache de imagem

> **Observação:**

> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

> Esta configuração habilita ou desabilita o armazenamento em cache e a recuperação de seções de imagens em sessões. O armazenamento em cache de imagens em seções e a recuperação dessas seções quando necessário proporciona o seguinte:

- Rolagem mais suave no dispositivo do usuário
- Reduz a quantidade de dados transmitidos pela rede no dispositivo do usuário
- Reduz o processamento necessário no dispositivo do usuário

Por padrão, a configuração de cache de imagem está habilitada.

> **Observação:**

> A configuração de cache de imagem controla como as imagens são armazenadas em cache e recuperadas. A configuração não controla se as imagens são armazenadas em cache. As

imagens são armazenadas em cache se a configuração do modo gráfico herdado estiver habilitada.

Modo gráfico herdado - não suportado. Apenas para compatibilidade com versões anteriores

Importante:

Não oferecemos suporte ao modo gráfico herdado e à Redireção de Composição da Área de Trabalho (DCR) nesta versão. Esta política é incluída apenas para compatibilidade com versões anteriores ao usar XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores do VDA com Windows 7 e Windows 2008 R2.

Esta configuração desabilita a experiência gráfica rica. Use esta configuração para reverter para a experiência gráfica herdada, reduzindo o consumo de largura de banda em uma conexão WAN ou móvel. As reduções de largura de banda introduzidas no XenApp e XenDesktop 7.13 tornam este modo obsoleto.

Por padrão, esta configuração está desabilitada e os usuários recebem a experiência gráfica rica.

O modo gráfico herdado é suportado nos seguintes:

- Windows 7
- VDAs do Windows Server 2008 R2.

O modo gráfico herdado não é compatível com o seguinte:

- Windows 8.x e 10
- Windows Server 2012, 2012 R2 e 2016.

Consulte CTX202687 para obter mais informações sobre como otimizar modos gráficos e políticas no XenApp e XenDesktop 7.6 FP3 ou superior.

Profundidade de cor máxima permitida

Observação:

> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

> Esta configuração especifica a profundidade de cor máxima permitida para uma sessão.

Por padrão, a profundidade de cor máxima permitida é de 32 bits por pixel.

Esta configuração se aplica apenas a drivers e conexões Thinwire. Ela não se aplica a VDAs que têm um driver não ThinWire como driver de vídeo principal. Esses VDAs são VDAs que usam um driver Windows Display Driver Model (WDDM) como driver de vídeo principal. Para VDAs de SO de sessão única que usam um driver WDDM como driver de vídeo principal, como o Windows 8, esta configuração não tem efeito. Para VDAs de SO de múltiplas sessões do Windows que usam um driver WDDM, como o Windows Server 2019, esta configuração pode impedir que os usuários se conectem ao VDA.

Definir uma alta profundidade de cor requer mais memória. Para degradar a profundidade de cor quando o limite de memória for atingido, configure a configuração **Preferência de degradação do modo de exibição**. Quando a profundidade de cor é degradada, as imagens exibidas usam menos cores.

Notificar o usuário quando o modo de exibição for degradado

> **Observação:**

> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

> Esta configuração exibe uma breve explicação ao usuário quando a profundidade de cor ou a resolução é degradada.

Por padrão, a notificação de usuários está desabilitada.

Otimizar para carga de trabalho de gráficos 3D

Esta configuração define as configurações padrão apropriadas que melhor se adequam a cargas de trabalho graficamente intensas. Habilite esta configuração para usuários cuja carga de trabalho se concentra em aplicativos graficamente intensos. Aplique esta política apenas em casos onde

uma GPU esteja disponível para a sessão. Quaisquer outras configurações que substituam explicitamente as configurações padrão definidas por esta política terão precedência.

Por padrão, a otimização para a carga de trabalho de gráficos 3D está desabilitada.

Enfileiramento e descarte

> **Observação:**
>
> Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.
>
> Esta configuração descarta imagens enfileiradas que são substituídas por outra imagem.

Por padrão, o enfileiramento e descarte está habilitado.

Esta configuração melhora a resposta quando os gráficos são enviados para o dispositivo do usuário. A configuração desta opção pode fazer com que as animações fiquem instáveis devido a quadros perdidos.

Usar codec de vídeo para compressão

Permite o uso de um codec de vídeo para compactar gráficos quando a decodificação de vídeo está disponível no endpoint. Quando **Para a tela inteira** é escolhido, o codec de vídeo é aplicado como o codec padrão para todos. Quando **Para regiões em mudança ativa** é selecionado, o codec de vídeo é usado para áreas onde há mudança constante na tela; outros dados usam compactação de imagem estática e cache de bitmap. Quando a decodificação de vídeo não está disponível no endpoint, ou quando você especifica **Não usar codec de vídeo**, uma combinação de compactação de imagem estática e cache de bitmap é usada. Quando **Usar quando preferencial** é selecionado, o sistema escolhe com base em vários fatores. Os resultados podem variar entre as versões à medida que o método de seleção é aprimorado.

Selecione **Usar quando preferencial** para permitir que o sistema faça o seu melhor para escolher as configurações apropriadas para o cenário atual.

Selecione **Para a tela inteira** para otimizar a experiência do usuário e a largura de banda, especialmente em casos de uso intenso de vídeo renderizado por servidor e gráficos 3D.

Selecione **Para regiões em mudança ativa** para otimizar o desempenho de vídeo, especialmente em baixa largura de banda, mantendo a escalabilidade para conteúdo estático e em mudança lenta. Esta configuração é suportada em implantações multi-monitor.

Selecione **Não usar codec de vídeo** para otimizar a carga da CPU do servidor e para casos que não possuem muitos vídeos renderizados por servidor ou outros aplicativos graficamente intensos.

O padrão é **Usar quando preferencial**.

Usar codificação de hardware para vídeo

Essa configuração permite o uso de hardware gráfico, se disponível, para compactar elementos da tela com o codec de vídeo. Se esse hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software.

A opção padrão para essa configuração de política é **Habilitado**.

Vários monitores são suportados.

Qualquer aplicativo Citrix Workspace™ que suporte decodificação de vídeo pode ser usado com codificação de hardware.

NVIDIA

Para GPUs NVIDIA GRID, a codificação de hardware é suportada com VDAs para SO de múltiplas sessões e SO de sessão única.

As GPUs NVIDIA devem suportar a codificação de hardware NVENC. Consulte NVIDIA video codec SDK para obter uma lista de GPUs suportadas.

NVIDIA GRID requer a versão de driver 3.1 ou superior. NVIDIA Quadro requer a versão de driver 362.56 ou superior. A Citrix recomenda drivers do branch NVIDIA Release R361.

O texto sem perdas não é compatível com a codificação de hardware NVENC. Se você habilitou o texto sem perdas, o texto sem perdas tem prioridade sobre a codificação de hardware NVENC.

O uso seletivo do codec de hardware H.264 para regiões em constante mudança é suportado.

A compressão visualmente sem perdas (YUV 4:4:4) é suportada. A compressão visualmente sem perdas (configuração de política gráfica, Permitir compressão visualmente sem perdas) requer o aplicativo Citrix Workspace 1808 ou superior ou o Citrix Receiver para Windows 4.5 ou superior.

INTEL

Para processadores gráficos Intel Iris Pro, a codificação de hardware é suportada com VDAs para SO de sessão única e SO de múltiplas sessões.

Os processadores gráficos Intel Iris Pro da família de processadores Intel Broadwell e posteriores são suportados. A versão 1.0 do Intel Remote Displays SDK é necessária e pode ser baixada do site da Intel: Remote Displays SDK.

O texto sem perdas é suportado apenas quando a política de codec de vídeo está definida para a tela inteira e a política **Otimizar para carga de trabalho de gráficos 3D** está desabilitada.

Visualmente sem perdas (YUV 4:4:4) não é suportado.

O codificador Intel oferece uma boa experiência do usuário para até oito sessões de codificação (por exemplo, um usuário usando oito monitores ou oito usuários usando um monitor cada). Se mais de oito sessões de codificação forem necessárias, verifique quantos monitores a máquina virtual se conecta. O administrador decide configurar esta definição de política por usuário ou por máquina para manter uma boa experiência do usuário.

AMD

Para AMD, a codificação de hardware é suportada com VDAs para um SO de sessão única.

As GPUs AMD devem suportar o SDK RapidFire. Por exemplo, as GPUs AMD Radeon Pro ou FirePro.

Para que a codificação funcione, instale os drivers AMD mais recentes. Você pode baixar esses drivers em `<https://www.amd.com/en/support>`.

O texto sem perdas não é compatível com a codificação de hardware AMD. Se você ativou o texto sem perdas, o texto sem perdas tem prioridade sobre a codificação de hardware AMD.

O uso seletivo do codec de hardware H.264 para regiões em mudança ativa é suportado.

Configurações de política do Framehawk

> **Importante:**

> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais compatível. Em vez disso, use Thinwire com transporte adaptável ativado.

> A seção **Framehawk** inclui configurações de política que habilitam e configuram o canal de exibição Framehawk no servidor.

CANAL DE EXIBIÇÃO FRAMEHAWK

Quando ativado, o servidor tenta usar o canal de exibição Framehawk para os gráficos e o acesso remoto de entrada do usuário. Esse canal de exibição usa UDP para fornecer uma melhor experiência do usuário em redes com alta perda e características de latência. No entanto, ele também pode usar mais recursos do servidor e largura de banda do que outros modos gráficos.

Por padrão, o canal de exibição Framehawk está desativado.

INTERVALO DE PORTAS DO CANAL DE EXIBIÇÃO FRAMEHAWK

Essa configuração de política especifica o intervalo de números de porta UDP que o VDA usa para trocar dados do canal de exibição Framehawk com o dispositivo do usuário. Os números de porta estão no formato *número de porta mais baixo ou número de porta mais alto*. O VDA tenta usar cada porta, começando com o número de porta mais baixo e incrementando para cada tentativa subsequente. A porta lida com o tráfego de entrada e saída.

Por padrão, o intervalo de portas é 3224,3324.

Configurações de política de multimídia

A seção **Multimídia** inclui configurações de política para gerenciar streaming de áudio e vídeo HTML5 e Windows em sessões de usuário.

> **Aviso**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Políticas de multimídia

Por padrão, todas as políticas de multimídia definidas no Delivery Controller™ são armazenadas nestes registros:

Políticas de máquina:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

Políticas de usuário:

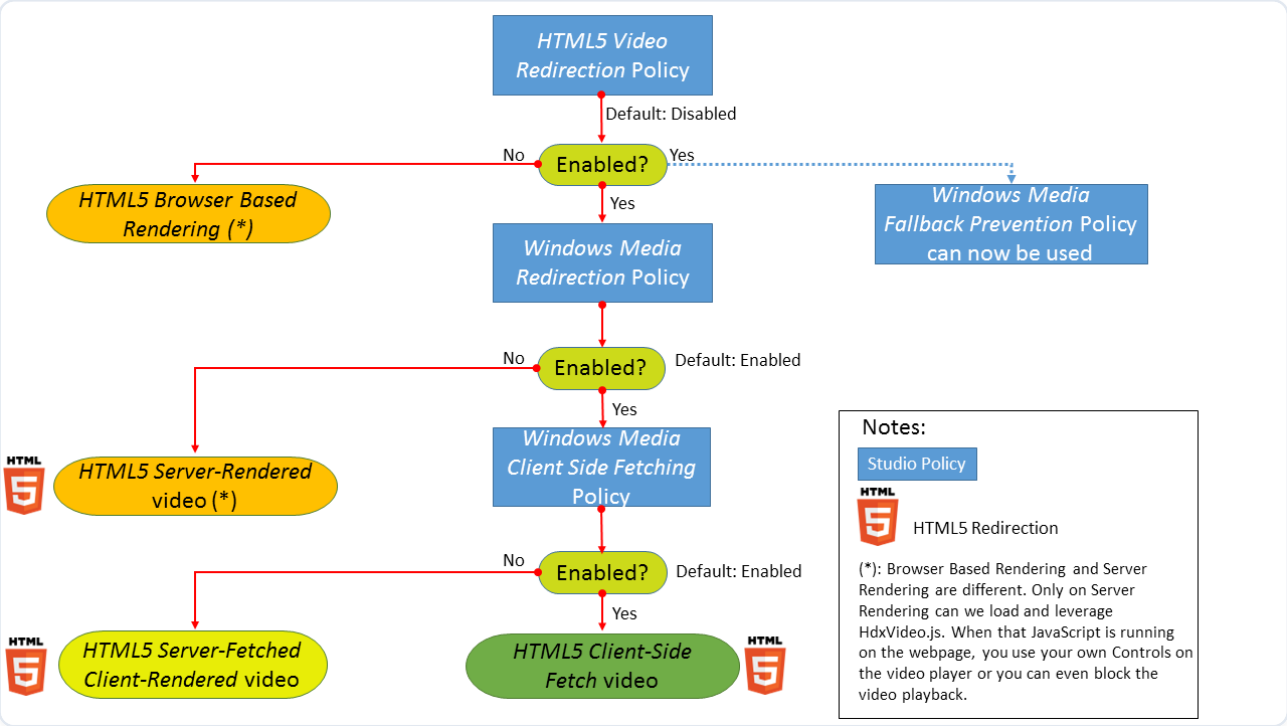
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

Para localizar o ID da sessão do usuário atual, execute o comando **qwinsta** na linha de comando do Windows.

Redirecionamento de vídeo HTML5

Controla e otimiza a forma como os servidores Citrix Virtual Apps and Desktops™ entregam conteúdo web multimídia HTML5 aos usuários.

Por padrão, esta configuração está desabilitada.



Nesta versão, este recurso está disponível apenas para páginas da web controladas. Ele requer a adição de JavaScript às páginas da web onde o conteúdo multimídia HTML5 está disponível, por exemplo, vídeos em um site de treinamento interno.

Para configurar o redirecionamento de vídeo HTML5:

1. Copie o arquivo, **HdxVideo.js**, de %Program Files%/Citrix/ICA Service/HTML5 Video Redirection na instalação do VDA para o local da sua página da web interna.
2. Insira esta linha em sua página da web (se sua página da web tiver outros scripts, inclua **HdxVideo.js** antes desses scripts): `<script src="HdxVideo.js" type="text/javascript"\></script>`

Nota: Se HdxVideo.js não estiver no mesmo local que sua página da web, use o atributo **src** para especificar o caminho completo para ele.

Considere que o JavaScript não é adicionado às suas páginas da web controladas e o usuário reproduz um vídeo HTML5. Neste caso, o Citrix Virtual Apps and Desktops assume o padrão de renderização do lado do servidor.

Para que o redirecionamento de vídeos HTML5 funcione, permita ***Redirecionamento de Mídia do Windows***. Esta política é obrigatória para Server Fetch Client Render e necessária para Client Side Fetching. Client Side Fetching, por sua vez, também exige que *a busca de conteúdo do lado do cliente do Windows Media* seja Permitida.

O Microsoft Edge não oferece suporte a este recurso.

HdxVideo.js substitui os controles do reprodutor HTML5 do navegador pelos seus próprios. Para verificar se a política de redirecionamento de vídeo HTML5 está em vigor em um determinado site, compare os controles do reprodutor com um cenário em que a política de **redirecionamento de vídeo HTML5** é Proibida:

(Controles personalizados do Citrix quando a política é Permitida)



(Controles nativos da página da web quando a política é Proibida ou não configurada)



Os seguintes controles de vídeo são suportados:

- reproduzir
- pausar
- procurar
- repetir
- áudio
- tela cheia

Você pode visualizar uma página de teste de redirecionamento de vídeo HTML5.

TLS, REDIRECIONAMENTO DE VÍDEO HTML5 E REDIRECIONAMENTO DE CONTEÚDO DO NAVEGADOR

Você pode usar o redirecionamento de vídeo HTML5 para:

- Redirecionar vídeos de sites HTTPS
- Ou

- Redirecionamento de conteúdo do navegador para redirecionar o site inteiro

O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX (WebSocketService.exe) em execução no VDA. O Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX no armazenamento de certificados no VDA gera dois certificados personalizados para:

- Realizar o redirecionamento de vídeo
- Manter a integridade TLS da página da web

HdxVideo.js usa Secure WebSockets para se comunicar com WebSocketService.exe em execução no VDA. Este processo é executado como uma conta de Sistema Local e realiza a terminação SSL e o mapeamento de sessão do usuário.

WebSocketService.exe está escutando na porta 9001 de 127.0.0.1.

Limitar qualidade de vídeo

Esta configuração se aplica apenas ao Windows Media e não ao HTML5. Ela exige que você habilite a **Otimização para redirecionamento multimídia do Windows Media sobre WAN**.

Esta configuração especifica o nível máximo de qualidade de vídeo permitido para uma conexão HDX™. Quando configurada, a qualidade máxima de vídeo é limitada ao valor especificado, garantindo que a Qualidade de Serviço (QoS) multimídia seja mantida em um ambiente.

Por padrão, esta configuração não está configurada.

Para limitar o nível máximo de qualidade de vídeo permitido, escolha uma das seguintes opções:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Reproduzir vários vídeos simultaneamente no mesmo servidor consome grandes quantidades de recursos e pode afetar a escalabilidade do servidor.

Redirecionamento do Microsoft Teams

Esta configuração permite a otimização do Microsoft Teams, com base na tecnologia HDX.

Se esta política estiver habilitada e você estiver usando uma versão compatível do aplicativo Citrix Workspace™, esta chave de registro é definida como **1** no VDA. O aplicativo Microsoft Teams lê a chave para carregar no modo VDI. Observe que não é necessário definir a chave de registro manualmente.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Nome: MSTeamsRedirSupport

Valor: DWORD (1 - ativado, 0 - desativado)

> **Observação:**

> Considere que você está usando VDAs versão 1906.2 ou posterior com versões mais antigas do Controller, que não têm a política disponível no Web Studio. Um exemplo de uma versão mais antiga do controller é a versão 7.15. Nesse caso, a otimização HDX é habilitada por padrão no VDA. Se a versão do aplicativo Workspace for 1907 ou posterior, o Microsoft Teams será iniciado no modo otimizado. Para obter informações sobre ressalvas na mistura de Controllers LTSR 7.15 e VDAs CR, consulte o artigo da Central de Conhecimento CTX205549.

> Nesse caso, para desabilitar o recurso para usuários específicos, você pode substituir a configuração do registro. Substitua as configurações do registro usando uma política de grupo para aplicar um script de logon à unidade organizacional do usuário.

> Por padrão, o redirecionamento do Microsoft Teams está habilitado.

Conferência multimídia

Essa configuração permite ou impede o uso da tecnologia de redirecionamento otimizado de webcam por aplicativos de videoconferência.

Por padrão, o suporte a videoconferência é permitido.

Ao adicionar essa configuração a uma política, verifique se a configuração de **redirecionamento do Windows Media** está presente e definida como **Permitido** (o padrão).

Ao usar a **Conferência multimídia**, verifique se as seguintes condições são atendidas:

- Drivers fornecidos pelo fabricante para a webcam usada para conferência multimídia estão instalados no cliente.
- Conecte a webcam ao dispositivo do usuário antes de iniciar uma sessão de videoconferência. O servidor usa apenas uma webcam instalada por vez. Se várias webcams estiverem instaladas no dispositivo do usuário, o servidor tentará usar cada webcam em sucessão. Essa tentativa continua até que uma sessão de videoconferência seja criada com sucesso.

Essa política não é necessária ao redirecionar a webcam usando o redirecionamento USB genérico. Nesse caso, instale os drivers da webcam no VDA.

Otimização para redirecionamento multimídia do Windows Media via WAN

Essa configuração se aplica apenas ao Windows Media e não ao HTML5. A configuração permite o seguinte:

- Transcodificação multimídia em tempo real
- Permite o streaming de mídia de áudio e vídeo para dispositivos móveis em redes degradadas
- Aprimora a experiência do usuário melhorando a forma como o conteúdo do Windows Media é entregue em uma WAN.

Por padrão, a entrega de conteúdo do Windows Media pela WAN é otimizada.

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento de Mídia do Windows** esteja presente e definida como **Permitido**.

Quando essa configuração está habilitada, a transcodificação multimídia em tempo real é implantada automaticamente conforme necessário para habilitar o streaming de mídia. Além disso, proporciona uma experiência de usuário perfeita mesmo em condições de rede extremas.

Usar GPU para otimizar o redirecionamento multimídia do Windows Media pela WAN

Essa configuração se aplica apenas ao Windows Media e permite que a transcodificação multimídia em tempo real seja feita na Unidade de Processamento Gráfico (GPU) no Virtual Delivery Agent (VDA). Ela melhora a escalabilidade do servidor. A transcodificação por GPU está disponível apenas se o VDA tiver uma GPU compatível para aceleração de hardware. Caso contrário, a transcodificação retorna para a CPU.

Nota: A transcodificação por GPU é suportada apenas em GPUs NVIDIA.

Por padrão, o uso da GPU no VDA para otimizar a entrega de conteúdo do Windows Media pela WAN é proibido.

Ao adicionar essa configuração a uma política, certifique-se de que as seguintes configurações estejam presentes e definidas como Permitido:

- **Redirecionamento de Mídia do Windows**
- **Otimização para configurações de redirecionamento multimídia do Windows Media pela WAN**

Prevenção de fallback do Windows Media

Essa configuração se aplica ao redirecionamento de conteúdo do navegador, HTML5 e Windows Media. Para que ela suporte HTML5, defina a política **Redirecionamento de vídeo HTML5** como **Permitido**.

Os administradores podem usar a configuração de política de **prevenção de fallback do Windows Media** para especificar os métodos que são tentados para entregar conteúdo transmitido por streaming aos usuários.

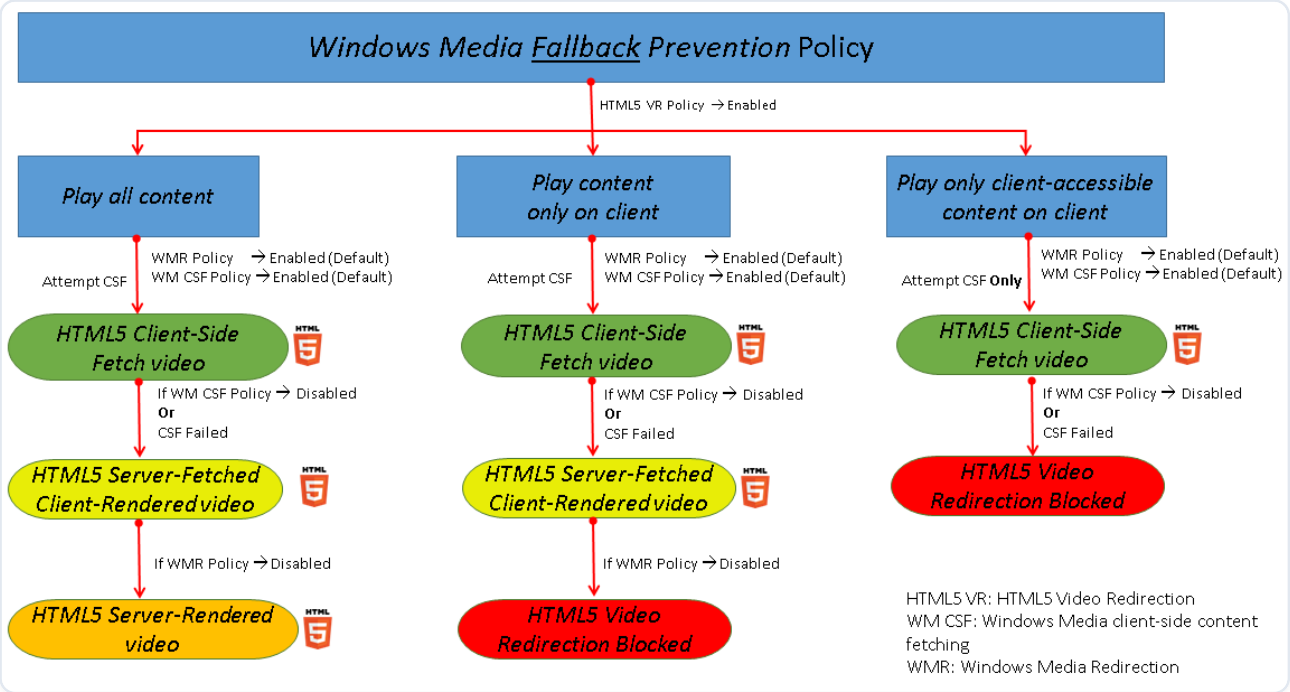
Por padrão, esta configuração não está configurada. Quando a configuração é definida como Não Configurado, o comportamento é o mesmo que **Reproduzir todo o conteúdo**.

Para configurar esta definição, escolha uma das seguintes opções:

- **Reproduzir todo o conteúdo**. Tentar a busca de conteúdo do lado do cliente, depois o Redirecionamento do Windows Media. Se não for bem-sucedido, reproduza o conteúdo no servidor.
- **Reproduzir todo o conteúdo apenas no cliente**. Tentar a busca do lado do cliente, depois o Redirecionamento do Windows Media. Se não for bem-sucedido, o conteúdo não será reproduzido.
- **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Tentar apenas a busca do lado do cliente. Se não for bem-sucedido, o conteúdo não será reproduzido.

Quando o conteúdo não é reproduzido, a seguinte mensagem de erro é exibida na janela do player (por uma duração padrão de 5 segundos):

"A empresa bloqueou o vídeo por falta de recursos"



A duração desta mensagem de erro pode ser personalizada com a seguinte chave de registro no VDA. Se a entrada de registro não existir, a duração padrão é de 5 segundos.

O caminho do registro varia dependendo da arquitetura do VDA:

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

Ou

\HKLM\SOFTWARE\Citrix\HdxMediastream

Chave de registro:

Nome: VideoLoadManagementErrDuration

Tipo: DWORD

Intervalo: 1 - até o limite DWORD (padrão = 5)

Unidade: segundos

Busca de conteúdo do lado do cliente do Windows Media

Essa configuração se aplica tanto ao HTML5 quanto ao Windows Media. A configuração permite que um dispositivo de usuário transmita arquivos multimídia diretamente do provedor de origem na internet ou intranet, em vez de através do servidor host do XenApp ou XenDesktop®.

Por padrão, essa configuração é **Permitida**. Permitir essa configuração melhora o uso da rede e a escalabilidade do servidor. Essa melhoria é alcançada movendo qualquer processamento de

mídia do servidor host para o dispositivo do usuário. Também remove a exigência de que uma estrutura multimídia avançada, como Microsoft DirectShow ou Media Foundation, seja instalada no dispositivo do usuário. O dispositivo do usuário requer apenas a capacidade de reproduzir um arquivo de uma URL

Ao adicionar essa configuração a uma política, certifique-se de que a configuração **Redirecionamento do Windows Media** esteja presente e definida como **Permitida**. Se o **Redirecionamento do Windows Media** estiver desabilitado, a transmissão de arquivos multimídia para o dispositivo do usuário diretamente do provedor de origem também será desabilitada.

Redirecionamento do Windows Media

Essa configuração se aplica tanto ao HTML5 quanto ao Windows Media e controla e otimiza a forma como os servidores entregam áudio e vídeo em streaming aos usuários.

Por padrão, essa configuração é **Permitida**. Para HTML5, essa configuração não tem efeito se a política **Redirecionamento de vídeo HTML5** for **Proibida**.

Quando essa configuração está habilitada, a qualidade do áudio e vídeo renderizados do servidor aumenta para um nível comparável ao áudio e vídeo reproduzidos localmente em um dispositivo de usuário. O servidor transmite multimídia para o cliente na forma original e compactada e permite que o dispositivo do usuário descompacte e renderize a mídia.

O redirecionamento do Windows Media otimiza arquivos multimídia codificados com codecs que aderem aos padrões Microsoft DirectShow, DirectX Media Objects (DMO) e Media Foundation. Para reproduzir um determinado arquivo multimídia, um codec compatível com o formato de codificação do arquivo multimídia deve estar presente no dispositivo do usuário.

Por padrão, o áudio está desabilitado no aplicativo Citrix Workspace. Para permitir que os usuários executem aplicativos multimídia em sessões ICA®, ative o áudio ou conceda aos usuários permissão para ativar o áudio na interface do aplicativo Citrix Workspace.

Selecione **Proibido** apenas se a reprodução de mídia usando o redirecionamento do Windows Media parecer pior do que quando renderizada usando compressão ICA básica e áudio regular. Essa situação é rara, mas pode ocorrer em condições de baixa largura de banda, por exemplo, com mídia com baixa frequência de quadros-chave.

Tamanho do buffer de redirecionamento do Windows Media

Essa configuração é legada e não se aplica ao HTML5.

Essa configuração especifica um tamanho de buffer de 1 a 10 segundos para aceleração multimídia.

Por padrão, o tamanho do buffer é de 5 segundos.

Uso do tamanho do buffer de redirecionamento do Windows Media

Esta configuração é legada e não se aplica ao HTML5.

Esta configuração habilita ou desabilita o uso do tamanho do buffer especificado na configuração **Tamanho do buffer de redirecionamento do Windows Media**.

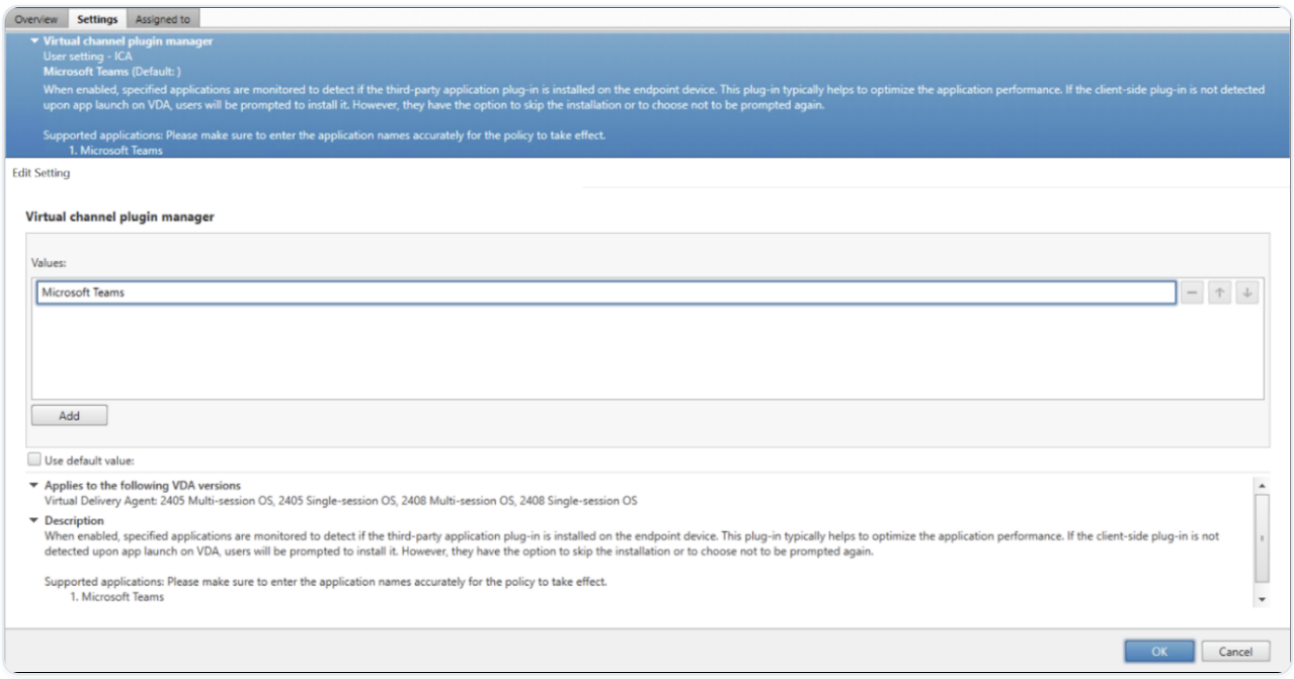
Por padrão, o tamanho do buffer especificado não é usado.

Se esta configuração estiver desabilitada ou se a configuração **Tamanho do buffer de redirecionamento do Windows Media** não estiver configurada, o servidor usará o valor padrão do tamanho do buffer (cinco segundos).

Política do gerenciador de plug-ins de canal virtual

A seção Gerenciador de plug-ins de canal virtual inclui configurações de política para configurar esse recurso.

O gerenciador de plug-ins de canal virtual foi projetado para implantar plug-ins em endpoints de cliente para determinados aplicativos especificados. O gerenciador de plug-ins detecta aplicativos específicos em execução no VDA e solicita ao usuário que instale o plug-in no endpoint para obter a melhor experiência ao executar o aplicativo.



- Os administradores podem usar a política e especificar o aplicativo para o qual precisam que o plug-in seja instalado em seus endpoints.
- O nome do aplicativo deve ser o mesmo que o nome mencionado em Aplicativos suportados na descrição da política.
- Por padrão, a política está desabilitada.
- Aplicativos atualmente suportados
  - “Microsoft Teams”
- No futuro, mais aplicativos estão planejados para serem suportados.

Configurações de política de conexões multi-stream

A seção **Conexões Multi-Stream** inclui configurações de política para gerenciar a priorização de Qualidade de Serviço para múltiplas conexões ICA® em uma sessão.

> **Observação:**
>
> A Descoberta de MTU não é suportada se a política de conexões Multi-Stream estiver habilitada.

Áudio sobre UDP

Esta configuração permite ou impede o áudio sobre UDP no servidor.

Por padrão, o áudio sobre UDP é permitido no servidor.

Quando habilitada, esta configuração abre uma porta UDP no servidor para suportar todas as conexões configuradas para usar o Transporte em Tempo Real de Áudio sobre UDP.

Intervalo de portas UDP de áudio

Esta configuração especifica o intervalo de números de porta (número de porta mais baixo, número de porta mais alto) usado pelo Virtual Delivery Agent (VDA). Esta especificação ajuda a trocar dados de pacotes de áudio com o dispositivo do usuário. O VDA tenta usar cada par de portas UDP para trocar dados com o dispositivo do usuário, começando com o mais baixo e incrementando em dois para cada tentativa subsequente. Cada porta lida com tráfego de entrada e saída.

Por padrão, este intervalo é definido como 16500,16509.

Política Multi-Porta

Esta configuração especifica as portas TCP a serem usadas para o tráfego ICA e estabelece a prioridade de rede para cada porta.

Por padrão, a porta primária (2598) tem prioridade Alta.

Ao configurar portas, você pode atribuir as seguintes prioridades:

- **Muito Alta:** para atividades em tempo real, como conferências por webcam
- **Alta:** para elementos interativos, como tela, teclado e mouse
- **Média:** para processos em massa, como mapeamento de unidade cliente
- **Baixa:** para atividades em segundo plano, como impressão

Cada porta deve ter uma prioridade exclusiva. Por exemplo, você não pode atribuir uma prioridade Muito Alta às portas CGP 1 e CGP 3.

Para remover uma porta da priorização, defina o número da porta como 0. Você não pode remover a porta primária e não pode alterar seu nível de prioridade.

Ao configurar esta definição, reinicie o servidor. Esta definição só entra em vigor quando a definição de política **Multi-Stream computer** está ativada.

Definição de computador Multi-Stream

Esta definição ativa ou desativa o Multi-Stream no servidor.

Por padrão, o Multi-Stream está desativado. Configure a definição de política de computador Multi-Stream se você usar Citrix SD-WAN™ ou roteadores de terceiros para obter a Qualidade de Serviço desejada.

Se o Multi-Stream estiver ativado, a Descoberta de MTU, um recurso do Adaptive Transport, não é suportada.

Ao configurar esta definição, reinicie o servidor para garantir que as alterações entrem em vigor.

> **Importante:**
>
> Usar esta definição de política com definições de política de limite de largura de banda, como o limite geral de largura de banda da sessão, pode produzir resultados inesperados. Ao incluir esta definição em uma política, certifique-se de que as definições de limite de largura de banda não estejam incluídas.

Definição de usuário Multi-Stream

Esta definição ativa ou desativa o Multi-Stream no dispositivo do usuário.

Por padrão, o Multi-Stream está desativado para todos os usuários. Configure a definição de usuário Multi-Stream se você usar Citrix SD-WAN ou roteadores de terceiros para obter a Qualidade de Serviço desejada.

Esta configuração só tem efeito em hosts onde a configuração de política **Computador Multi-Stream** está ativada.

> **Importante:**
>
> Usar esta configuração de política com configurações de política de limite de largura de banda, como Limite geral de largura de banda da sessão, pode produzir resultados inesperados. Ao incluir esta configuração em uma política, certifique-se de que as configurações de limite de largura de banda não estejam incluídas.

Configurações de atribuição de canal virtual Multi-Stream

Esta configuração especifica o fluxo ICA ao qual os canais virtuais são atribuídos quando o multi-stream é usado.

Se você não configurar essas configurações, os canais virtuais serão mantidos em seu fluxo padrão. Para atribuir um canal virtual a um fluxo ICA, selecione o número do fluxo desejado (0, 1, 2, 3) na lista **Número do Fluxo** ao lado do nome do canal virtual.

Se houver um canal virtual personalizado em uso no ambiente, clique em **Adicionar**, especifique o nome do canal virtual na caixa de texto em **Canais Virtuais** e selecione o número do fluxo desejado na lista **Número do Fluxo** ao lado dele. O nome que você especificar deve ser o nome real do canal virtual e não um nome amigável. Por exemplo, CTXSBR em vez de Citrix Browser Acceleration.

Essas configurações só entram em vigor quando você ativou a configuração de computador multi-stream.

Por padrão, os canais virtuais e suas atribuições de fluxo são:

- AppFlow®: 2
- Áudio: 0

- Redirecionamento de Conteúdo do Navegador: 2
- Mapeamento de Porta COM do Cliente: 3
- Mapeamento de Unidade do Cliente: 2
- Mapeamento de Impressora do Cliente: 3
- Área de Transferência: 2
- CTXDND: 1 (**Observação:** Isso suporta arrastar e soltar arquivos entre uma sessão Citrix e um endpoint local.)
- Plug-in DVC (nome VC estático gerado automaticamente a partir do Nome Amigável do Plug-in DVC, ou atribuído pelo administrador): 2
- Monitoramento da Experiência do Usuário Final: 1
- Transferência de Arquivos (HTML5 Receiver): 2
- Transferência Genérica de Dados: 2
- Controle ICA: 1
- Editor de Método de Entrada: 1
- Mapeamento de Impressora Cliente Legado (COM1): 1, 3
- Mapeamento de Impressora Cliente Legado (COM2): 2, 3
- Mapeamento de Impressora Cliente Legado (LPT1): 1, 3
- Mapeamento de Impressora Cliente Legado (LPT2): 2, 3
- Gerenciamento de Licenças: 1
- Redirecionamento do Microsoft Teams/WebRTC: 1
- Receiver Móvel: 1
- Multitoque: 1
- Encaminhamento de Porta: 2
- Extensões de Áudio e Vídeo Remotas (RAVE): 2
- Seamless (Integração Transparente de Janelas): 1
- Sensor e Localização: 1
- Cartão Inteligente: 1
- Gráficos Thinwire: 1
- Integração Transparente da UI/Status de Logon: 2
- Redirecionamento TWAIN: 2

- USB: 2
- Fonte e Teclado de Latência Zero: 2
- Canal de Dados de Latência Zero: 2

Para obter mais informações sobre atribuições e prioridades de canais virtuais, consulte o artigo do Knowledge Center CTX131001.

Configurações de política de redirecionamento de porta

A seção **Redirecionamento de Porta** contém configurações de política para mapeamento de porta LPT e COM do cliente.

Para versões do Virtual Delivery Agent **anteriores a 7.0**, use as seguintes configurações de política para configurar o redirecionamento de porta. Para as versões do VDA **7.0 a 7.8**, configure essas configurações usando o registro; consulte Configurar as configurações de redirecionamento de porta COM e porta LPT usando o registro. Para a versão do VDA **7.9**, use as seguintes configurações de política.

Conectar automaticamente portas COM do cliente

Essa configuração habilita ou desabilita a conexão automática de portas COM em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas COM do cliente não são conectadas automaticamente.

Conectar automaticamente portas LPT do cliente

Essa configuração habilita ou desabilita a conexão automática de portas LPT em dispositivos de usuário quando os usuários fazem logon em um site.

Por padrão, as portas LPT do cliente não são conectadas automaticamente.

Redirecionamento de porta COM do cliente

Essa configuração permite ou impede o acesso a portas COM no dispositivo do usuário.

Por padrão, o redirecionamento de porta COM é proibido.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta COM
- Porcentagem de limite de largura de banda de redirecionamento de porta COM

Redirecionamento de porta LPT do cliente

Esta configuração permite ou impede o acesso às portas LPT no dispositivo do usuário.

Por padrão, o redirecionamento de porta LPT é proibido.

As portas LPT são usadas apenas por aplicativos legados que enviam trabalhos de impressão para as portas LPT. Essas portas não são usadas por aplicativos legados que enviam trabalhos de impressão para os objetos de impressão no dispositivo do usuário. A maioria dos aplicativos hoje pode enviar trabalhos de impressão para objetos de impressora. Essa configuração de política é necessária apenas para servidores que hospedam aplicativos legados que imprimem em portas LPT.

Observe que, embora o redirecionamento de porta COM do cliente seja bidirecional, o redirecionamento de porta LPT é apenas de saída e limitado a `\client\LPT1` e `\client\LPT2` dentro de uma sessão ICA.

As seguintes configurações de política estão relacionadas:

- Limite de largura de banda de redirecionamento de porta LPT
- Porcentagem de limite de largura de banda de redirecionamento de porta LPT

Configurações de política de impressão

A seção Impressão contém configurações de política para gerenciar a impressão do cliente.

Redirecionamento de impressora cliente

Essa configuração controla se as impressoras cliente são mapeadas para um servidor quando um usuário faz logon em uma sessão.

Por padrão, o mapeamento de impressora cliente é permitido. Se essa configuração estiver desabilitada, a impressora PDF para a sessão não será criada automaticamente.

Configurações de política relacionadas: criar impressoras cliente automaticamente

Impressora padrão

Essa configuração especifica como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como a impressora padrão para a sessão.

Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar a impressora padrão do usuário. Se você

escolher essa opção, a impressora padrão não será salva no perfil e não será alterada de acordo com outras propriedades da sessão ou do cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é uma das seguintes:

- A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e **Impressoras**.
- A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

Você pode usar essa opção para apresentar aos usuários a impressora mais próxima por meio das configurações de perfil (conhecido como impressão por proximidade).

Atribuições de impressora

Essa configuração oferece uma alternativa às configurações de Impressora padrão e Impressoras de sessão. Use as configurações individuais de Impressora padrão e Impressoras de sessão para configurar comportamentos para um site, um grupo grande ou uma unidade organizacional. Use a configuração **Atribuições de impressora** para atribuir um grande grupo de impressoras a vários usuários.

Esta configuração especifica como a impressora padrão nos dispositivos de usuário listados é estabelecida em uma sessão.

Por padrão, a impressora atual do usuário é usada como a impressora padrão para a sessão.

Também especifica as impressoras de rede a serem criadas automaticamente em uma sessão para cada dispositivo de usuário. Por padrão, nenhuma impressora é especificada.

- Ao definir o valor da impressora padrão:

  Para usar a impressora padrão atual para o dispositivo de usuário, selecione Não ajustar.

  Para usar a configuração atual do perfil de usuário do Remote Desktop Services ou do Windows para a impressora padrão, selecione Não ajustar. Se você escolher esta opção, a impressora padrão não será salva no perfil e não mudará de acordo com outras propriedades da sessão ou do cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é uma das seguintes:

  - A primeira impressora adicionada localmente ao servidor Windows em **Painel de Controle > Dispositivos** e Impressoras.
  - A primeira impressora criada automaticamente, se não houver impressoras adicionadas localmente ao servidor.

- Ao definir o valor das impressoras de sessão: para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Após adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual a cada logon.

Preferência de log de eventos de criação automática de impressora

Esta configuração especifica os eventos que são registrados durante o processo de criação automática de impressora. Você pode optar por não registrar erros ou avisos, apenas erros, ou erros e avisos.

Por padrão, erros e avisos são registrados.

Um exemplo de aviso é um evento em que o driver nativo de uma impressora não pode ser instalado e o driver de impressão universal é instalado em seu lugar. Para usar o driver de impressão universal neste cenário, configure a configuração de uso do driver de impressão universal para Usar somente impressão universal ou Usar somente impressão universal se o driver solicitado não estiver disponível.

Impressoras de sessão

Esta configuração especifica as impressoras de rede a serem criadas automaticamente em uma sessão. Dentro da sessão ICA/HDX, o serviço Citrix Print Manager (CpSvc.exe) cria uma conexão de impressora de rede durante o logon da sessão para cada impressora de rede especificada na configuração de política **Impressora de Sessão**. Ele exclui as impressoras durante o logoff da sessão. Por padrão, nenhuma impressora é especificada.

Na configuração de política de **Impressora de Sessão**, as impressoras de rede podem residir em um Servidor de Impressão Windows ou em um Servidor de Impressão Universal™ Citrix.

- **Servidor de Impressão Windows:** Compartilha uma ou mais impressoras de rede. Ele também possui os drivers de impressora nativos necessários para usar as impressoras de rede.
- **Servidor de Impressão Universal:** Um Servidor de Impressão Windows onde o software Citrix Universal Print Server foi instalado.

Ao usar um Servidor de Impressão Windows, o serviço Citrix Print Manager cria as conexões de impressora de rede usando drivers de impressora nativos. O servidor Citrix Virtual Apps™ deve ter os drivers de impressora nativos instalados nele.

Ao usar um Servidor de Impressão Universal Citrix, o serviço Citrix Print Manager cria as conexões de impressora de rede usando drivers de impressora nativos, Citrix Universal Printer

Driver ou Citrix Universal XPS Printer Driver. O driver que você usa é controlado pela configuração de política de uso do Universal Print Driver.

Todos os drivers de impressora Windows atualmente se enquadram nas versões de driver v3 ou v4. Para obter mais informações, consulte Suporte para as Arquiteturas de Driver de Impressora Microsoft V3 e V4.

Para adicionar impressoras de sessão e verificar se elas aparecem nas sessões, conclua o seguinte procedimento:

1. Faça login no Web Studio, selecione **Políticas** no painel esquerdo e, em seguida, clique na guia **Políticas**.
2. Habilite a política de **Impressoras de sessão**.
3. Na política, adicione a impressora de sessão. Para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Após adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual a cada logon. A impressora de sessão deve ser exibida na lista.
4. Depois que a política for definida, o aplicativo publicado pode não exibir as impressoras de sessão. Esse problema pode ocorrer porque o driver da impressora está ausente no servidor Citrix Virtual Apps ou a política foi criada, mas não habilitada.

   > **Observação:**
   >
   > Se uma impressora de sessão precisar de um driver de impressora nativo e o driver de impressora nativo não estiver instalado no VDA, a impressora de sessão poderá não ser criada na sessão.

5. Inicie o desktop publicado e adicione manualmente a impressora de sessão em **Dispositivos e Impressoras > Painel de Controle**.
6. Se isso falhar, investigue a comunicação entre o servidor Citrix Virtual Apps e o servidor de impressão. Considere executar um teste com RDP.

Aguardar a criação das impressoras

Use a política no Delivery Controller para habilitar o recurso no Citrix Virtual Desktops.

Aguardar a criação de impressoras (Server Desktop):

Essa configuração permite um atraso na conexão a uma sessão para que as impressoras redirecionadas do cliente possam ser criadas automaticamente.

Por padrão, um atraso na conexão não ocorre.

Aguardar a criação de impressoras (Citrix Virtual Apps):

A execução do seguinte cmdlet do PowerShell permite um atraso na conexão a aplicativos virtuais em execução em hosts de várias sessões para que as impressoras redirecionadas do cliente possam ser criadas automaticamente antes que o aplicativo seja aberto.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

Por padrão, um atraso na conexão não ocorre.

Configurações de política de impressoras cliente

A seção **Impressoras Cliente** inclui configurações de política para impressoras cliente, incluindo configurações para criar automaticamente impressoras cliente, reter propriedades de impressora e conectar-se a servidores de impressão.

CRIAR AUTOMATICAMENTE IMPRESSORAS CLIENTE

Esta configuração especifica as impressoras cliente que são criadas automaticamente. Esta configuração substitui as configurações padrão de criação automática de impressoras cliente.

Por padrão, todas as impressoras cliente são criadas automaticamente.

Esta configuração só entra em vigor se a configuração **Redirecionamento de impressora cliente** estiver presente e definida como **Permitido**.

Ao adicionar esta configuração a uma política, selecione uma opção:

- **Criar automaticamente todas as impressoras cliente** cria automaticamente todas as impressoras em um dispositivo de usuário.
- **Criar automaticamente apenas a impressora padrão do cliente** cria automaticamente apenas a impressora selecionada como impressora padrão no dispositivo do usuário.
- **Criar automaticamente apenas impressoras cliente locais (não de rede)** cria automaticamente apenas impressoras conectadas diretamente ao dispositivo do usuário através de uma porta LPT, COM, USB, TCP/IP ou outra porta local.
- **Não criar automaticamente impressoras cliente** desativa a criação automática para todas as impressoras cliente quando os usuários fazem logon. A escolha desta opção faz com que

as configurações dos Serviços de Área de Trabalho Remota (RDS) para criação automática de impressoras cliente substituam esta configuração em políticas de menor prioridade.

CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL GENÉRICA

Esta configuração habilita ou desabilita a criação automática do objeto de Impressora Universal™ Citrix genérica para sessões. Essas sessões incluem apenas as sessões em que um dispositivo de usuário compatível com Impressão Universal está em uso.

Por padrão, o objeto de Impressora Universal genérica não é criado automaticamente.

As seguintes configurações de política estão relacionadas:

- Uso do driver de impressão universal
- Preferência de driver universal

CRIAR AUTOMATICAMENTE IMPRESSORA UNIVERSAL PDF

Esta configuração ativa ou desativa a criação automática da impressora PDF Citrix para sessões que usam:

- Aplicativo Citrix Workspace para Windows (a partir do VDA 7.19)
- Aplicativo Citrix Workspace™ para HTML5
- Aplicativo Citrix Workspace para Chrome

Por padrão, a impressora PDF Citrix não é criada automaticamente.

NOMES DE IMPRESSORAS CLIENTE

Esta configuração seleciona a convenção de nomenclatura para impressoras cliente criadas automaticamente.

Por padrão, nomes de impressoras padrão são usados.

Selecione **Nomes de impressoras padrão** para usar nomes de impressoras como "HPLaserJet 4 do nome do cliente na sessão 3."

Selecione **Nomes de impressoras herdados** para usar nomes de impressoras cliente de estilo antigo e para preservar a compatibilidade retroativa com nomes de impressoras herdados, como os presentes nas versões XenDesktop do produto. Você pode usar esta opção com as versões atuais do Citrix Virtual Apps and Desktops do produto. Um exemplo de nome de impressora herdado é "Cliente/nomedocliente#/HPLaserJet 4." Esta opção é menos segura.

Ao usar a impressora PDF Citrix em uma sessão iniciada a partir do aplicativo Citrix Workspace para HTML5, defina a configuração **Nomes de impressoras cliente** como padrão ou selecione

Nomes de impressoras padrão. Se você selecionar **Nomes de impressoras herdados**, o aplicativo Citrix Workspace para HTML5 não oferece suporte à opção Impressora PDF Citrix.

CONEXÕES DIRETAS A SERVIDORES DE IMPRESSÃO

Esta configuração ativa ou desativa conexões diretas do desktop virtual ou de aplicativos de hospedagem de servidor para um servidor de impressão para impressoras cliente. Aqui, as impressoras cliente são hospedadas em um compartilhamento de rede acessível.

Por padrão, as conexões diretas estão habilitadas.

Habilite conexões diretas se o servidor de impressão em rede não estiver em uma WAN a partir do desktop virtual ou de aplicativos de hospedagem de servidor. A comunicação direta resulta em impressão mais rápida se o servidor de impressão em rede e o desktop virtual ou aplicativos de hospedagem de servidor estiverem na mesma LAN.

Desabilite as conexões diretas se a rede estiver em uma WAN ou tiver latência substancial ou largura de banda limitada. Os trabalhos de impressão são roteados através do dispositivo do usuário, onde são redirecionados para o servidor de impressão em rede. Os dados enviados para o dispositivo do usuário são compactados, de modo que menos largura de banda é consumida à medida que os dados viajam pela WAN.

Se duas impressoras de rede tiverem o mesmo nome, a impressora na mesma rede que o dispositivo do usuário será usada.

MAPEAMENTO E COMPATIBILIDADE DE DRIVER DE IMPRESSORA

Esta configuração especifica as regras de substituição de driver para impressoras cliente criadas automaticamente.

Esta configuração está definida para excluir o Microsoft OneNote e o XPS Document Writer da lista de impressoras cliente criadas automaticamente.

Ao definir regras de substituição de driver, você pode permitir ou impedir que impressoras sejam criadas com o driver especificado. Além disso, você pode permitir que impressoras criadas usem apenas drivers de impressão universais. A substituição de driver substitui ou mapeia os nomes dos drivers de impressora fornecidos pelo dispositivo do usuário, substituindo um driver equivalente no servidor. Essas regras dão aos aplicativos de servidor acesso a impressoras cliente que têm os mesmos drivers que o servidor, mas nomes de driver diferentes.

Você pode fazer o seguinte:

- Adicionar um mapeamento de driver

- Editar um mapeamento existente
- Substituir configurações personalizadas para um mapeamento
- Remover um mapeamento
- Alterar a ordem das entradas de driver na lista

Ao adicionar um mapeamento, insira o nome do driver da impressora cliente e, em seguida, selecione o driver do servidor que você deseja substituir.

RETENÇÃO DE PROPRIEDADES DA IMPRESSORA

Esta configuração especifica se as propriedades da impressora devem ser armazenadas e onde armazená-las.

Por padrão, o sistema determina se as propriedades da impressora são armazenadas no dispositivo do usuário, se disponível, ou no perfil do usuário.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Salvo apenas no dispositivo cliente é para dispositivos de usuário que possuem um perfil obrigatório ou de roaming que não é salvo.
- Retido apenas no perfil do usuário é para dispositivos de usuário limitados pela largura de banda (esta opção reduz o tráfego de rede) e velocidade de logon ou para usuários com plug-ins legados. Esta opção armazena as propriedades da impressora no perfil do usuário no servidor e impede qualquer troca de propriedades com o dispositivo do usuário. Esta opção é aplicável apenas se um perfil de roaming do Remote Desktop Services (RDS) for usado.
- Mantido no perfil apenas se não for salvo no cliente permite que o sistema determine onde as propriedades da impressora são armazenadas. As propriedades da impressora são armazenadas no dispositivo do usuário, se disponível, ou no perfil do usuário. Embora esta opção seja a mais flexível, ela também pode atrasar o tempo de logon e usar largura de banda extra para a verificação do sistema.
- Não reter propriedades da impressora impede o armazenamento de propriedades da impressora.

IMPRESSORAS CLIENTE RETIDAS E RESTAURADAS

Esta configuração habilita ou desabilita a retenção e recriação de impressoras no dispositivo do usuário. Por padrão, as impressoras cliente são retidas e restauradas automaticamente.

Impressoras retidas são impressoras criadas pelo usuário que são criadas novamente, ou lembradas, no início da próxima sessão. Quando o Citrix Virtual Apps™ recria uma impressora

retida, ele considera todas as configurações de política, exceto a configuração **Criar impressoras cliente automaticamente**.

Impressoras restauradas são impressoras totalmente personalizadas por um administrador, com um estado salvo que está permanentemente anexado a uma porta cliente.

DRIVER DE IMPRESSORA UNIVERSAL PDF DA CITRIX

O driver de Impressora Universal PDF da Citrix permite que os usuários imprimam documentos abertos com aplicativos hospedados ou aplicativos que estão sendo executados em desktops virtuais entregues pelo Citrix Virtual Apps and Desktops. Quando um usuário seleciona a opção **Citrix PDF Printer**, o driver converte o arquivo para PDF e transfere o PDF para o dispositivo local. O PDF é então aberto para visualização e impressão a partir de uma impressora conectada localmente. PDF é um dos formatos suportados com a Impressão Universal da Citrix (além de EMF e XPS). A impressora PDF pode ser habilitada, configurada e definida como padrão usando uma Política Citrix. A opção **Citrix PDF Printer** está disponível para usuários do aplicativo Citrix Workspace para Windows, Chrome e HTML5.

> **Observação:**
>
> Um visualizador de PDF é necessário para endpoints Windows. O cliente deve ter um aplicativo que tenha associação de tipo de arquivo registrada no Windows para abrir arquivos PDF.

Configurações de política de drivers

A seção **Drivers** inclui configurações de política relacionadas a drivers de impressora.

INSTALAÇÃO AUTOMÁTICA DE DRIVERS DE IMPRESSORA EMBUTIDOS

> **Observação**
>
> Esta política não oferece suporte a VDAs nesta versão.

Esta configuração habilita ou desabilita a instalação automática de drivers de impressora a partir do seguinte:

- Conjunto de drivers embutidos do Windows
- Pacotes de drivers preparados no host usando `pnputil.exe /a`

Por padrão, esses drivers são instalados conforme necessário.

PREFERÊNCIA DE DRIVER UNIVERSAL

Esta configuração especifica a ordem em que os drivers de impressora universais são usados, começando com a primeira entrada na lista.

Por padrão, a ordem de preferência é:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.

USO DO DRIVER DE IMPRESSÃO UNIVERSAL

Essa configuração especifica quando usar a impressão universal.

Por padrão, a impressão universal é usada somente se o driver solicitado não estiver disponível.

A impressão universal emprega drivers de impressora genéricos em vez de drivers padrão específicos do modelo, o que pode simplificar a carga de gerenciamento de drivers em computadores host. A disponibilidade de drivers de impressão universais depende dos recursos do dispositivo do usuário, do host e do software do servidor de impressão. Em certas configurações, a impressão universal pode não estar disponível.

Ao adicionar essa configuração a uma política, selecione uma opção na tabela a seguir:

OPÇÃO	DESCRIÇÃO
Usar somente drivers específicos do modelo da impressora	Especifica que a impressora cliente usa apenas os drivers padrão específicos do modelo que são criados automaticamente durante o logon. Se o driver solicitado não estiver disponível, a impressora cliente não poderá ser criada automaticamente.
Usar somente impressão universal	Especifica que nenhum driver padrão específico do modelo é usado. Somente

OPÇÃO	DESCRIÇÃO
	drivers de impressão universais são usados para criar impressoras.
Usar impressão universal somente se o driver solicitado não estiver disponível	Usa drivers padrão específicos do modelo para a criação da impressora, se estiverem disponíveis. Se o driver não estiver disponível no servidor, a impressora cliente será criada automaticamente com o driver universal apropriado.
Usar drivers específicos do modelo da impressora somente se a impressão universal não estiver disponível	Usa o driver de impressão universal se ele estiver disponível. Se o driver não estiver disponível no servidor, a impressora cliente será criada automaticamente com o driver de impressora específico do modelo apropriado.

Configurações de política do Universal Print Server

A seção **Universal Print Server** inclui configurações de política para gerenciar o Universal Print Server.

CONJUNTO DE CIFRAS SSL

Essa configuração especifica o conjunto de conjuntos de cifras SSL/TLS que são usados no Universal Print Client para conexões de fluxo de dados de impressão criptografados (CGP).

Para controlar o pacote de conjuntos de cifras usado pelo Universal Print Client para conexões de serviço web de impressão criptografadas (HTTPS/SOAP), consulte .

Valor padrão: ALL

Essa configuração tem os seguintes valores: ALL, COM ou GOV.

Os conjuntos de cifras correspondentes a cada valor são os seguintes:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

MODO DE CONFORMIDADE SSL

Esta configuração especifica o nível de conformidade com a Publicação Especial 800-52 do NIST que é usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão criptografados (CGP).

Valor padrão: Nenhum.

Esta configuração possui os seguintes valores:

Nenhum.

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade padrão.

SP800-52.

As conexões de fluxo de dados de impressão criptografados (CGP) usam o modo de conformidade da Publicação Especial 800-52 do NIST.

SSL ATIVADO

Esta configuração especifica se SSL/TLS é usado pelo Cliente de Impressão Universal para o seguinte:

- Conexões de fluxo de dados de impressão (CGP)
- Conexões de serviço web (HTTP/SOAP)

Quando você define **Ativar Servidor de Impressão Universal** como **Ativado com fallback para impressão remota nativa do Windows**, as conexões de fallback são feitas pelo Provedor de Impressão de Rede do Microsoft Windows. Esta configuração não afeta essas conexões de fallback.

Valor padrão: Desabilitado

Esta configuração tem os seguintes valores:

Habilitado.

O Cliente de Impressão Universal usa SSL/TLS para se conectar ao Servidor de Impressão Universal.

Desabilitado.

O Cliente de Impressão Universal usa SSL/TLS para se conectar ao Servidor de Impressão Universal.

MODO FIPS SSL

Esta configuração especifica se o módulo criptográfico SSL/TLS usado pelo Cliente de Impressão Universal para conexões de fluxo de dados de impressão (CGP) é executado no modo FIPS.

Valor padrão: Desabilitado

Esta configuração tem os seguintes valores:

Habilitado.

O modo FIPS está ativado.

Desabilitado.

O modo FIPS está desativado.

VERSÃO DO PROTOCOLO SSL

Esta configuração especifica a versão do protocolo SSL/TLS usada pelo Cliente de Impressão Universal.

Valor padrão: ALL

Esta configuração tem os seguintes valores:

ALL.

Use as versões TLS 1.0, 1.1 ou 1.2.

TLSv1.

Use a versão TLS 1.0.

TLSv1.1.

Use a versão TLS 1.1.

TLSv1.2.

Use a versão TLS 1.2.

PORTA DO FLUXO DE DADOS DE IMPRESSÃO CRIPTOGRAFADO (CGP) DO SERVIDOR DE IMPRESSÃO UNIVERSAL SSL

Esta configuração especifica o número da porta TCP da porta do fluxo de dados de impressão criptografado (CGP) do Servidor de Impressão Universal. Esta porta recebe dados para trabalhos de impressão.

Valor padrão: 443

PORTA DO SERVIÇO WEB CRIPTOGRAFADO (HTTPS/SOAP) DO SERVIDOR DE IMPRESSÃO UNIVERSAL SSL

Esta configuração especifica o número da porta TCP do serviço web criptografado (HTTPS/SOAP) do Universal Print Server. Esta porta recebe dados para comandos de impressão.

Valor padrão: 8443

HABILITAR UNIVERSAL PRINT SERVER

Esta política habilita ou desabilita o uso do Citrix Universal Print Server (UPS). Aplique esta configuração de política a Unidades Organizacionais (OUs) que incluem o desktop virtual ou aplicativos de hospedagem de servidor. Estas configurações de política incluem opções de fallback para permitir conexões a servidores de impressão usando o serviço de impressão remota nativo do Windows, caso o componente Citrix UPS não esteja instalado ou disponível no servidor de impressão solicitado. As alterações a esta política são aplicáveis somente após a reinicialização do VDA.

Por padrão, o Universal Print Server está desabilitado.

Ao adicionar esta configuração a uma política, selecione uma das seguintes opções:

- **Habilitado com fallback para impressão remota nativa do Windows**: O Universal Print Server atende às conexões de impressora de rede, se possível. Se o Universal Print Server não estiver disponível, o Provedor de Impressão do Windows será usado. O Provedor de Impressão do Windows continua a manipular todas as impressoras criadas anteriormente com o Provedor de Impressão do Windows.
- **Habilitado sem fallback para impressão remota nativa do Windows**: O Universal Print Server atende às conexões de impressora de rede exclusivamente. Se o Universal Print Server estiver indisponível, a conexão da impressora de rede falhará. Esta configuração desabilita efetivamente a impressão em rede através do Provedor de Impressão do Windows. Impressoras criadas anteriormente com o Provedor de Impressão do Windows não são criadas enquanto uma política contendo esta configuração estiver ativa.

- **Desabilitado**: O recurso Universal Print Server está desabilitado. Nenhuma tentativa é feita para conectar-se ao Universal Print Server ao conectar-se a uma impressora de rede com um nome UNC. As conexões com impressoras remotas continuam a usar o recurso de impressão remota nativo do Windows.

PORTA DO FLUXO DE DADOS DE IMPRESSÃO (CGP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número da porta TCP usado pelo listener do Common Gateway Protocol (CGP) do fluxo de dados de impressão do Universal Print Server. Aplique esta configuração de política apenas a OUs que contêm o servidor de impressão.

Por padrão, o número da porta é definido como 7229.

Os números de porta válidos devem estar no intervalo de 1 a 65535.

LIMITE DE LARGURA DE BANDA DE ENTRADA DO FLUXO DE IMPRESSÃO DO UNIVERSAL PRINT SERVER (KBPS)

Esta configuração especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão. A taxa de transferência é calculada para os dados de impressão que são entregues de cada trabalho de impressão ao Universal Print Server usando CGP. Aplique esta configuração de política a OUs que contêm o desktop virtual ou aplicativos de hospedagem de servidor.

Por padrão, o valor é 0, o que especifica nenhum limite superior.

PORTA DO SERVIÇO WEB (HTTP/SOAP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número da porta TCP usado pelo ouvinte do serviço web (HTTP/SOAP) do Universal Print Server. O Universal Print Server é um componente opcional que permite o uso de drivers de impressão universais da Citrix para cenários de impressão em rede.

Quando o Universal Print Server é usado, os comandos de impressão são enviados dos hosts do Citrix Virtual Apps and Desktops para o Universal Print Server via SOAP sobre HTTP. Esta configuração modifica a porta TCP padrão na qual o Universal Print Server escuta as solicitações HTTP/SOAP de entrada.

Você deve configurar a porta HTTP do host e do servidor de impressão de forma idêntica. Se você não configurar as portas de forma idêntica, o software do host não se conectará ao Universal Print Server. Esta configuração altera o VDA no Citrix Virtual Apps and Desktops. Além disso, você deve alterar a porta padrão no Universal Print Server.

Por padrão, o número da porta é definido como 8080.

Os números de porta válidos devem estar no intervalo de 0 a 65535.

UNIVERSAL PRINT SERVERS PARA BALANCEAMENTO DE CARGA

Esta configuração lista os Universal Print Servers a serem usados para balancear a carga das conexões de impressora estabelecidas no início da sessão, após avaliar outras configurações de política de impressão da Citrix®. Para otimizar o tempo de criação da impressora, a Citrix recomenda que todos os servidores de impressão tenham o mesmo conjunto de impressoras compartilhadas. Não há limite superior para o número de servidores de impressão que podem ser adicionados para balanceamento de carga.

Esta configuração também implementa a detecção de failover do servidor de impressão e a recuperação de conexões de impressora. Os servidores de impressão são verificados periodicamente quanto à disponibilidade. Se uma falha de servidor for detectada, esse servidor é removido do esquema de balanceamento de carga. Além disso, as conexões de impressora nesse servidor são redistribuídas entre outros servidores de impressão disponíveis. Quando o servidor de impressão com falha se recupera, ele é retornado ao esquema de balanceamento de carga.

Clique em **Validar Servidores** para verificar se cada servidor é um servidor de impressão, se a lista de servidores não inclui nomes de servidores duplicados e se todos os servidores têm um conjunto idêntico de impressoras compartilhadas instaladas. Esta operação pode levar algum tempo.

LIMITE DE UNIVERSAL PRINT SERVERS FORA DE SERVIÇO

Esta configuração especifica quanto tempo o balanceador de carga deve esperar que um servidor de impressão indisponível se recupere antes de determinar que o servidor está permanentemente offline e redistribuir sua carga para outros servidores de impressão disponíveis.

Por padrão, o valor limite é definido como 180 (segundos).

TEMPO LIMITE DE CONEXÃO DO SERVIÇO WEB (HTTP/SOAP) DO UNIVERSAL PRINT SERVER

Esta configuração especifica o número de segundos que o Universal Print Client deve esperar até que uma operação connect() do serviço web do Universal Print Server atinja o tempo limite. Esta configuração possui os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de socket TCP de conexão. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível nas versões anteriores do Universal Print Client antes desta alteração.

O Universal Print Client é o componente do Virtual Delivery Agent (VDA) que se comunica com o Universal Print Server.

> **Observação:**
>
> Esta configuração de política é aplicável na versão 7.35 do VDA e posteriores.

TEMPO LIMITE DE RECEBIMENTO DO SERVIÇO WEB DO UNIVERSAL PRINT SERVER (HTTP/SOAP)

Esta configuração especifica o número de segundos que o Universal Print Client deve esperar até que uma operação recv() do serviço web do Universal Print Server atinja o tempo limite. Esta configuração possui os seguintes valores e todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de socket TCP de recebimento. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível nas versões anteriores do Universal Print Client antes desta alteração.

O Universal Print Client é o componente do Virtual Delivery Agent (VDA) que se comunica com o Universal Print Server.

> **Observação:**
>
> Esta configuração de política é aplicável na versão 7.35 do VDA e posteriores.

TEMPO LIMITE DE ENVIO DO SERVIÇO WEB DO UNIVERSAL PRINT SERVER (HTTP/SOAP)

Esta configuração especifica o número de segundos que o Universal Print Client deve esperar até que uma operação send() do serviço web do Universal Print Server atinja o tempo limite. Esta configuração tem os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de envio de socket TCP. Sockets são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Esta configuração era a configuração disponível nas versões anteriores do Universal Print Client antes desta alteração.

O Universal Print Client é o componente do VDA que se comunica com o Universal Print Server.

> **Observação:**
>
> Esta configuração de política é aplicável na versão 7.35 do VDA e posteriores.

Configurações de política de impressão universal

A seção **Impressão Universal** inclui configurações de política para gerenciar a impressão universal.

MODO DE PROCESSAMENTO EMF DE IMPRESSÃO UNIVERSAL

Esta configuração controla o método de processamento do arquivo de spool EMF no dispositivo de usuário Windows.

Por padrão, os registros EMF são enviados diretamente para a impressora.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Reprocessar EMFs para impressora força o arquivo de spool EMF a ser reprocessado e enviado através do subsistema GDI no dispositivo do usuário. Você pode usar esta configuração para drivers que exigem reprocessamento de EMF, mas que podem não ser selecionados automaticamente em uma sessão.
- Enviar diretamente para a impressora, quando usado com o driver de impressão Citrix Universal™, garante que os registros EMF sejam enviados e entregues ao dispositivo do usuário para processamento. Normalmente, esses arquivos de spool EMF são injetados diretamente na fila de spool do cliente. Para impressoras e drivers compatíveis com o formato EMF, este é o método de impressão mais rápido.

LIMITE DE COMPACTAÇÃO DE IMAGEM DE IMPRESSÃO UNIVERSAL

Esta configuração especifica o seguinte:

- Qualidade máxima disponível para imagens impressas com o driver de impressão Citrix Universal
- Nível mínimo de compactação disponível para imagens impressas com o driver de impressão Citrix Universal

Por padrão, o limite de compactação de imagem é definido como Melhor qualidade (compactação sem perdas).

Se Nenhuma Compactação for selecionada, a compactação será desabilitada apenas para impressão EMF.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Sem compressão
- Melhor qualidade (compressão sem perdas)
- Alta qualidade
- Qualidade padrão
- Qualidade reduzida (compressão máxima)

Ao adicionar esta configuração a uma política que inclui a configuração **Padrões de otimização de impressão universal**, esteja ciente do seguinte:

- Considere que o nível de compressão na configuração **Limite de compressão de imagem de impressão universal** é inferior ao nível definido na configuração **Padrões de otimização de impressão universal**. Neste caso, as imagens são compactadas no nível definido na configuração Limites de compressão de imagem de impressão universal.
- Se a compressão estiver desativada, as opções Qualidade de imagem desejada e Habilitar compressão pesada da configuração Padrões de otimização de impressão universal não terão efeito na política.

PADRÕES DE OTIMIZAÇÃO DE IMPRESSÃO UNIVERSAL

Esta configuração especifica os valores padrão para otimização de impressão quando o driver de impressão universal é criado para uma sessão.

- A qualidade de imagem desejada especifica o limite de compressão de imagem padrão aplicado à impressão universal. Por padrão, a Qualidade Padrão está ativada, o que significa que os usuários só podem imprimir imagens usando compressão de qualidade padrão ou reduzida.
- Habilitar compressão pesada ativa ou desativa a redução da largura de banda além do nível de compressão definido pela Qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compressão pesada está desativada.
- As configurações de Cache de Imagem e Fonte especificam se as imagens e fontes que aparecem várias vezes no fluxo de impressão devem ser armazenadas em cache ou não. Esta configuração garante que cada imagem ou fonte exclusiva seja enviada para a impressora apenas uma vez. Por padrão, imagens e fontes incorporadas são armazenadas em cache. Essas configurações se aplicam somente se o dispositivo do usuário suportar esse comportamento.
- Permitir que não administradores modifiquem essas configurações especifica se os usuários podem alterar as configurações padrão de otimização de impressão dentro de uma sessão ou não. Por padrão, os usuários não têm permissão para alterar as configurações padrão de otimização de impressão.

Nota: Todas essas opções são suportadas para impressão EMF. Para impressão XPS, apenas a opção Qualidade de imagem desejada é suportada.

Ao adicionar esta configuração a uma política que inclui a configuração **Limite de compactação de imagem de impressão universal**, esteja ciente do seguinte:

- Considere que o nível de compactação na configuração **Limite de compactação de imagem de impressão universal** é inferior ao nível definido na configuração **Padrões de otimização**

de impressão universal. Neste caso, as imagens são compactadas no nível definido na configuração Limites de compactação de imagem de impressão universal.

- Se a compactação estiver desabilitada, as opções Qualidade de imagem desejada e Habilitar compactação pesada da configuração Padrões de otimização de impressão universal não terão efeito na política.

PREFERÊNCIA DE VISUALIZAÇÃO DE IMPRESSÃO UNIVERSAL

Esta configuração especifica se deve usar a função de visualização de impressão para impressoras universais genéricas ou criadas automaticamente.

Por padrão, a visualização de impressão não é usada para impressoras universais genéricas ou criadas automaticamente.

Ao adicionar esta configuração a uma política, selecione uma opção:

- Não usar visualização de impressão para impressoras universais genéricas ou criadas automaticamente
- Usar visualização de impressão apenas para impressoras criadas automaticamente
- Usar visualização de impressão apenas para impressoras universais genéricas
- Usar visualização de impressão para impressoras universais genéricas e criadas automaticamente

LIMITE DE QUALIDADE DE IMPRESSÃO UNIVERSAL

Esta configuração especifica o número máximo de pontos por polegada (dpi) disponível para gerar saída impressa em uma sessão.

Por padrão, Sem Limite está habilitado, o que significa que os usuários podem selecionar a qualidade máxima de impressão permitida pela impressora à qual se conectam.

Se esta configuração for configurada, ela limita a qualidade máxima de impressão disponível para os usuários em termos de resolução de saída. Tanto a própria qualidade de impressão quanto os recursos de qualidade de impressão da impressora à qual o usuário se conecta são restritos à configuração definida.

Por exemplo, se configurado para Resolução Média (600 DPI), os usuários podem imprimir a saída com uma qualidade máxima de apenas 600 DPI. Além disso, a configuração **Qualidade de Impressão** na guia **Avançado** da caixa de diálogo **Impressora Universal** mostra as configurações de resolução apenas até e incluindo Qualidade Média (600 DPI).

Ao adicionar esta configuração a uma política, selecione uma opção:

- Rascunho (150 DPI)
- Baixa Resolução (300 DPI)
- Média Resolução (600 DPI)
- Alta Resolução (1200 DPI)
- Sem Limite

Configurações de política de limites do servidor

A seção **Limites do Servidor** inclui a configuração de política para controlar conexões ociosas.

Intervalo do temporizador de inatividade do servidor

Esta configuração determina por quanto tempo uma sessão de usuário ininterrupta é mantida se não houver entrada do usuário. Os dados são calculados em milissegundos.

Por padrão, as conexões ociosas não são desconectadas (intervalo do temporizador de inatividade do servidor = 0). A Citrix® recomenda definir este valor para um mínimo de 60000 milissegundos (60 segundos).

Para exibir a política, selecione **Múltiplas Versões**, desmarque as versões do SO de sessão única e, em seguida, selecione **Limites do Servidor**.

> **Observação**
>
> Quando esta configuração de política é usada, uma caixa de diálogo "Idle timer expired" pode aparecer para os usuários quando a sessão estiver ociosa pelo tempo especificado. As configurações de política da Citrix não controlam esta mensagem da caixa de diálogo da Microsoft. Para obter mais informações, consulte `<http://support.citrix.com/article/CTX118618>`.

Configurações de política de limites de sessão

A seção **Limites de Sessão** inclui configurações de política que controlam por quanto tempo as sessões permanecem conectadas antes de serem forçadas a fazer logoff.

Temporizador de sessão desconectada

Esta configuração habilita ou desabilita um temporizador que especifica por quanto tempo uma área de trabalho desconectada e bloqueada permanece bloqueada antes que a sessão seja desconectada.

Se este temporizador estiver habilitado, a sessão desconectada é desconectada quando o temporizador expira.

Por padrão, as sessões desconectadas não são desconectadas.

Temporizador de sessão desconectada do Acesso para PC Remoto

Esta configuração habilita ou desabilita um temporizador que desconecta uma sessão de usuário desconectada após o temporizador expirar. Se você habilitar esta configuração, use a configuração **Intervalo do temporizador de sessão desconectada** para especificar quantos minutos uma área de trabalho desconectada permanece bloqueada antes que a sessão do usuário seja desconectada.

Por padrão, esta configuração está desabilitada.

Intervalo do temporizador de sessão desconectada

Esta configuração especifica quantos minutos uma área de trabalho desconectada e bloqueada permanece bloqueada antes que a sessão seja desconectada.

Por padrão, o período de tempo é de 1.440 minutos (24 horas).

Temporizador de sessão desconectada – Multissessão

Esta configuração habilita ou desabilita um temporizador para determinar por quanto tempo uma sessão RDS desconectada pode persistir antes que a sessão seja desconectada. Por padrão, este temporizador está desabilitado e as sessões desconectadas não são desconectadas.

Intervalo do temporizador de sessão desconectada – Multissessão

Esta configuração determina quantos minutos uma sessão RDS desconectada pode persistir antes que a sessão seja desconectada. Por padrão, o período de tempo é de 1440 minutos (24 horas).

Temporizador de conexão de sessão

Esta configuração habilita ou desabilita um temporizador que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop. Se este temporizador estiver habilitado, a sessão é desconectada ou encerrada quando o temporizador expira. A configuração da Microsoft **Encerrar sessão quando os limites de tempo forem atingidos** determina o próximo estado para a sessão.

Por padrão, este temporizador está desabilitado.

Intervalo do temporizador de conexão de sessão

Esta configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e um desktop.

Por padrão, a duração máxima é de 1.440 minutos (24 horas).

Temporizador de conexão de sessão – Multissessão

Esta configuração habilita ou desabilita um temporizador que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um servidor de terminal. Por padrão, este temporizador está desabilitado.

Intervalo do temporizador de conexão de sessão – Multissessão

Esta configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e uma sessão RDS. Por padrão, a duração máxima é de 1440 minutos (24 horas).

Temporizador de inatividade da sessão

Quando um usuário não fornece nenhuma entrada, esta configuração é usada para habilitar ou desabilitar:

- Um temporizador que especifica por quanto tempo uma conexão ininterrupta de dispositivo de usuário a um desktop é mantida.

Quando este temporizador expira, a sessão é colocada no estado desconectado e o **Temporizador de sessão desconectada** é aplicado. Se o **Temporizador de sessão desconectada** estiver desabilitado, a sessão não é encerrada.

Por padrão, este temporizador está ativado.

Intervalo do temporizador de inatividade da sessão

Quando não há entrada do usuário, esta configuração é usada para especificar:

- O número de minutos durante os quais uma conexão ininterrupta do dispositivo do usuário a uma área de trabalho é mantida.

Por padrão, as conexões ociosas são mantidas por 1.440 minutos (24 horas).

Temporizador de inatividade da sessão – Multi-sessão

Esta configuração ativa ou desativa um temporizador para determinar a duração máxima de uma conexão ociosa entre um dispositivo de usuário e um servidor de terminal. Por padrão, este temporizador está desativado.

Intervalo do temporizador de inatividade da sessão – Multi-sessão

Esta configuração especifica por quantos minutos uma conexão ociosa entre um dispositivo de usuário e uma sessão RDS é mantida. Por padrão, a duração máxima é de 1440 minutos (24 horas).

> **Observação:**
>
> As configurações de temporizador para máquinas multi-sessão configuradas usando políticas Citrix® devem substituir as configurações de temporizador configuradas por meio de Políticas de Grupo da Microsoft. Para evitar comportamento inesperado, recomendamos que você configure as configurações de temporizador usando um dos dois métodos.

Configurações de política de confiabilidade da sessão

A seção **confiabilidade da sessão** inclui configurações de política para gerenciar conexões de confiabilidade da sessão.

Conexões de confiabilidade da sessão

Essa configuração permite ou impede que as sessões permaneçam abertas durante uma perda de conectividade de rede. A confiabilidade da sessão, juntamente com a reconexão automática do cliente, permite que os usuários se reconectem automaticamente às suas sessões do aplicativo Citrix Workspace™ após se recuperarem de interrupções de rede. Por padrão, a confiabilidade da sessão é Permitida.

As configurações no Web Studio são aplicadas no cliente para o seguinte:

- Aplicativo Citrix Workspace 1808 e posterior
- Citrix Receiver para Windows 4.7 e posterior.

A política do Web Studio substitui o Objeto de Política de Grupo do Citrix Receiver™ nos clientes. As atualizações dessas políticas no Web Studio sincronizam a confiabilidade da sessão do servidor para o cliente.

> **Observação:**
>
> - Citrix Receiver para Windows 4.7 e posterior e aplicativos Citrix Workspace para Windows - Defina a política no Web Studio.

- Citrix Receivers para Windows anteriores a 4.7 - Defina as políticas no Web Studio. Defina também o modelo de Objeto de Política de Grupo do Citrix Receiver no cliente para um comportamento consistente.

A confiabilidade da sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Use a confiabilidade da sessão para manter a sessão ativa no servidor. Para indicar que a conectividade foi perdida, a exibição do usuário fica opaca. O usuário pode ver uma sessão congelada durante a interrupção. O usuário pode retomar a interação com o aplicativo quando a conexão de rede for restaurada. A confiabilidade da sessão reconecta os usuários sem solicitações de reautenticação.

Se você usar a confiabilidade da sessão e a reconexão automática do cliente, os dois recursos funcionarão em sequência. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração de tempo limite de confiabilidade da sessão. Depois disso, as configurações de reconexão automática do cliente entram em vigor, tentando reconectar o usuário à sessão desconectada.

Por padrão, a confiabilidade da sessão é Permitida.

Observação:

Quando o Citrix ADC está em uso, você deve selecionar **Habilitar confiabilidade da sessão** no Citrix StoreFront > **Gerenciar Citrix Gateways** / **Secure Ticket Authority** para fazer proxy de conexões ICA.

Número da porta de confiabilidade da sessão

Esta configuração especifica o número da porta TCP para conexões de confiabilidade da sessão de entrada.

Por padrão, o número da porta é definido como 2598.

Tempo limite de confiabilidade da sessão

Esta configuração especifica a duração, em segundos. Este tempo é o tempo que o proxy de confiabilidade da sessão aguarda um usuário se reconectar antes de permitir que a sessão seja desconectada.

Embora você possa estender o tempo em que uma sessão é mantida aberta, este recurso é uma conveniência e não solicita ao usuário uma nova autenticação. Quanto mais tempo uma sessão permanecer aberta, maiores as chances de um usuário deixar o dispositivo sem supervisão e potencialmente acessível a usuários não autorizados.

Por padrão, o tempo limite é definido como 180 segundos, ou três minutos.

Configurações da política de marca d'água da sessão

A seção de **marca d'água da sessão** inclui configurações de política para configurar este recurso. A habilitação deste recurso causa um aumento significativo na largura de banda da rede e no uso da CPU pela máquina VDA. Recomendamos que você configure a marca d'água da sessão para máquinas VDA selecionadas com base nos seus recursos de hardware disponíveis.

> **Importante**
>
> Habilite a marca d'água da sessão para que as outras configurações de política de marca d'água sejam eficazes. Para obter uma melhor experiência do usuário, não habilite mais de dois itens de texto de marca d'água.

Habilitar marca d'água da sessão

Ao habilitar esta configuração, a exibição da sessão terá uma marca d'água textual opaca exibindo informações específicas da sessão. As outras configurações de marca d'água dependem desta estar habilitada.

Por padrão, a marca d'água da sessão está desabilitada.

Incluir endereço IP do cliente

Ao habilitar esta configuração, a sessão exibe o endereço IP do cliente atual como uma marca d'água.

Por padrão, Incluir endereço IP do cliente está desabilitado.

Incluir tempo de conexão

Ao habilitar esta configuração, a marca d'água da sessão exibe um tempo de conexão. O formato é aaaa/mm/dd hh:mm. A hora exibida é baseada no relógio do sistema e no fuso horário.

Por padrão, Incluir tempo de conexão está desabilitado.

Incluir nome de usuário de logon

Ao habilitar esta configuração, a sessão exibe o nome de usuário de logon atual como uma marca d'água. O formato de exibição é NOME_DE_USUÁRIO@NOME_DE_DOMÍNIO. Recomendamos que o nome de usuário tenha no máximo 20 caracteres. Quando um nome de usuário tem mais de 20 caracteres, fontes de caracteres excessivamente pequenas ou truncamento podem ocorrer e diminuir a eficácia da marca d'água.

Por padrão, Incluir nome de usuário de logon está habilitado.

Incluir nome do host VDA

Quando você habilita esta configuração, a sessão exibe o nome do host VDA da sessão ICA® atual como uma marca d'água.

Por padrão, Incluir nome do host VDA está habilitado.

Incluir endereço IP do VDA

Quando você habilita esta configuração, a sessão exibe o endereço IP do VDA da sessão ICA atual como uma marca d'água.

Por padrão, o endereço IP do VDA está desabilitado.

Estilo da marca d'água da sessão

Esta configuração controla se você exibe um único rótulo de texto de marca d'água ou vários rótulos. Escolha **Múltiplo** ou **Único** no menu suspenso **Valor**.

Múltiplo exibe cinco rótulos de marca d'água na sessão. Um no centro e quatro nos cantos.

Único exibe um único rótulo de marca d'água no centro da sessão.

Por padrão, o estilo da marca d'água da sessão é Múltiplo.

Texto personalizado da marca d'água

Esta configuração permite aplicar texto personalizado (por exemplo, o nome da empresa) para exibir na marca d'água da sessão. Ao configurar uma string não vazia, ela exibe o texto em uma nova linha, anexando outras informações habilitadas na marca d'água. O texto personalizado da

marca d'água é limitado a 25 caracteres Unicode. Se você configurar uma string mais longa, ela será truncada para 25 caracteres.

Não há texto padrão.

A partir do Citrix Virtual Apps and Desktops™ 7 2206, você pode adicionar mais personalização usando tags personalizadas no texto. Como resultado, o número máximo de caracteres no texto personalizado é aumentado para 1024.

As tags disponíveis para as configurações de marca d'água são descritas na tabela a seguir:

TAG	DESCRIÇÃO	EXEMPLO
`<font=value>`	Permite alterar a fonte do texto da marca d'água. O valor é o nome de uma fonte disponível no VDA.	`<font=Courier New>`
`<fontzoom=value>`	Permite definir a porcentagem do fator de zoom da fonte. O valor é 200 para zoom de 200% no texto da marca d'água.	`<fontzoom=200>`
`<position=value>`	Permite alterar a posição do texto da marca d'água. Os valores são `center`, `topleft`, `topright`, `bottomleft` e `bottomright`. Esta tag é aplicável apenas com estilo único.	`<position=topright>`
`<rotation=value>`	Permite girar o texto da marca d'água. O valor é especificado em graus e o intervalo é de -360 a 360.	`<rotation=45>`
`<style=value>`	Permite alterar o estilo de exibição. Esta tag substitui a política de estilo de marca d'água da sessão.	`<style=single>`

Os seguintes estilos de marca d'água estão disponíveis:

- Estilo único - Um único rótulo de texto de marca d'água aparece no centro da sessão. Você pode usar a tag de posição para alterar o local.
- xstyle ou múltiplo - Cinco rótulos de marca d'água aparecem na sessão - um no centro e um em cada canto.
- Lado a lado - Vários rótulos aparecem na sessão. O texto da marca d'água é colocado igualmente em toda a tela.

As tags disponíveis para alterar o texto da marca d'água são descritas na tabela a seguir:

TAG	DESCRIÇÃO
`<clientip>`	O endereço IP do endpoint.
`<date>`	A data em que a sessão foi estabelecida.
`<domain>`	O nome de domínio da conta de usuário logada.
`<hostname>`	O nome da máquina do VDA.
`<newline>`	Cria uma linha extra.
`<serverip>`	O endereço IP do VDA.
`<time>`	A hora em que a sessão foi estabelecida.
`<username>`	O nome do usuário.

Observação:

- A política **Texto personalizado da marca d'água** entra em vigor somente quando a política **Habilitar marca d'água da sessão** está habilitada. Seu valor padrão é *Desabilitado*.
- Se você usar as tags para alterar o texto da marca d'água, todas as outras políticas de marca d'água da sessão, exceto **Habilitar marca d'água da sessão**, serão ignoradas.

> Se você usar as tags para as configurações de texto da marca d'água, poderá usar todas as outras políticas de marca d'água.

Transparência da marca d'água

Você pode especificar a opacidade da marca d'água de 0 a 100. Quanto maior o valor especificado, mais opaca será a marca d'água.

Por padrão, o valor é 17.

Configurações de política de controle de fuso horário

A seção **Controle de Fuso Horário** inclui configurações de política relacionadas ao uso da hora local nas sessões.

Estimar hora local para clientes legados

Essa configuração habilita ou desabilita a estimativa do fuso horário local dos dispositivos do usuário. Esses dispositivos incluem os dispositivos do usuário que enviam informações imprecisas de fuso horário para o servidor.

Por padrão, o servidor estima o fuso horário local quando necessário.

Essa configuração destina-se ao uso com Citrix Receivers legados ou clientes ICA que não enviam informações detalhadas de fuso horário para o servidor. Considere que essa configuração é usada com Citrix Receivers que enviam informações detalhadas de fuso horário para o servidor. Por exemplo, versões compatíveis do Citrix Receiver™ para Windows. Nesse caso, essa configuração não tem efeito.

Restaurar fuso horário do SO da área de trabalho na desconexão ou logoff da sessão

Considere que o usuário se desconecta ou faz logoff de uma sessão. Nesse caso, essa configuração determina se a configuração de fuso horário para um VDA de SO de sessão única é restaurada para o fuso horário original da máquina. Se você habilitar essa configuração, o VDA restaurará o fuso horário da máquina para sua configuração original quando o usuário se desconectar ou fizer logoff. Para que essa configuração entre em vigor, defina **Usar hora local do cliente** como **Usar fuso horário do cliente**.

Por padrão, essa configuração está habilitada.

Usar hora local do cliente

Essa configuração determina a configuração de fuso horário da sessão do usuário. As opções são o fuso horário da sessão do usuário (fuso horário do servidor) ou o fuso horário do dispositivo do usuário (fuso horário do cliente).

Por padrão, o fuso horário da sessão do usuário é usado.

Para que essa configuração entre em vigor, habilite a configuração **Permitir redirecionamento de fuso horário** no Editor de Política de Grupo. A configuração está em **Política de Computador Local** > **Configuração do Computador** > **Modelos Administrativos** > **Componentes do Windows** > **Serviços de Área de Trabalho Remota** > **Host da Sessão da Área de Trabalho Remota** > **Redirecionamento de Dispositivo e Recurso**.

Se você estiver usando VDA de sessão única (anteriormente conhecido como VDA de Estação de Trabalho) em máquinas que executam um SO de servidor, configure o direito de usuário local **Alterar o fuso horário** para **Todos**. Esse direito de usuário pode ser encontrado em **Política de Computador Local** > **Configuração do Computador** > **Configurações do Windows** > **Configurações de Segurança** > **Políticas Locais** > **Atribuição de Direitos de Usuário**.

> **Observação:**
>
> Em um SO de sessão única, os **Usuários** estão incluídos na Atribuição de Direitos de Usuário **Alterar o fuso horário**, embora não em um SO de várias sessões. Em um SO de várias sessões, o fuso horário é sincronizado usando a seguinte política de grupo: Configuração do Computador\Modelos Administrativos\Componentes do Windows\Serviços de Área de Trabalho Remota\Host da Sessão da Área de Trabalho Remota\Redirecionamento de Dispositivo e Recurso\Permitir redirecionamento de fuso horário. Essa política é aplicável quando o Servidor é um Host da Sessão da Área de Trabalho Remota no VDA de SO de várias sessões (instalado com o comando `/ServerVDI`). Em um SO de várias sessões, por padrão e por design, os usuários não têm o direito local de alterar o fuso horário.

Configurações de política de dispositivos TWAIN

A seção **Dispositivos TWAIN** inclui configurações de política relacionadas ao seguinte:

- Mapeamento de dispositivos TWAIN do cliente, como câmeras digitais ou scanners
- Otimização de transferências de imagem do servidor para o cliente

Observação:

O TWAIN 2.0 é compatível com o Citrix Receiver para Windows 4.5.

Redirecionamento de dispositivo TWAIN do cliente

Os dispositivos TWAIN se comunicam com aplicativos de processamento de imagem hospedados no servidor usando o protocolo TWAIN.

Essa configuração permite ou impede que os usuários acessem dispositivos TWAIN no dispositivo do usuário. Por padrão, o redirecionamento de dispositivo TWAIN é permitido.

As seguintes configurações de política estão relacionadas:

- Nível de compactação TWAIN
- Limite de largura de banda de redirecionamento de dispositivo TWAIN
- Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN

Nível de compactação TWAIN

Essa configuração especifica o nível de compactação das transferências de imagem do cliente para o servidor. Use Baixo para melhor qualidade de imagem, Médio para boa qualidade de imagem ou Alto para baixa qualidade de imagem. Por padrão, a compactação média é aplicada.

Configurações de política de dispositivos USB

A seção **Dispositivos USB** inclui configurações de política para gerenciar o redirecionamento de arquivos para dispositivos USB.

Regras de otimização de dispositivos USB do cliente

As regras de otimização de dispositivos USB do cliente podem ser aplicadas aos dispositivos para desativar a otimização ou para alterar o modo de otimização.

Quando um usuário conecta um dispositivo de entrada USB, o host verifica se as configurações da **política USB** permitem o dispositivo. Se o dispositivo for permitido, o host verifica as **regras de otimização de dispositivos USB do cliente** para o dispositivo. Se nenhuma regra for especificada, o dispositivo não será otimizado. O modo de captura (04) é o modo recomendado para dispositivos de assinatura. Para outros dispositivos que apresentam desempenho degradado em latências mais altas, os administradores podem habilitar o modo interativo (02). Consulte as descrições dos modos disponíveis na tabela neste artigo.

É bom saber

- Para o uso de mesas digitalizadoras e tablets Wacom, recomendamos que você desative o protetor de tela. As etapas sobre como desativar o protetor de tela estão no final desta seção.
- O suporte para a otimização de mesas digitalizadoras e tablets da série Wacom STU foi pré-configurado na instalação das políticas do Citrix Virtual Apps and Desktops™.
- Dispositivos de assinatura funcionam em todo o Citrix Virtual Apps and Desktops e não exigem um driver para serem usados como um dispositivo de assinatura. A Wacom possui mais software que pode ser instalado para personalizar ainda mais o dispositivo. Consulte `<http://www.wacom.com/>`.
- Mesas digitalizadoras. Certos dispositivos de entrada de desenho podem se apresentar como um dispositivo HID em barramentos PCI/ACPI e não são suportados. Conecte esses dispositivos a um controlador de host USB no cliente para serem redirecionados dentro de uma sessão do Citrix Virtual Desktops.

As regras de política seguem o formato de expressões tag=valor separadas por espaço em branco. As seguintes tags são suportadas:

NOME DA TAG	DESCRIÇÃO
Modo	O modo de otimização é suportado para dispositivos de entrada para class=**03**. Os modos suportados são: Sem otimização - valor **01**. Modo interativo - valor **02**. Recomendado para dispositivos como tablets de caneta e mouses 3D Pro. Modo de captura - valor **04**. Preferencial para dispositivos como mesas de assinatura.
VID	ID do fornecedor do descritor do dispositivo, como um número hexadecimal de quatro dígitos.
PID	ID do produto do descritor do dispositivo, como um número hexadecimal de quatro dígitos.
REV	ID de revisão do descritor do dispositivo, como um número hexadecimal de quatro dígitos.
Classe	Classe do descritor do dispositivo ou de um descritor de interface.

NOME DA TAG	DESCRIÇÃO
Subclasse	Subclasse do descritor do dispositivo ou de um descritor de interface.
Prot	Protocolo do descritor do dispositivo ou de um descritor de interface.

Exemplos

Mode=00000004 VID=067B PID=1230 class=03 #Dispositivo de entrada operando no modo de captura

Mode=00000002 VID=067B PID=1230 class=03 #Dispositivo de entrada operando no modo interativo (padrão)

Mode=00000001 VID=067B PID=1230 class=03 #Dispositivo de entrada operando sem qualquer otimização

Mode=00000100 VID=067B PID=1230 # Otimização de configuração do dispositivo desabilitada (padrão)

Mode=00000200 VID=067B PID=1230 # Otimização de configuração do dispositivo habilitada

Desativando o protetor de tela para dispositivos de mesa digitalizadora Wacom

Para o uso de mesas digitalizadoras e tablets Wacom, a Citrix® recomenda que você desative o protetor de tela da seguinte forma:

1. Instale o **Wacom-STU-Driver** após redirecionar o dispositivo.
2. Instale o **Wacom-STU-Display MSI** para ter acesso ao painel de controle da mesa digitalizadora.
3. Vá para **Painel de Controle > Wacom STU Display > STU430** ou **STU530** e selecione a guia do seu modelo.
4. Escolha **Alterar** e, em seguida, selecione **Sim** quando a janela de segurança do UAC aparecer.
5. Selecione **Desativar apresentação de slides** e, em seguida, **Aplicar**.

Depois que a configuração é definida para um modelo de mesa digitalizadora, ela é aplicada a todos os modelos.

Redirecionamento de dispositivo USB do cliente

Essa configuração permite ou impede o redirecionamento de dispositivos USB para e do dispositivo do usuário.

Por padrão, os dispositivos USB não são redirecionados.

Regras de redirecionamento de dispositivo USB do cliente

Essa configuração especifica as regras de redirecionamento para dispositivos USB.

Por padrão, nenhuma regra é especificada.

Quando um usuário conecta um dispositivo USB, o dispositivo host o verifica em relação a cada regra de política, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva. Se a primeira correspondência for uma regra de Permissão, o dispositivo é remotado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo estará disponível apenas para o desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

As regras da política têm o formato {Permitir: | Negar:} seguido por um conjunto de expressões tag=valor separadas por espaço em branco. Os seguintes tags são suportados:

NOME DA TAG	DESCRIÇÃO
VID	ID do Fornecedor do descritor do dispositivo
PID	ID do Produto do descritor do dispositivo
REL	ID da Versão do descritor do dispositivo
Classe	Classe do descritor do dispositivo ou de um descritor de interface
Subclasse	Subclasse do descritor do dispositivo ou de um descritor de interface
Prot	Protocolo do descritor do dispositivo ou de um descritor de interface

Ao criar regras de política, lembre-se:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por #.

- Linhas em branco e linhas de comentário puro são ignoradas.
- As tags devem usar o operador de correspondência = (por exemplo, VID=067B_.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.
- Consulte os códigos de classe USB disponíveis no site da USB Implementers Forum, Inc.

Exemplos de regras de política USB definidas pelo administrador:

- Allow: VID=067B PID=0007 # Outra Indústria, Outro Pen Drive
- Deny: Class=08 subclass=05 # Armazenamento em Massa
- Para criar uma regra que nega todos os dispositivos USB, use "DENY:" sem outras tags.

Redirecionamento de dispositivo plug and play USB do cliente

Essa configuração permite ou impede que dispositivos plug-and-play, como câmeras ou dispositivos de ponto de venda (POS), sejam usados em uma sessão de cliente.

Por padrão, o redirecionamento de dispositivos plug-and-play é permitido. Quando definido como Permitido, todos os dispositivos plug-and-play para um usuário ou grupo específico são redirecionados. Quando definido como Proibido, nenhum dispositivo é redirecionado.

Configurar o redirecionamento automático de dispositivos USB

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB.

> **Observação:**
>
> No Receiver para Windows 4.2, os dispositivos USB também são redirecionados automaticamente ao operar no modo de Dispositivo de Área de Trabalho. Além disso, a barra de conexão não está presente. Em versões anteriores do Citrix Receiver para Windows, os dispositivos USB também são redirecionados automaticamente ao operar no seguinte:
>
> - Modo de dispositivo de área de trabalho
> - Aplicativos hospedados em máquina virtual (VM)

> Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use as DeviceRules no endpoint do cliente ou na política DDC. Consulte os Guias de Administração para obter mais detalhes.

> **Cuidado:**

> O uso incorreto do Editor do Registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

CONFIGURAÇÕES DE PREFERÊNCIAS DO USUÁRIO PARA REDIRECIONAMENTO AUTOMÁTICO DE DISPOSITIVOS USB

Política:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.
2. Abra **Novos Dispositivos USB**, selecione **Habilitado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Habilitado** e clique em **OK**.

Citrix Receiver:

1. Vá para **Preferências do Citrix Receiver > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
   - Quando uma sessão é iniciada, conectar dispositivos automaticamente
   - Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

Todas as chaves de registro e as alterações de política são aplicadas ao dispositivo cliente Windows.

REDIRECIONAMENTO DE IMPRESSORAS USB SIMPLES

A melhor solução para impressoras USB simples é usar o Driver de Impressora Universal dedicado e o canal virtual para realizar a impressão. Por padrão, as impressoras USB simples não são redirecionadas automaticamente.

As impressoras simples são detectadas usando heurísticas. Além disso, espera-se que impressoras avançadas com funções de digitalização, por exemplo, possam precisar ser redirecionadas usando o suporte USB para funcionar completamente.

Use este registro para configurar se as impressoras simples são redirecionadas automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Tipo: DWORD

Data: 00000000

O valor padrão é 0 (não redireciona automaticamente). Alterar o valor para qualquer número maior que zero habilita o suporte USB para redirecionar impressoras USB simples.

Você também pode implantar políticas do Active Directory para esta chave de registro e substituir o valor não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Name: AutoRedirectPrinters

Tipo: DWORD

Data: 00000000

REDIRECIONAMENTO DE DISPOSITIVOS DE ÁUDIO SIMPLES

Assim como as impressoras simples, a melhor experiência do usuário é alcançada usando o canal virtual de áudio dedicado do ICA® para enviar dados de áudio de dispositivos de áudio simples. No entanto, você pode precisar redirecionar alguns dispositivos especiais usando o suporte USB. Heurísticas são usadas para determinar quais dispositivos são dispositivos de áudio simples.

Use este registro no endpoint do cliente para configurar se os dispositivos de áudio simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos de áudio USB simples com suporte USB.

Você pode usar políticas do Active Directory para implantar este valor na chave do registro e substituir o valor não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

REDIRECIONAMENTO DE DISPOSITIVOS DE ARMAZENAMENTO SIMPLES (DISPOSITIVO DE ARMAZENAMENTO EM MASSA)

Para dispositivos de armazenamento simples, você obtém a melhor experiência do usuário usando o canal virtual dedicado, como o mapeamento de unidade cliente que também realiza otimização. Além de simplesmente ler ou gravar arquivos, para executar certas tarefas especiais como gravar um CD/DVD ou acessar dispositivos de sistemas de arquivos criptografados, o dispositivo ainda pode precisar ser redirecionado usando o suporte USB genérico.

Heurísticas são usadas para determinar quais dispositivos são dispositivos de armazenamento simples. Use esta chave de registro para configurar se os dispositivos de armazenamento simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos de armazenamento USB simples usando o suporte USB genérico.

Você também pode usar políticas do Active Directory para implantar este valor na seguinte chave de registro e substituir o valor não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

> **Observação:**
>
> O acesso somente leitura ao dispositivo de armazenamento simples não é configurável se você estiver usando o suporte USB genérico, enquanto é configurável se estiver usando CDM.

REDIRECIONAMENTO DE UNIDADES FLASH USB COM CRIPTOGRAFIA DE HARDWARE

As unidades flash USB com criptografia de hardware geralmente consistem em uma partição de armazenamento criptografada e uma segunda partição de *utilitário* que contém um utilitário para desbloquear a partição criptografada. Para dispositivos de unidade flash USB, obtenha a melhor experiência do usuário usando o canal virtual HDX dedicado de mapeamento de unidade cliente/ mapeamento de unidade removível dinâmica que também realiza otimização.

O redirecionamento USB genérico é necessário para o seguinte:

- Clientes não-Windows (por exemplo, clientes Linux)
- Clientes onde o cliente restringiu (bloqueou) o acesso do usuário a funções locais no cliente

O redirecionamento USB genérico pode redirecionar qualquer dispositivo de armazenamento USB sem criptografia de hardware para sessões VDA de SO de sessão única e SO de múltiplas sessões.

Antes do Citrix Virtual Apps and Desktops 7 1808, as unidades flash USB com criptografia de hardware não podiam ser redirecionadas de forma útil para sessões VDA de SO de sessão única ou SO de múltiplas sessões. Uma nova melhoria de recurso introduzida no Citrix Virtual Apps and Desktops 7 1808 oferece suporte ao redirecionamento USB genérico de unidades flash USB com criptografia de hardware para sessões VDA de SO de sessão única e SO de múltiplas sessões. Depois que o dispositivo é redirecionado, nenhuma de suas unidades aparece no cliente local.

Portanto, se o desbloqueio da unidade for necessário, execute-o na sessão. Este recurso requer a atualização do Windows KB4074590.

DISPOSITIVOS DE IMAGEM ESTÁTICA SIMPLES (SCANNERS E CÂMERAS DIGITAIS)

Para dispositivos de imagem estática simples, obtenha a melhor experiência do usuário usando o canal virtual dedicado (como o canal virtual TWAIN) que também realiza otimização. Esses dispositivos devem aderir aos padrões da indústria. Considere que um dispositivo não está em conformidade ou não é usado de acordo com as intenções originais. Neste caso, o redirecionamento USB genérico pode ser a única maneira de usar o dispositivo. Heurísticas são usadas para determinar quais dispositivos são dispositivos de imagem estática simples.

Use esta chave de registro para configurar se dispositivos de imagem estática simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterar o valor para diferente de zero redireciona dispositivos USB de imagem estática simples com USB genérico.

Você também pode usar políticas do Active Directory para implantar este valor nesta chave de registro e substituir o valor não-político se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dados: 00000000

CONFIGURAÇÕES ESPECÍFICAS DO DISPOSITIVO

As heurísticas usadas para selecionar dispositivos otimizáveis do Citrix nem sempre correspondem ao que você deseja. Os exemplos de dispositivos otimizáveis do Citrix são impressoras, áudio, vídeo, armazenamento e dispositivos de imagem estática. Você pode querer controlar o redirecionamento automático de dispositivos que não estão listados acima. Você pode controlar o redirecionamento automático com base em cada dispositivo.

Por exemplo, o leitor de código de barras DemoTech 2.000 não precisa ser redirecionado usando o suporte USB. Ele tem um identificador de fornecedor de 12AB e um identificador de produto de 5678. Esses números hexadecimais podem ser encontrados no Gerenciador de Dispositivos.

Para evitar que isso seja redirecionado automaticamente, crie esta chave de registro específica do dispositivo:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dados: 00000000

Um valor de 0 impede que o dispositivo seja redirecionado automaticamente. Um valor diferente de zero indica que o dispositivo deve ser considerado para redirecionamento automático (sujeito às preferências do usuário). Há um único caractere de espaço entre os identificadores de fornecedor e produto.

Você também pode implantar este valor usando políticas do Active Directory para esta chave de registro. Ele substitui o valor não-político se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nome: AutoRedirect

Tipo: DWORD

Dados: 00000000

As configurações de AutoRedirect específicas do dispositivo têm precedência sobre os valores AutoRedirectXXX mais gerais explicados acima. As heurísticas padrão para dispositivos otimizados da Citrix podem interpretar um dispositivo como genérico. Portanto, defina o valor AutoRedirect específico do dispositivo como 1 para redirecioná-lo automaticamente.

Permitir que dispositivos USB existentes sejam conectados automaticamente

Esta configuração permite ou impede a conexão automática dos dispositivos USB existentes que estão conectados ao endpoint no início de uma sessão à sessão remota.

Ao adicionar esta configuração a uma política, selecione uma das seguintes opções:

- Perguntar antes de redirecionar dispositivos USB disponíveis.

- Não redirecionar automaticamente dispositivos USB disponíveis.
- Redirecionar automaticamente dispositivos USB disponíveis.

Por padrão, a opção **Perguntar antes de redirecionar dispositivos USB disponíveis** está selecionada. Com base na política selecionada, a opção selecionada na seção **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Observação:**
>
> Atualmente, a política **Permitir que dispositivos USB existentes sejam conectados automaticamente** é aplicável apenas para o aplicativo Citrix Workspace™ para Windows.

Permitir que dispositivos USB recém-chegados sejam conectados automaticamente

Esta configuração permite ou impede a conexão automática de dispositivos USB inseridos no endpoint durante uma sessão para a sessão remota.

Ao adicionar esta configuração a uma política, selecione uma das seguintes opções:

- Perguntar antes de redirecionar dispositivos USB disponíveis.
- Não redirecionar automaticamente dispositivos USB disponíveis.
- Redirecionar automaticamente dispositivos USB disponíveis.

Por padrão, a opção **Perguntar antes de redirecionar dispositivos USB disponíveis** é selecionada. Com base na política selecionada, a opção selecionada na seção **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Observação:**
>
> Atualmente, a política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente** é aplicável apenas para o Citrix Workspace app para Windows.

Regras de redirecionamento de dispositivo USB do cliente (Versão 2)

Esta configuração especifica regras para filtrar, dividir e conectar automaticamente dispositivos USB a uma sessão remota.

Quando esta configuração é selecionada, o host substitui a configuração *Regras de redirecionamento de dispositivo USB do cliente* pelas regras de dispositivo configuradas nesta configuração.

Para obter mais informações, consulte Configurando o redirecionamento de dispositivo USB composto.

Configurações da política de lista de permissões de canais virtuais

A configuração de política **Lista de permissões de canais virtuais** permite o uso de uma lista de permissões que especifica quais canais virtuais podem ser abertos em uma sessão ICA®.

Quando desativado, todos os canais virtuais são permitidos.

Quando ativado, apenas os canais virtuais Citrix® são permitidos.

Para usar canais virtuais personalizados ou de terceiros, adicione os canais virtuais à lista. Para adicionar um canal virtual à lista:

1. Insira o nome do canal virtual seguido por uma vírgula.
2. Insira o caminho para o processo que acessa o canal virtual.

Mais caminhos executáveis podem ser listados, e os caminhos são separados por vírgulas.

Por exemplo,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

A partir do Citrix Virtual Apps and Desktops 7 2109, as listas de permissões de canais virtuais são ativadas por padrão. Para obter mais informações sobre como adicionar canais virtuais à lista de permissões, consulte Adicionar canais virtuais à lista de permissões

Se você estiver usando o HDX RealTime Optimization Pack para Skype for Business, adicione o canal virtual à lista de permissões. Para obter mais informações, consulte a documentação do HDX RealTime Optimization Pack.

> **Importante:**
>
> As máquinas VDA devem ser reiniciadas para que a configuração entre em vigor.

> Para obter mais informações sobre canais virtuais, consulte Canais virtuais ICA.

Registro da lista de permissões de canais virtuais

Você pode usar esta configuração de política para configurar o nível de registro da Lista de Permissões de Canais Virtuais.

As seguintes opções estão disponíveis:

Opções	Descrição
Desativado	Desativa todos os eventos de log.
Registrar apenas avisos	Os eventos são registrados apenas para Canais Virtuais personalizados que tentam abrir e que não fazem parte da lista de permissões.
Registrar todos os eventos	Todos os eventos são registrados

Limitação de log da lista de permissões de canais virtuais

Você pode usar esta configuração de política para configurar a frequência de registro de eventos para uma sessão ativa.

Todos os eventos para cada canal virtual serão registrados em sua primeira ocorrência. Eventos repetidos serão suprimidos durante o período de limitação enquanto a sessão estiver ativa. Se uma sessão for desconectada, o período de limitação será redefinido.

Lista de permissões de canais virtuais para DVC

Permite o uso de uma lista de permissões que especifica quais canais virtuais dinâmicos podem ser abertos em uma sessão ICA.

Quando desativado, todos os canais virtuais dinâmicos são permitidos.

Quando ativado, nenhum canal virtual dinâmico é permitido. Para usar canais virtuais dinâmicos (DVC) com este recurso, os DVCs devem ser adicionados à lista. Para adicionar um DVC à lista, insira o caminho para o processo que acessa o DVC no host da sessão, seguido por uma vírgula, depois o nome do plug-in do lado do cliente, seguido por uma vírgula e o nome do listener usado pelo plug-in. Vários nomes de listener podem ser adicionados separados por vírgulas.

Você pode usar um curinga para permitir todos os listeners suportados pelo plug-in.

Você também pode usar um curinga para substituir um único nome de diretório no caminho do processo, parte de um nome de diretório no caminho do processo, substituir o nome do executável ou substituir parte do nome do executável.

As alterações nesta configuração só serão aplicadas após a reinicialização do host da sessão.

Exemplo: Plug-ins do lado do cliente: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

Entrada da lista de permissões: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

Configurações de política de exibição visual

A seção **Exibição Visual** inclui configurações de política para controlar a qualidade das imagens que são enviadas de desktops virtuais para o dispositivo do usuário.

Profundidade de cor preferencial para gráficos simples

Esta configuração de política está disponível nas versões VDA 7.6 FP3 e posteriores. A opção de 8 bits está disponível nas versões VDA 7.12 e posteriores.

Esta configuração possibilita diminuir a profundidade de cor na qual gráficos simples são enviados pela rede. A redução para 8 bits ou 16 bits por pixel pode melhorar a capacidade de resposta em conexões de baixa largura de banda. No entanto, esta ação pode causar uma ligeira degradação na qualidade da imagem. A profundidade de cor de 8 bits não é suportada quando a configuração de política Usar codec de vídeo para compressão está definida como **Para a tela inteira**.

A profundidade de cor preferencial padrão é de 24 bits por pixel.

Os VDAs voltam para a profundidade de cor de 24 bits (padrão) se a configuração de 8 bits for aplicada na versão VDA 7.11 e anteriores.

Taxa de quadros alvo

Esta configuração especifica o número máximo de quadros por segundo enviados do desktop virtual para o dispositivo do usuário.

Por padrão, o máximo é de 30 quadros por segundo.

Definir um alto número de quadros por segundo (por exemplo, 30) melhora a experiência do usuário, mas requer mais largura de banda. Diminuir o número de quadros por segundo (por exemplo, 10) maximiza a escalabilidade do servidor em detrimento da experiência do usuário.

Para dispositivos de usuário com CPUs mais lentas, especifique um valor menor para melhorar a experiência do usuário.

A taxa de quadros máxima suportada por segundo é 60.

Qualidade visual

Esta configuração especifica a qualidade visual desejada para as imagens exibidas no dispositivo do usuário.

Por padrão, esta configuração é Média.

Para especificar a qualidade das imagens, escolha uma das seguintes opções:

- **Baixa** - Recomendado para redes com largura de banda limitada, onde a qualidade visual pode ser sacrificada em prol da interatividade
- **Média** - Oferece o melhor desempenho e eficiência de largura de banda na maioria dos casos de uso
- **Alta** - Recomendado se você precisar de qualidade de imagem visualmente sem perdas
- **Construir para sem perdas** - Envia imagens com perdas para o dispositivo do usuário durante períodos de alta atividade de rede e imagens sem perdas após a redução da atividade de rede. Essa configuração melhora o desempenho em conexões de rede com largura de banda limitada
- **Sempre sem perdas** - Quando a preservação dos dados da imagem é vital, selecione **Sempre sem perdas** para garantir que dados com perdas nunca sejam enviados para o dispositivo do usuário. Por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável.

Configurações de política de imagens em movimento

A seção **Imagens em Movimento** contém configurações que permitem remover ou alterar a compactação para imagens dinâmicas.

QUALIDADE MÍNIMA DA IMAGEM

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está ativada.

Esta configuração especifica a qualidade mínima aceitável da imagem para o Adaptive Display. Quanto menos compactação for usada, maior será a qualidade das imagens exibidas. Escolha entre compactação Ultra Alta, Muito Alta, Alta, Normal ou Baixa.

Por padrão, isso é definido como Normal.

COMPACTAÇÃO DE IMAGEM EM MOVIMENTO

Esta configuração especifica se o Adaptive Display está ativado ou não. O Adaptive Display ajusta automaticamente a qualidade da imagem de vídeos e slides de transição em apresentações de slides com base na largura de banda disponível. Com o Adaptive Display ativado, os usuários devem ver apresentações fluindo sem redução na qualidade.

Por padrão, o Adaptive Display está ativado.

Para as versões 7.0 a 7.6 do VDA, esta configuração se aplica somente quando o modo gráfico herdado está ativado. Para as versões 7.6 FP1 e posteriores do VDA, esta configuração se aplica quando o modo gráfico herdado está ativado, ou quando o modo gráfico herdado está desativado e um codec de vídeo não é usado para compactar gráficos.

Quando o modo gráfico herdado está ativado, a sessão deve ser reiniciada para que as alterações de política entrem em vigor. O Adaptive Display é mutuamente exclusivo com o Progressive Display; ativar o Adaptive Display desativa o Progressive Display e vice-versa. No entanto, tanto o Progressive Display quanto o Adaptive Display podem ser desativados ao mesmo tempo. O Progressive Display, como um recurso herdado, não é recomendado para XenApp ou XenDesktop. Definir o Nível de Limite Progressivo desativará o Adaptive Display.

NÍVEL DE COMPRESSÃO PROGRESSIVA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está ativada.

Esta configuração fornece uma exibição inicial de imagens menos detalhada, mas mais rápida.

Por padrão, nenhuma compactação progressiva é aplicada.

A imagem mais detalhada, definida pela configuração de compactação com perdas normal, aparece quando disponível. Use compactação Muito Alta ou Ultra Alta para uma visualização aprimorada de gráficos que consomem muita largura de banda, como fotografias.

Para que a compressão progressiva seja eficaz, seu nível de compressão deve ser maior do que a configuração de nível de compressão com perdas.

Nota: O nível aumentado de compressão associado à compressão progressiva também aprimora a interatividade de imagens dinâmicas em conexões de cliente. A qualidade de uma imagem dinâmica, como um modelo tridimensional rotativo, é temporariamente diminuída até que a imagem pare de se mover, momento em que a configuração normal de compressão com perdas é aplicada.

As seguintes configurações de política estão relacionadas:

- Valor limite de compressão progressiva
- Compressão progressiva pesada

VALOR LIMITE DE COMPRESSÃO PROGRESSIVA

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está ativada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual a compressão progressiva é aplicada. Isso é aplicado apenas a conexões de cliente abaixo dessa largura de banda.

Por padrão, o valor limite é de 2147483647 kilobits por segundo.

As seguintes configurações de política estão relacionadas:

- Valor limite de compressão progressiva
- Compressão progressiva pesada

TAXA DE QUADROS MÍNIMA DE DESTINO

Esta configuração especifica a taxa de quadros mínima por segundo que o sistema tenta manter, para imagens dinâmicas, em condições de baixa largura de banda.

Por padrão, isso é definido como 10fps.

Para versões VDA 7.0 a 7.6, esta configuração se aplica somente quando o modo gráfico herdado está ativado. Para versões VDA 7.6 FP1 e posteriores, esta configuração se aplica quando o modo gráfico herdado está desativado ou ativado.

> **Observação:**
>
> A política de taxa de quadros mínima de destino foi descontinuada e está definida para 10 fps. Isso pode ser alterado pelos usuários finais usando o controle deslizante de Qualidade no indicador de status gráfico.

Configurações de política de imagens estáticas

A seção **Imagens Estáticas** contém configurações que permitem remover ou alterar a compactação de imagens estáticas.

COMPACTAÇÃO DE COR EXTRA

Essa configuração habilita ou desabilita o uso de compactação de cor extra em imagens entregues por conexões de cliente com largura de banda limitada, melhorando a capacidade de resposta ao reduzir a qualidade das imagens exibidas.

Por padrão, a compactação de cor extra está desabilitada.

Quando habilitada, a compactação de cor extra é aplicada somente quando a largura de banda da conexão do cliente está abaixo do valor limite de compactação de cor extra. Quando a largura de banda da conexão do cliente está acima do valor limite ou a opção Desabilitado é selecionada, a compactação de cor extra não é aplicada.

LIMITE DE COMPACTAÇÃO DE COR EXTRA

Observação: Para o Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

Essa configuração representa a largura de banda máxima em kilobits por segundo para uma conexão abaixo da qual a compactação de cor extra é aplicada. Se a largura de banda da conexão do cliente cair abaixo do valor definido, a compactação de cor extra, se habilitada, será aplicada.

Por padrão, o valor limite é de 8192 kilobits por segundo.

COMPACTAÇÃO PESADA

Observação: Para o Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração de política de modo gráfico herdado está habilitada.

Essa configuração habilita ou desabilita a redução da largura de banda além da compactação progressiva sem perda de qualidade da imagem, usando um algoritmo gráfico mais avançado, mas que exige mais CPU.

Por padrão, a compactação pesada está desabilitada.

Se habilitada, a compactação pesada se aplica a todas as configurações de compactação com perdas. Ela é suportada no aplicativo Citrix Workspace™ mas não tem efeito em outros plug-ins.

As seguintes configurações de política estão relacionadas:

- Nível de compressão progressiva
- Valor limite de compactação progressiva

NÍVEL DE COMPACTAÇÃO COM PERDAS

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política do modo gráfico herdado está ativada.

Esta configuração controla o grau de compactação com perdas usado em imagens entregues por conexões de cliente que são limitadas em largura de banda. Nesses casos, exibir imagens sem compactação pode ser lento.

Por padrão, a compactação média é selecionada.

Para melhorar a capacidade de resposta com imagens que consomem muita largura de banda, use alta compactação. Onde a preservação dos dados da imagem é vital; por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável, você pode não querer usar compactação com perdas.

Configuração de política relacionada: Valor limite de compactação com perdas

VALOR LIMITE DE COMPACTAÇÃO COM PERDAS

Nota: Para o Virtual Delivery Agent 7.x, esta configuração de política se aplica somente quando a configuração de política do modo gráfico herdado está ativada.

Esta configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual a compactação com perdas é aplicada.

Por padrão, o valor limite é 2147483647 kilobits por segundo.

Adicionar a configuração Nível de compactação com perdas a uma política e não incluir nenhum limite especificado pode melhorar a velocidade de exibição de bitmaps de alta detalhes, como fotografias, em uma LAN.

Configuração de política relacionada: Nível de compactação com perdas

Configurações de política de WebSockets

A seção **WebSockets** inclui configurações de política para acessar desktops virtuais e aplicativos hospedados usando o aplicativo Citrix Workspace™ para HTML5. O recurso WebSockets aumenta a segurança e reduz a sobrecarga ao conduzir a comunicação bidirecional entre aplicativos baseados em navegador e servidores. O recurso faz isso sem abrir várias conexões HTTP.

Conexões WebSockets

Esta configuração permite ou proíbe conexões WebSockets.

Por padrão, as conexões WebSocket são proibidas.

Número da porta WebSockets

Esta configuração identifica a porta para conexões WebSocket de entrada.

Por padrão, o valor é 8008.

Lista de servidores de origem confiáveis de WebSockets

Esta configuração fornece uma lista separada por vírgulas de servidores de origem confiáveis, geralmente o aplicativo Citrix Workspace para Web, expressos como URLs. O servidor aceita apenas conexões WebSockets originadas de um desses endereços.

Por padrão, o curinga * é usado para confiar em todas as URLs do aplicativo Citrix Workspace para Web.

Se você optar por digitar um endereço na lista, use esta sintaxe:

\<protocol>://\<Nome de domínio totalmente qualificado do host>:

O protocolo deve ser HTTP ou HTTPS. Se a porta não for especificada, a porta 80 será usada para HTTP e a porta 443 para HTTPS.

O curinga `*` pode ser usado dentro da URL, exceto como parte de um endereço IP (`10.105.*.*`).

Configurações de política de dispositivos WIA

A seção **Dispositivos WIA** inclui configurações de política para gerenciar o redirecionamento de scanner usando o Windows Image Acquisition (WIA).

Redirecionamento WIA

Dispositivos WIA, como câmeras digitais e scanners, se comunicam com aplicativos de processamento de imagem hospedados em servidor usando a estrutura WIA. Essa configuração permite ou proíbe que os usuários acessem dispositivos WIA no dispositivo do usuário. Por padrão, o redirecionamento WIA é proibido.

Para obter informações sobre dispositivos compatíveis com WIA, consulte Dispositivos WIA.

Recursos HDX™ gerenciados através do registro

> **Observação:**

> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> Para abrir o Editor do Registro, execute `regedit.exe` no servidor. Em seguida, navegar até a chave do registro para adicionar ou editar as configurações.

Dispositivos

Teclados Bloomberg

O Citrix Virtual Apps and Desktops™ oferece suporte aos teclados Bloomberg modelo 4 e modelo 3 starboard. Por padrão, o suporte para o teclado Bloomberg aprimorado está desabilitado.

Para habilitar o suporte ao teclado Bloomberg, defina o seguinte valor de registro na máquina cliente antes de iniciar uma conexão:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Nome do valor**: `EnableBloombergHID`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `0` - Desabilitar
  - `1` - Habilitar

Para obter mais informações, consulte Teclado Bloomberg.

Unidades de cliente mapeadas

Como precaução de segurança, quando um usuário faz login no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades do cliente sem permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis localizados em unidades de cliente mapeadas, substitua esse padrão editando o registro no servidor.

Para permitir o acesso, edite o seguinte valor do registro (crie **CDMSettings** se não existir):

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **Nome do valor**: `ExecuteFromMappedDrive`
- **Tipo de valor**: `DWORD`

- **Dados do valor**:
  - `1` - Permitir permissão
  - `0` - Negar permissão em unidades mapeadas

A alteração entra em vigor para as sessões conectadas após a edição do registro.

O Citrix Virtual Apps and Desktops 7 2006 é a primeira versão a conter este local de registro. Versões anteriores do Citrix Virtual Apps and Desktops usavam um local de registro diferente.

Para obter mais informações, consulte Mapeamento de Unidade Cliente.

Canetas Microsoft Surface Pro e Surface Book

O Citrix Virtual Apps and Desktops oferece suporte à funcionalidade padrão de caneta com aplicativos baseados em Windows Ink. Por padrão, esse recurso está habilitado.

Para desabilitar ou habilitar esse recurso, defina o seguinte valor do registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Nome do valor**: `DisablePen`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desabilitar
  - `0` - Habilitar

Para obter mais informações, consulte Canetas Microsoft Surface Pro e Surface Book.

Lista de permissões de aplicativos do Windows Image Acquisition

Essa configuração permite controlar quais aplicativos no VDA podem acessar o redirecionamento de scanner da Aquisição de Imagens do Windows.

Por padrão, nenhum aplicativo tem acesso à Aquisição de Imagens do Windows.

Para ajustar a Aquisição de Imagens do Windows para aplicativos no VDA, crie a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **Nome do valor**: `WIAAllowedProcesses`

Selecione e clique com o botão direito em **WIAAllowedProcesses**. Escolha **Novo > Valor de Cadeia de Caracteres Múltiplas** e renomeie o novo valor para **AllowProcesses**.

- Dados do valor: Insira o caminho completo e o nome do processo para cada aplicativo que pode acessar a Aquisição de Imagens do Windows. Forneça cada aplicativo em uma nova linha.

Quaisquer alterações a essa configuração entrarão em vigor na próxima vez que você iniciar uma sessão no VDA.

Geral

HDX Reducer

Você pode configurar a versão do algoritmo de compactação HDX (Reducer) que deseja usar no host da sessão.

Para habilitar o Reducer V4 em um VDA de sessão única, defina o seguinte valor de registro:

Chave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **Nome do valor**: `ReducerOverrideMask` **Tipo de valor**: `DWORD` **Dados do valor**: `23` (Decimal)

Para habilitar o Reducer V4 em um VDA de várias sessões, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nome do valor**: `ReducerOverrideMask`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `23` (Decimal)

Configurar tempo limite de EDT

Você pode configurar o tempo limite de EDT para qualquer valor entre 5 e 25 segundos no VDA. O valor padrão do tempo limite de EDT é de 25 segundos.

- **Chave**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **Tipo de valor**: `DWORD`
- **Nome do valor**: `edtConnectionTimeout`
- **Dados do valor**: tempo em segundos entre 5 e 25 (decimal)

Você também pode configurar o tempo limite para o aplicativo Citrix Workspace™ para Windows:

- **Chave**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **Tipo de valor**: `String / REG_SZ`
- **Nome do valor**: `edtConnectionTimeout`
- **Dados do valor**: tempo em segundos entre 5 e 25 (decimal)

Configurar a versão do Rendezvous

Para configurar a versão do Rendezvous a ser usada, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **Tipo de valor**: `DWORD`
- **Nome do valor**: `GctRegistration`
- **Dados do valor**:
  - `1` - Para habilitar V2
  - `0` - Para habilitar V1

Configurar logon automático no VDA

Essa configuração permite habilitar ou desabilitar a configuração de política da Microsoft **Sempre solicitar senha** nos VDAs do Windows 10 de SO de sessão única e SO de múltiplas sessões.

Se **Sempre solicitar senha** estiver habilitado, os usuários devem inserir as credenciais no VDA ao iniciar uma sessão remota. Se essa configuração estiver desabilitada, os usuários se conectam automaticamente à sessão remota sem fornecer credenciais no VDA.

Por padrão, a configuração de política da Microsoft está desabilitada. Para habilitar ou desabilitar a configuração **Sempre solicitar senha**, defina o seguinte valor de registro no VDA:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **Nome do valor**: `AutoLogon`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desativa a configuração de política da Microsoft e permite que os usuários façam login automaticamente em uma sessão remota.
  - `0` – Ativa a configuração de política da Microsoft e solicita que os usuários forneçam credenciais ao iniciar uma sessão remota.

Desativar aviso de tempo limite

Por padrão, usuários com sessões inativas ou ociosas recebem uma mensagem de aviso dois minutos antes que sua sessão seja desconectada automaticamente.

Essa configuração desativa e remove a mensagem de aviso para usuários que atingem o limite de tempo limite de sessão ociosa nos seguintes:

- Windows Server 2004
- Windows 10 multissessão 2004 ou SO multissessão posterior

Para remover o aviso, defina o seguinte valor de registro no VDA:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **Nome do valor**: `fEnableTimeoutWarning`
- **Tipo do valor**: `DWORD`
- **Dados do valor**:
  - `1` - Desativar a mensagem de aviso
  - `0` - Ativar a mensagem de aviso

Para exibir a mensagem de aviso, exclua o valor do registro ou defina-o como `0`.

Descoberta de MTU EDT

A Descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso evita a fragmentação de pacotes EDT que pode resultar em degradação do desempenho ou falha ao estabelecer uma sessão.

Essa configuração está habilitada por padrão. Para desabilitar a Descoberta de MTU EDT, configure o seguinte valor de registro e reinicie o VDA.

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nome do valor**: `MtuDiscovery`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Essa configuração é para toda a máquina e afeta todas as sessões que se conectam de um cliente compatível.

Redirecionamento geral de conteúdo

Adicionar tipos de URL para redirecionamento do host para o cliente

Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL: HTTP, HTTPS, RTSP, RTSPU, PNM e MMS. Você pode adicionar tipos de URL à lista criando as seguintes chaves e valores de registro no cliente Windows.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **Nome do valor**: `ExtraURLProtocols`
- **Tipo de valor**: `REG_SZ`
- **Dados do valor**: Especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade da URL. Por exemplo: `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL apenas para clientes Windows. Clientes que não possuem essa configuração de registro rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para manipular os tipos de URL especificados.

Para obter mais informações, consulte Redirecionamento do host para o cliente.

Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Considere que você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo do usuário. Nesse caso, a parte do volume local especificada pelo usuário é redirecionada.

Para habilitar o redirecionamento de pasta do cliente no servidor, defina o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **Nome do valor**: `CFROnlyModeAvailable`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para obter mais informações, consulte Redirecionamento de pasta do cliente.

Redirecionamento do host para o cliente para um conjunto específico de sites

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, defina o seguinte valor de registro no VDA do servidor.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nome do valor**: `ValidSites`
- **Tipo de valor**: `REG_MULTI_SZ`
- **Dados do valor**: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este caractere curinga corresponde a um único nível de domínio, o que é consistente com as regras no RFC 6125. Por exemplo:

`www.example.com`

`*.example.com`

Para obter mais informações, consulte Redirecionamento do host para o cliente.

Comportamento do aplicativo local ao fazer logoff e desconectar

Por padrão, os aplicativos locais continuam a ser executados quando um usuário faz logoff ou se desconecta da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual. Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, defina o seguinte valor de registro na área de trabalho hospedada:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **Nome do valor**: `Session State`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Os aplicativos locais continuam a ser executados quando um usuário faz logoff ou se desconecta da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.
  - `3` - Os aplicativos locais são fechados quando um usuário faz logoff ou se desconecta da área de trabalho virtual.

Para obter mais informações, consulte Acesso a aplicativos locais e redirecionamento de URL.

Remover tipos de URL da lista padrão para redirecionamento do host para o cliente

Para remover tipos de URL da lista de redirecionamento padrão, crie as seguintes chaves e valores de registro no VDA do servidor.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nome do valor**: `DisableServerFTA`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`
- **Nome do valor**: `NoRedirectClasses`
- **Tipo de valor**: `REG_MULTI_SZ`
- **Dados do valor**: Especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

`http`

`https`

`rtsp`

Para obter mais informações, consulte Redirecionamento do host para o cliente.

Configuração do navegador padrão do VDA do servidor

Você pode habilitar o redirecionamento do host para o cliente para substituir qualquer configuração de navegador padrão no VDA do Servidor. Se uma URL da web não for redirecionada, o iniciador Citrix passará 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.

- Internet Explorer (Padrão)
  - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nome do valor**: `Default`

  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

- Google Chrome
  - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- Microsoft Edge
  - **Chave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **Chave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nome do valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Dados do valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

O Acesso a Aplicativos Locais para aplicativos publicados

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Para fornecer acesso a aplicativos publicados, defina o seguinte valor de registro no servidor:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`

- **Nome do valor**: `ClientHostedAppsEnabled`
- **Tipo de valor**: `DWORD`
- **Dados do valor**:
  - `1` - Habilitar
  - `0` - Desabilitar

Para obter mais informações, consulte Acesso a Aplicativos Locais e redirecionamento de URL.

Gráficos

Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos POC de aceleração CUDA, habilite a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\GraphicsHelper`
- **Nome do valor**: `CUDA`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `00000001`

Para usar os recursos POC de aceleração OpenCL, habilite a seguinte configuração de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\GraphicsHelper`
- **Nome do valor**: `OpenCL`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `00000001`

Para obter mais informações, consulte Aceleração de GPU para SO multi-sessão do Windows

Modo progressivo

O modo progressivo está desativado por padrão. Você pode alterar o estado do modo progressivo com o seguinte valor de registro:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **Tipo de valor**: `REG_DWORD`
- **Nome do valor**: `ProgressiveDisplay`
- **Dados do valor**:
  - `0` - Sempre desativado (Desativa o modo progressivo. Este valor é o padrão.)
  - `1` - Automático (Alterna com base nas condições da rede.)
  - 2 = Sempre ativado

Para obter mais informações, consulte Modo progressivo.

> **Observação:**
>
> O modo progressivo foi preterido. O Thinwire é uma opção alternativa que otimiza a entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

Renderização do Windows Presentation Foundation (WPF)

O HDX 3D Pro permite que aplicativos com uso intenso de gráficos executados em sessões do Windows Multi-session OS sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor.

Para habilitar a renderização de aplicativos WPF usando a GPU do servidor, crie a seguinte configuração no registro do servidor que executa o Windows multi-session OS:

1. Abra o Editor do Registro no VDA e vá para a seguinte chave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Crie ou edite os seguintes valores de registro:
   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - Flag = 0x00000412
   - WPF = 0x00000001

3. Crie uma subchave com o nome do executável do seu aplicativo WPF. Por exemplo, se seu aplicativo for chamado de "mywpfapp.exe", crie a seguinte chave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Reinicie o servidor para que a configuração entre em vigor.

Para obter mais informações, consulte aceleração de GPU para SO multi-sessão do Windows e o blog sobre Como obter o melhor dos aplicativos WPF no SO multi-sessão do Windows.

Multimídia

Evitar eco durante conferências multimídia

O Citrix Virtual Apps and Desktops oferece uma opção de cancelamento de eco que minimiza qualquer eco. Esse recurso é ativado por padrão. Para desativar o cancelamento de eco, você pode alterar uma das seguintes configurações de registro:

- **Chave**:
  - 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nome do valor**: `EchoCancellation`
- **Tipo de valor**: `String/REG_SZ`
- **Dados do valor**: `False`

Para obter mais informações, consulte Recursos de áudio.

Limitação de áudio

Depois de instalar um dispositivo de áudio no seu cliente, habilitar o redirecionamento de áudio e iniciar uma sessão RDS, os arquivos de áudio podem não reproduzir som. Como solução alternativa, adicione a seguinte chave de registro na máquina RDS e reinicie a máquina:

- **Chave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **Nome do valor**: `EnableSvchostMitigationPolicy`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Para obter mais informações, consulte Recursos de áudio.

Redirecionamento de conteúdo do navegador e DPI

Ao usar o redirecionamento de conteúdo do navegador com o DPI (dimensionamento) definido para qualquer valor acima de 100% na máquina do usuário, a tela de conteúdo do navegador redirecionado é exibida incorretamente. Para evitar o problema, desative a aceleração de GPU do redirecionamento de conteúdo do navegador para o Chrome criando o seguinte valor de registro na máquina do usuário:

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`
- **Nome do valor**: `GPU`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Para obter mais informações, consulte Redirecionamento de conteúdo do navegador e DPI.

Resolução de webcam de alta definição

Se a negociação do tipo de mídia falhar, o HDX retorna para a resolução VGA padrão (640 x 480 pixels). Você pode usar chaves de registro no cliente para configurar a resolução padrão. Antes de definir as seguintes chaves de registro, certifique-se de que a câmera suporte a resolução especificada.

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- Largura
  - **Nome do valor**: `DefaultWidth`
  - **Tipo de valor**: `DWORD`
  - **Dados do valor**: largura desejada em decimal (por exemplo: 1280)
- Altura
  - **Nome do valor**: `DefaultHeight`
  - **Tipo de valor**: `DWORD`
  - **Dados do valor**: altura desejada em decimal (por exemplo: 720)

Modo de fallback do Microsoft Teams

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Not Connected" em Teams/Sobre/Versão), o VDA retorna para tecnologias HDX legadas, como redirecionamento de

webcam e redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão do aplicativo Workspace/SO da plataforma que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam.

Para controlar o mecanismo de fallback, defina um dos seguintes valores de registro no VDA:

- **Chave** (apenas uma é necessária):
  - **Configuração do computador:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **Configuração do usuário:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **Nome do valor**: `DisableFallback`
- **Tipo de valor**: `DWORD`
- Dados do valor:
  - `1` - Desabilitar modo de fallback
  - `2` - Habilitar somente áudio

Se o valor não estiver presente ou estiver definido como 0, o modo de fallback será habilitado. Este recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior. Para obter mais informações, consulte Otimização para Microsoft Teams.

Otimização para Microsoft Teams com Citrix App Layering™

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, crie uma chave de registro vazia chamada **PortICA** no Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Mantenha o nome, tipo e dados do valor padrão.

- Chave para a versão de 32 bits do Editor do Registro:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- Chave para a versão de 64 bits do Editor do Registro:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

Para obter mais informações, consulte Otimização para Microsoft Teams.

Logon único com Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

Essa configuração fornece logon único a um servidor web configurado com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA. Para habilitar o logon único, defina o seguinte valor de registro como 1:

- **Chave**:
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

  ou

  - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream`
- **Nome do valor**: `WebBrowserRedirectionIwaSupport`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para obter mais informações, consulte Logon único com Autenticação Integrada do Windows.

Cabeçalho de solicitação do user-agent

O cabeçalho user-agent ajuda a identificar solicitações HTTP enviadas do redirecionamento de conteúdo do navegador. Essa configuração pode ser útil ao configurar as 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 user-agent para ignorar certos requisitos. Somente dispositivos Windows suportam o cabeçalho de solicitação do user-agent.

Por padrão, a string do cabeçalho de solicitação do user-agent está desabilitada. Para habilitar o cabeçalho user-agent para conteúdo renderizado pelo cliente, use o editor do Registro.

Em cada aplicativo Citrix Workspace para clientes Windows, defina uma das seguintes configurações de registro:

- **Chave**:
  - 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream`
  - 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`
- **Nome do valor**: `EnableCefUserAgentString`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Depois de adicionar o valor do registro, o cabeçalho user-agent contém o texto CitrixBCR/2102.1, onde 2102.1 é a versão do aplicativo Citrix Workspace para Windows.

Compressão de software da webcam

Se uma webcam suportar codificação de hardware, a compressão de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compressão de software, adicione os seguintes valores ao cliente:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **Nome do valor**: `DeepCompress_ForceSWEncode`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `1`

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

Compressão de vídeo da webcam

A compressão de vídeo da webcam HDX envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compressão da webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Este recurso é habilitado por padrão.

Para desabilitar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina o seguinte valor de registro no VDA.

- **Chave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **Nome do valor**: `OfferH264ToApp`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `0`

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

Taxa de quadros da compressão de vídeo da webcam

Para ajustar a taxa de quadros de vídeo preferida, edite o seguinte valor de registro no cliente:

- **Chave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **Nome do valor**: `FramesPerSecond`
- **Tipo de valor**: `DWORD`
- **Dados do valor**: `15`

Se a webcam não suportar a taxa de quadros especificada, o aplicativo usa 15 FPS por padrão.

Para obter mais informações, consulte compressão de vídeo da webcam HDX.

Configurações de política de gerenciamento de carga

A seção **Gerenciamento de Carga** inclui configurações de política para habilitar e configurar o gerenciamento de carga entre servidores que fornecem máquinas com SO de múltiplas sessões do Windows.

Para obter informações sobre como calcular o índice do avaliador de carga, consulte CTX202150.

Tolerância de logon simultâneo

Essa configuração especifica o número máximo de logons simultâneos que um servidor pode aceitar.

Por padrão, esse valor é definido como 2.

Quando essa configuração está habilitada, o balanceamento de carga tenta evitar ter mais do que o número especificado de logons ativos em um VDA de servidor ao mesmo tempo. No entanto, o limite não é estritamente imposto. Para impor o limite (e fazer com que os logons simultâneos que excedem o número especificado falhem), crie a seguinte chave de registro:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit Type: DWORD Value: 1

Uso da CPU

Essa configuração especifica o nível de uso da CPU, como uma porcentagem, no qual o servidor relata uma carga total. Quando habilitada, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, essa configuração está desabilitada e o uso da CPU é excluído dos cálculos de carga.

Prioridade de processo excluída do uso da CPU

> **Observação:**
>
> Em cenários em que o Workspace Environment Management gerencia máquinas, usar essa configuração junto com as configurações de Prioridade da CPU pode ter resultados indesejados. Recomendamos que você desabilite essa configuração se optar por usar as configurações de Prioridade da CPU.

> Essa configuração especifica o nível de prioridade no qual o uso da CPU de um processo é excluído do índice de carga de Uso da CPU.

Por padrão, esse valor é definido como **Abaixo do Normal** ou **Baixo**.

Uso de disco

Essa configuração especifica o comprimento da fila de disco no qual o servidor relata uma carga de 75%. Quando habilitada, o valor padrão para o comprimento da fila de disco é 8.

Por padrão, essa configuração está desabilitada e o uso do disco é excluído dos cálculos de carga.

Número máximo de sessões

Essa configuração especifica o número máximo de sessões que um servidor pode hospedar. Quando ativada, a configuração padrão para o número máximo de sessões que um servidor pode hospedar é 250.

Por padrão, essa configuração está ativada.

Uso de memória

Essa configuração especifica o nível de uso da memória, como uma porcentagem, no qual o servidor relata uma carga total. Quando ativada, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, essa configuração está desativada e o uso da memória é excluído dos cálculos de carga.

Carga base de uso da memória

Essa configuração especifica uma aproximação do uso de memória do sistema operacional base. Além disso, define, em MB, o uso de memória abaixo do qual um servidor é considerado com carga zero.

Por padrão, esse valor é definido como 768 MB.

Configurações de política de gerenciamento de perfil

Esta seção contém configurações de política para habilitar e configurar o Gerenciamento de Perfil.

Para outras informações, como as seguintes, consulte Políticas de Gerenciamento de Perfil:

- Nomes da configuração equivalente do arquivo .ini

- Qual versão do Gerenciamento de Perfil é necessária para uma configuração de política

Configurações avançadas de política

Número de tentativas ao acessar arquivos bloqueados

Define o número de tentativas ao acessar arquivos bloqueados.

Se esta política estiver desabilitada, o valor padrão de cinco tentativas será usado. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o valor padrão será usado.

Processar arquivos de cookie da Internet no logoff

Algumas implantações deixam cookies de Internet extras que `Index.dat` não referencia. Os cookies extras deixados no sistema de arquivos após navegação prolongada podem levar ao inchaço do perfil. Esta política permite que você habilite o Profile Management para forçar o processamento de Index.dat e remover os cookies extras. A política aumenta os tempos de logoff, então habilite-a somente depois de experimentar esse problema.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada nem aqui nem no arquivo .ini, nenhum processamento de Index.dat ocorrerá.

Desabilitar configuração automática

O Profile Management examina qualquer ambiente Citrix Virtual Desktops™, por exemplo, para a presença de vDisks pessoais, e configura a Política de Grupo de acordo. Apenas as políticas do Profile Management no estado Não Configurado são ajustadas, de modo que quaisquer personalizações que você tenha feito são preservadas.

Esta política permite acelerar a implantação e simplifica a otimização. Você não precisa configurar esta política. No entanto, você pode desabilitar a configuração automática ao fazer uma das seguintes ações:

- Atualizar para reter configurações de versões anteriores
- Solução de problemas

Você pode considerar a configuração automática como um verificador de configuração dinâmico que configura automaticamente as configurações de política padrão de acordo com os ambientes em tempo de execução. Isso elimina a necessidade de configurar as configurações manualmente. Os ambientes de tempo de execução incluem:

- Windows SO

- Versões do sistema operacional Windows
- Presença de Citrix Virtual Desktops
- Presença de vDisks pessoais

A configuração automática pode alterar as seguintes políticas se o ambiente mudar:

- Gravação de retorno ativa
- Sempre armazenar em cache
- Excluir perfis armazenados em cache localmente no logoff
- Atraso antes de excluir perfis armazenados em cache
- Streaming de perfil

Consulte a tabela a seguir para o status padrão das políticas em diferentes sistemas operacionais:

	SO MULTISSESSÃO	SO DE SESSÃO ÚNICA
Gravação de retorno ativa	Ativado	*Desativado* se o Personal vDisk estiver em uso; caso contrário, ativado.
Sempre armazenar em cache	Desabilitado	*Desativado* se o Personal vDisk estiver em uso; caso contrário, ativado.
Excluir perfis armazenados em cache localmente no logoff	Ativado	*Desativado* se uma das seguintes situações ocorrer: Personal vDisk estiver em uso, Citrix Virtual Desktops for atribuído ou Citrix Virtual Desktops não estiver instalado; caso contrário, ativado.
Atraso antes de excluir perfis armazenados em cache	0 segundos	60 segundos se as alterações do usuário não forem persistentes; caso contrário, 0 segundos.
Streaming de perfil	Ativado	*Desabilitado* se o Personal vDisk estiver em uso; caso contrário, habilitado.

No entanto, com a configuração automática desabilitada, todas as políticas acima são padronizadas para **Desabilitado**.

> **Importante:**
>
> O Personal vDisk foi descontinuado. Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.
>
> A partir do Profile Management 1909, você pode ter uma experiência aprimorada com o menu Iniciar no Windows 10 (versão 1607 e posterior). Essa melhoria é alcançada por meio da configuração automática das seguintes políticas:

- Adicione `Appdata\Local\Microsoft\Windows\Caches` e `Appdata\Local\Packages` a **Pastas para Espelhar**.
- Adicione `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` a **Arquivos para sincronizar**.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui nem no arquivo .ini, a configuração automática será ativada. Nesse caso, as configurações do Profile Management podem mudar se o ambiente mudar.

Fazer logoff do usuário se um problema for encontrado

Permite especificar se o Profile Management faz logoff dos usuários se um problema for encontrado.

Se esta política estiver desabilitada ou não configurada, o Profile Management atribui um perfil temporário aos usuários se um problema for encontrado. Por exemplo, o armazenamento do usuário está indisponível.

Se estiver habilitado, uma mensagem de erro será exibida e os usuários serão desconectados. Essa configuração pode simplificar a solução de problemas.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui nem no arquivo .ini, um perfil temporário será fornecido.

Programa de Melhoria da Experiência do Cliente

Por padrão, o Programa de Melhoria da Experiência do Cliente é ativado para ajudar a melhorar a qualidade e o desempenho dos produtos Citrix® coletando estatísticas anônimas e dados de uso.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Habilitar roaming do índice de pesquisa para o Outlook

Permite uma experiência de pesquisa do Outlook baseada no usuário, fazendo o roaming automático dos dados de pesquisa do Outlook junto com o perfil do usuário. Este recurso requer espaço extra no armazenamento do usuário para armazenar os índices de pesquisa do Outlook.

Faça logoff e, em seguida, faça logon novamente para que esta política entre em vigor.

Banco de dados do índice de pesquisa do Outlook – backup e restauração

Permite especificar o que o Profile Management faz durante o logon quando a política Habilitar roaming do índice de pesquisa para o Outlook está ativada.

Se esta política estiver ativada, o Profile Management faz backup do banco de dados do índice de pesquisa cada vez que o banco de dados é montado com sucesso no logon. O Profile Management trata o backup como a cópia boa do banco de dados do índice de pesquisa. Quando uma tentativa de montar o banco de dados do índice de pesquisa falha devido à corrupção do banco de dados, o Profile Management reverte o banco de dados do índice de pesquisa para a última cópia boa conhecida.

> Nota:
>
> O Profile Management exclui o backup salvo anteriormente depois que um novo backup é salvo com sucesso. O backup consome o armazenamento VHDX disponível.

HABILITAR SUPORTE A SESSÕES SIMULTÂNEAS PARA ROAMING DE DADOS DE PESQUISA DO OUTLOOK

Permite que o Profile Management forneça uma experiência de pesquisa nativa do Outlook em sessões simultâneas do mesmo usuário. Use esta política com a política Roaming do índice de pesquisa para o Outlook.

Com esta política ativada, cada sessão simultânea usa um arquivo OST do Outlook separado.

Por padrão, apenas dois discos VHDX podem ser usados para armazenar arquivos OST do Outlook (um arquivo por disco). Se o usuário iniciar mais sessões, seus arquivos OST do Outlook

serão armazenados no perfil de usuário local. Você pode especificar o número máximo de discos VHDX para armazenar arquivos OST do Outlook.

HABILITAR CONTÊINER DO ONEDRIVE

Permite que as pastas do OneDrive sejam itinerantes com os usuários.

O contêiner do OneDrive é uma solução de roaming de pastas baseada em VHDX. O Profile Management cria um arquivo VHDX por usuário em um compartilhamento de arquivos e armazena as pastas do OneDrive dos usuários nos arquivos VHDX. Os arquivos VHDX são anexados quando os usuários fazem logon e desanexados quando os usuários fazem logoff.

Roaming de aplicativos UWP

Permite habilitar que aplicativos UWP (Universal Windows Platform) sejam itinerantes com os usuários. Como resultado, os usuários podem acessar os mesmos aplicativos UWP de diferentes dispositivos.

Com esta política ativada, o Profile Management permite que os aplicativos UWP sejam itinerantes com os usuários, armazenando os aplicativos em discos VHDX separados. Esses discos são anexados durante os logons dos usuários e desanexados durante os logoffs dos usuários.

Precedência de configuração:

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não for configurada nem aqui nem no arquivo .ini, este recurso será desativado.

HABILITAR PROCESSAMENTO ASSÍNCRONO PARA POLÍTICA DE GRUPO DE USUÁRIO NO LOGON

O Windows oferece dois modos de processamento para a Política de Grupo de usuário: síncrono e assíncrono. O Windows usa um valor de registro para determinar o modo de processamento para o próximo logon do usuário. Se o valor de registro não existir, o modo síncrono será aplicado. O valor de registro é uma configuração de nível de máquina e não é itinerante com os usuários. Assim, o modo assíncrono não será aplicado conforme o esperado se os usuários:

- Fizerem logon em máquinas diferentes.
- Fizerem logon na mesma máquina onde a política Excluir perfis armazenados em cache localmente no logoff está ativada.

Com esta política ativada, o valor de registro é itinerante com os usuários. Como resultado, o modo de processamento é aplicado cada vez que os usuários fazem logon.

PROPORÇÃO DE ESPAÇO LIVRE PARA ACIONAR A COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar a proporção de espaço livre para acionar a compactação de disco VHD. Quando a proporção de espaço livre excede o valor especificado no logoff do usuário, a compactação de disco é acionada.

Proporção de espaço livre = (tamanho atual do arquivo VHD – tamanho mínimo necessário do arquivo VHD*) ÷ tamanho atual do arquivo VHD

* Obtido usando o método GetSupportedSize da classe `MSFT_Partition` do sistema operacional Microsoft Windows.

NÚMERO DE LOGOFFS PARA ACIONAR A COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar o número de logoffs de usuário para acionar a compactação de disco VHD.

Quando o número de logoffs desde a última compactação atinge o valor especificado, a compactação de disco é acionada novamente.

DESABILITAR DESFRAGMENTAÇÃO PARA COMPACTAÇÃO DE DISCO VHD

Aplicável quando Habilitar compactação de disco VHD está habilitado. Permite especificar se a desfragmentação de arquivo deve ser desabilitada para a compactação de disco VHD.

Quando a compactação de disco VHD está habilitada, o arquivo de disco VHD é primeiro desfragmentado automaticamente usando a ferramenta `defrag` integrada do Windows e, em seguida, compactado. A desfragmentação de disco VHD produz melhores resultados de compactação, enquanto desabilitá-la pode economizar recursos do sistema.

Habilitar gravação de retorno de várias sessões para contêineres de perfil

Habilita a gravação de retorno para contêineres de perfil em cenários de várias sessões. Se habilitado, as alterações em todas as sessões são gravadas de volta nos contêineres de perfil. Caso contrário, apenas as alterações na primeira sessão são salvas porque apenas a primeira sessão está no modo de leitura/gravação nos contêineres de perfil. Os contêineres de perfil do Citrix Profile Management são suportados a partir do Citrix Profile Management 2103. O FSLogix Profile Container é suportado a partir do Citrix Profile Management 2003.

Para usar esta política para o FSLogix Profile Container, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O recurso FSLogix Profile Container está instalado e habilitado.
- O tipo de perfil está definido como **Tentar perfil de leitura-gravação e fallback para somente leitura** no FSLogix.

Replicar armazenamentos de usuário

Permite replicar o armazenamento de perfil de usuário remoto para vários caminhos em cada logon e logoff. Isso permite que o Profile Management forneça redundância de perfil para logons de usuário.

A habilitação da política aumenta o I/O do sistema e pode prolongar os logoffs.

> **Observação:**
>
> Este recurso está disponível para soluções de perfil baseadas em arquivo e baseadas em contêiner.

Habilitar acesso baseado em credenciais a armazenamentos de usuário

Por padrão, o Citrix Profile Management personifica o usuário atual para acessar o armazenamento de usuário. Habilite este recurso se você não quiser que o Profile Management personifique o usuário atual ao acessar o armazenamento de usuário. Você pode colocar armazenamentos de usuário em repositórios de armazenamento (por exemplo, Azure Files) aos quais o usuário atual não tem permissão para acessar.

Para garantir que o Profile Management possa acessar os armazenamentos de usuário, salve as credenciais do servidor de armazenamento de perfil no Workspace Environment Management™ (WEM) ou no Windows Credential Manager. Recomendamos que você use o Workspace Environment Management para eliminar a necessidade de configurar as mesmas credenciais para cada máquina onde o Profile Management é executado. Se você usar o Windows Credential Manager, use a conta do Sistema Local para salvar as credenciais com segurança.

> **Observação:**
>
> Esta política está disponível para armazenamentos de usuário baseados em arquivo e baseados em VHDX. Para versões do Profile Management anteriores à 2212, esta política está disponível apenas para armazenamentos de usuário baseados em VHDX.

> Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não for configurada nem aqui nem no arquivo .ini, ela será desabilitada por padrão.

Personalizar caminho de armazenamento para arquivos VHDX

O Profile Management oferece as seguintes políticas baseadas em VHDX: Contêiner de perfil, Roaming de índice de pesquisa para Outlook e Espelhamento de pasta acelerado. Por padrão, os arquivos VHDX são armazenados no armazenamento de usuário. Esta política permite especificar um caminho separado para armazená-los.

Capacidade padrão de contêineres VHD

Permite especificar a capacidade de armazenamento padrão (em GB) dos contêineres VHD.

Precedência de configuração:

1. Se esta política não for configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, o padrão é 50 (GB).

Reanexar automaticamente discos VHDX em sessões

Com esta política ativada, o Profile Management garante um alto nível de estabilidade das políticas baseadas em VHDX. Por padrão, esta política está ativada.

Quando esta política está ativada, o Profile Management monitora os discos VHDX que estão em uso por políticas baseadas em VHDX. Se algum dos discos for desanexado, o Profile Management o reanexa automaticamente.

Limite de autoexpansão do contêiner de perfil

Permite especificar a porcentagem de utilização da capacidade de armazenamento na qual os contêineres de perfil acionam a autoexpansão.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui ou no arquivo .ini, o padrão é 90 (%) da capacidade de armazenamento.

Incremento de autoexpansão do contêiner de perfil

Permite especificar a quantidade de capacidade de armazenamento (em GB) pela qual os contêineres de perfil se expandem automaticamente quando a autoexpansão é acionada.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui ou no arquivo .ini, o padrão é 10 (GB).

Limite de autoexpansão do contêiner de perfil

Permite especificar a capacidade máxima de armazenamento (em GB) para a qual os contêineres de perfil podem se expandir automaticamente quando a expansão automática é acionada.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada nem aqui nem no arquivo .ini, o padrão é 80 (GB).

Habilitar configurações de política no nível do usuário

Com esta política habilitada, as configurações de política no nível da máquina podem funcionar no nível do usuário, e as configurações no nível do usuário substituem as configurações no nível da máquina.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada nem aqui nem no arquivo .ini, ela será desabilitada.

Definir ordem de prioridade para grupos de usuários

Permite especificar a ordem de prioridade para grupos de usuários. A ordem determina qual grupo tem precedência quando um usuário pertence a vários grupos com diferentes configurações de política.

Quando um usuário pertence a vários grupos com configurações de política conflitantes, considere o seguinte:

- Se o usuário pertencer a um ou mais grupos definidos nesta política, o grupo com a maior prioridade terá precedência.
- Se o usuário não pertencer a nenhum dos grupos definidos nesta política, o grupo com o SID listado primeiro em ordem alfabética terá precedência.

Método de seleção de armazenamento de usuário

Permite especificar o método de seleção do armazenamento de usuário quando vários armazenamentos de usuário estão disponíveis. As opções incluem:

- **Ordem de configuração.** O Profile Management seleciona o armazenamento configurado mais cedo.
- **Desempenho de acesso.** O Profile Management seleciona o armazenamento com o melhor desempenho de acesso.

Precedência de configuração:

1. Se essa configuração não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se essa configuração não estiver configurada aqui ou no arquivo .ini, a **Ordem de configuração** será usada.

HABILITAR FAILOVER DE CONTÊINER DE PERFIL NA SESSÃO ENTRE ARMAZENAMENTOS DE USUÁRIO

Por padrão, quando vários armazenamentos de usuário são implantados, o failover do contêiner de perfil ocorre apenas no logon do usuário. Como resultado, a redundância de perfil está disponível apenas no logon do usuário. Esta política permite expandir o escopo do failover para toda a sessão, garantindo a redundância do perfil durante toda a sessão. Com a política habilitada, se o Profile Management perder a conexão com o contêiner de perfil ativo durante uma sessão, ele alternará automaticamente para outro disponível.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, a configuração será desabilitada.

Configurações básicas de política

Esta seção contém configurações de política relacionadas à configuração básica do Profile Management.

Habilitar Profile Management

Por padrão, para facilitar a implantação, o Profile Management não processa logons ou logoffs. Habilite o Profile Management somente após realizar todas as outras tarefas de configuração e testar o desempenho dos perfis de usuário Citrix® em seu ambiente.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o Profile Management não processará perfis de usuário do Windows de forma alguma.

Grupos processados

Podem ser usados grupos locais do computador e grupos de domínio (locais, globais e universais). Os grupos de domínio devem ser especificados no formato: NOME DO DOMÍNIO\NOME DO GRUPO.

Se esta política estiver configurada aqui, o Profile Management processará apenas os membros desses grupos de usuários. Se esta política estiver desabilitada, o Profile Management processará todos os usuários. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, os membros de todos os grupos de usuários serão processados.

Grupos excluídos

Você pode usar grupos locais do computador e grupos de domínio (locais, globais e universais) para evitar que perfis de usuário específicos sejam processados. Especifique os grupos de domínio no formato NOME DO DOMÍNIO\ NOME DO GRUPO.

Se esta configuração estiver configurada aqui, o Profile Management excluirá os membros desses grupos de usuários. Se esta configuração estiver desabilitada, o Profile Management não excluirá nenhum usuário. Se esta configuração não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta configuração não estiver configurada aqui ou no arquivo .ini, nenhum membro de nenhum grupo será excluído.

Processar logons de administradores locais

Especifica se os logons de membros do grupo BUILTIN\Administrators são processados. Considere que esta política está desabilitada ou não configurada em sistemas operacionais multi-sessão, como ambientes Citrix Virtual Apps. Neste caso, o Profile Management assume que os logons de usuários de domínio, mas não de administradores locais, devem ser processados. Em sistemas operacionais de sessão única (como ambientes Citrix Virtual Desktops), os logons de administrador local são processados. Esta política permite que usuários de domínio com direitos de administrador local, tipicamente usuários do Citrix Virtual Desktops com desktops virtuais atribuídos, possam:

- Ignorar qualquer processamento
- Fazer logon
- Solucionar problemas do desktop com o Profile Management

Nota: Os logons de usuários de domínio podem estar sujeitos a restrições impostas pela associação a grupos, geralmente para garantir a conformidade com o licenciamento do produto. Se esta política estiver desabilitada, o Profile Management não processa os logons de administradores locais. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, os administradores não serão processados.

Caminho para o armazenamento de usuário

Define o caminho para o diretório (o armazenamento de usuário) no qual as configurações do usuário (alterações de registro e arquivos sincronizados) são salvas.

O caminho pode ser:

- Um caminho relativo. Deve ser relativo ao diretório inicial (que é tipicamente configurado como o atributo #homeDirectory# para um usuário no Active Directory).
- Um caminho UNC. Geralmente especifica um compartilhamento de servidor ou um namespace DFS.
- Desabilitado ou não configurado. Neste caso, um valor de #homeDirectory#\Windows é assumido.

Os seguintes tipos de variáveis podem ser usados para esta política:

- Variáveis de ambiente do sistema entre sinais de porcentagem (por exemplo, %ProfVer%). As variáveis de ambiente do sistema geralmente exigem configuração adicional.
- Atributos do objeto de usuário do Active Directory entre sinais de cerquilha (por exemplo, #sAMAccountName#).
- Variáveis do Profile Management. Para obter mais informações, consulte o documento do produto sobre variáveis do Profile Management.

Variáveis de ambiente de usuário não podem ser usadas, exceto para `%username%` e `%userdomain%`. Você também pode criar atributos personalizados para definir variáveis organizacionais, como localização ou usuários, de forma completa. Atributos diferenciam maiúsculas de minúsculas.

Exemplos:

- `\\server\share#sAMAccountName#` armazena as configurações do usuário no caminho UNC `\\server\share\JohnSmith` (se #sAMAccountName# resolver para JohnSmith para o usuário atual)
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!` pode expandir para `\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`

Importante: Quaisquer que sejam os atributos ou variáveis que você use, verifique se esta política se expande para a pasta um nível acima da pasta que contém NTUSER.DAT. Por exemplo, se este arquivo estiver contido em `\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`, defina o caminho para o armazenamento de

usuário como `\\server\profiles$\JohnSmith.Finance\Win8x64` (não a subpasta \UPM_Profile).

Para obter mais informações sobre como usar variáveis ao especificar o caminho para o armazenamento de usuário, consulte os seguintes tópicos:

- Compartilhar perfis de usuário Citrix em vários servidores de arquivos
- Administrar perfis dentro e entre UOs
- Alta disponibilidade e recuperação de desastres com o Profile Management

Se o Caminho para o armazenamento de usuário estiver desativado, as configurações do usuário serão salvas no subdiretório do Windows do diretório inicial.

Se esta política estiver desativada, as configurações do usuário serão salvas no subdiretório do Windows do diretório inicial. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o diretório do Windows na unidade inicial será usado.

Migrar armazenamento de usuário

Especifica o caminho para a pasta onde as configurações do usuário (alterações de registro e arquivos sincronizados) foram salvas anteriormente (o caminho do armazenamento de usuário que você usou anteriormente).

Se esta configuração estiver configurada, as configurações do usuário armazenadas no armazenamento de usuário anterior serão migradas para o armazenamento de usuário atual especificado na política "Caminho para o armazenamento de usuário".

O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial.

Em ambos os casos, você pode usar os seguintes tipos de variáveis:

- Variáveis de ambiente do sistema entre sinais de porcentagem
- Atributos do objeto de usuário do Active Directory entre sinais de hash

Exemplos:

- A pasta `Windows\%ProfileVer%` armazena as configurações do usuário em uma subpasta chamada `Windows\W2K3` do armazenamento de usuário (se %ProfileVer% for uma variável de ambiente do sistema que se resolve para W2K3).

- `\\server\share#SAMAccountName#` armazena as configurações do usuário no caminho UNC `\\server\share\<JohnSmith>` (se `#SAMAccountName#` resolver para JohnSmith para o usuário atual).

No caminho, você pode usar variáveis de ambiente do usuário, exceto `%username%` e `%userdomain%`.

Se esta configuração estiver desabilitada, as configurações do usuário serão salvas no armazenamento de usuário atual.

Se esta configuração não for definida aqui, a configuração correspondente do arquivo .ini será usada.

Se esta configuração não for definida aqui ou no arquivo .ini, as configurações do usuário serão salvas no armazenamento de usuário atual.

Gravação ativa

Arquivos e pastas (mas não entradas de registro) que são modificados podem ser sincronizados com o armazenamento de usuário no meio de uma sessão, antes do logoff.

Se esta política não for definida aqui, o valor do arquivo .ini será usado. Se esta política não for definida aqui ou no arquivo .ini, ela será habilitada.

Suporte a perfil offline

Esta política permite que os perfis sejam sincronizados com o armazenamento de usuário na primeira oportunidade possível. Ela é destinada a usuários de laptop ou dispositivos móveis que fazem roaming. Quando ocorre uma desconexão de rede, os perfis permanecem intactos no laptop ou dispositivo mesmo após reiniciar ou hibernar. À medida que os usuários móveis trabalham, seus perfis são atualizados localmente. Além disso, são eventualmente sincronizados com o armazenamento de usuário quando a conexão de rede é restabelecida.

Se esta política não for definida aqui, o valor do arquivo .ini será usado. Se esta política não for definida aqui ou no arquivo .ini, os perfis offline serão desabilitados.

Registro de gravação ativa

Use esta política juntamente com "Gravação ativa". As entradas de registro que são modificadas podem ser sincronizadas com o armazenamento de usuário no meio de uma sessão.

Se você não definir esta configuração aqui, o valor do arquivo .ini será usado.

Se você não definir esta configuração aqui ou no arquivo .ini, o registro de gravação ativa será desabilitado.

GRAVAÇÃO ATIVA NO BLOQUEIO E DESCONEXÃO DA SESSÃO

Com esta política e a política de **Gravação ativa** habilitadas, os arquivos e pastas de perfil são gravados de volta somente quando uma sessão é bloqueada ou desconectada.

Com esta política e as políticas de **Gravação ativa** e **Gravação ativa do registro** habilitadas, as entradas do registro são gravadas de volta somente quando uma sessão é bloqueada ou desconectada.

Suporte a perfis offline

Habilita o recurso de perfis offline. Este recurso é destinado a computadores que são frequentemente removidos das redes. Por exemplo, laptops ou dispositivos móveis, não servidores ou desktops.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, o suporte a perfil offline será desabilitado.

Configurações de política multiplataforma

Esta seção contém configurações de política relacionadas à configuração do recurso de configurações **multiplataforma do Profile Management**.

Habilitar configurações multiplataforma

Por padrão, para facilitar a implantação, as configurações multiplataforma são desabilitadas. Ative o processamento habilitando esta política, mas somente após um planejamento e teste completos desse recurso.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

Grupos de usuários de configurações multiplataforma

Insira um ou mais grupos de usuários do Windows. Por exemplo, você pode usar esta política para processar apenas os perfis de um grupo de usuários de teste. Se esta política estiver configurada, o recurso de configurações multiplataforma do Profile Management processará apenas os membros desses grupos de usuários. Se esta política estiver desabilitada, o recurso processará todos os usuários especificados pela política de grupos processados.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, todos os grupos de usuários serão processados.

Caminho para definições multiplataforma

Identifica o local de rede dos arquivos de definição que você copiou do pacote de download. Este caminho deve ser um caminho UNC. Os usuários devem ter acesso de leitura a este local, e os administradores devem ter acesso de gravação a ele. O local deve ser um compartilhamento de arquivos Server Message Block (SMB) ou Common Internet File System (CIFS).

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma configuração multiplataforma será aplicada.

Caminho para o armazenamento de configurações multiplataforma

Define o caminho para o armazenamento de configurações multiplataforma, a pasta onde as configurações multiplataforma dos usuários são salvas. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial.

Esta área é a área comum do armazenamento de usuário onde os dados de perfil compartilhados por várias plataformas estão localizados. Os usuários devem ter acesso de gravação a esta área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório inicial. Você pode usar as mesmas variáveis que para o **Caminho para o armazenamento de usuário**.

Se esta política estiver desabilitada, o caminho Windows\PM_CP será usado. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, o valor padrão será usado.

Fonte para criar configurações multiplataforma

Especifica uma plataforma como a plataforma base se esta política estiver habilitada na UO dessa plataforma. Esta política migra dados dos perfis da plataforma base para o armazenamento de configurações multiplataforma.

O conjunto de perfis de cada plataforma é armazenado em uma UO separada. Você deve decidir quais dados de perfil da plataforma usar para preencher o armazenamento de configurações multiplataforma. Isso é referido como a plataforma base. Considere que o armazenamento de configurações multiplataforma contém um arquivo de definição sem dados, ou que os dados em cache em um perfil de plataforma única são mais recentes do que os dados da definição no

armazenamento. Neste caso, o Profile Management migra os dados do perfil de plataforma única para o armazenamento, a menos que você desabilite esta política.

Importante:

Se esta política estiver habilitada em várias UOs, ou em vários objetos de usuário ou máquina, a plataforma na qual o primeiro usuário faz logon se torna o perfil base. Por padrão, esta política está Habilitada.

Configurações de política do sistema de arquivos

Configurações da política de exclusões

Esta seção descreve as configurações de política para configurar quais arquivos e diretórios no perfil de um usuário são excluídos do processo de sincronização.

LISTA DE EXCLUSÃO - ARQUIVOS

Lista de arquivos que são ignorados durante a sincronização. Os nomes dos arquivos devem ser caminhos relativos ao perfil do usuário (%USERPROFILE%). Curingas são suportados em nomes de arquivos e em nomes de pastas, mas apenas curingas em nomes de arquivos são aplicados recursivamente.

Exemplos:

- `Desktop\Desktop.ini` ignora o arquivo `Desktop.ini` na pasta `Desktop`
- `%USERPROFILE%*.tmp` ignora todos os arquivos com a extensão `.tmp` em todo o perfil
- `AppData\Roaming\MyApp*.tmp` ignora todos os arquivos com a extensão `.tmp` em uma parte do perfil
- `Downloads*\a.txt` ignora `a.txt` em qualquer subpasta imediata da pasta `Downloads`.

Se esta política estiver desabilitada, nenhum arquivo será excluído. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhum arquivo será excluído.

HABILITAR LISTA DE EXCLUSÃO PADRÃO - DIRETÓRIOS

Lista padrão de diretórios ignorados durante a sincronização. Use esta política para especificar diretórios de exclusão de GPO sem precisar preenchê-los manualmente.

Se você desabilitar esta política, o Profile Management não excluirá nenhum diretório por padrão.

Se você não configurar esta política aqui, o Profile Management usará o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não excluirá nenhum diretório por padrão.

LISTA DE EXCLUSÃO - DIRETÓRIOS

Lista de pastas que são ignoradas durante a sincronização. Os nomes das pastas devem ser especificados como caminhos relativos ao perfil do usuário (%USERPROFILE%). Curingas em nomes de pastas são suportados, mas não são aplicados recursivamente.

Exemplo:

- `Desktop` ignora a pasta `Desktop` no perfil do usuário

Se esta política estiver desabilitada, nenhuma pasta será excluída. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será excluída.

VERIFICAÇÃO DE EXCLUSÃO DE LOGON

Esta configuração define o que o Profile Management faz se um perfil no armazenamento de usuário contiver arquivos ou pastas excluídos. As possíveis configurações de política e as ações correspondentes estão listadas na tabela a seguir:

CONFIGURAÇÃO DA POLÍTICA	AÇÃO
A configuração está desabilitada ou o valor de "Sincronizar arquivos ou pastas excluídos no logon" está definido como padrão	O Profile Management sincroniza arquivos ou pastas excluídos do armazenamento de usuário para o perfil local quando um usuário faz logon.
A configuração está definida como "Ignorar arquivos ou pastas excluídos no logon"	O Profile Management ignora os arquivos ou pastas excluídos no armazenamento de usuário quando um usuário faz logon.
A configuração está definida como "Excluir arquivos ou pastas excluídos no logon"	O Profile Management exclui os arquivos ou pastas excluídos no armazenamento de usuário quando um usuário faz logon.
A configuração não está configurada no Web Studio	O valor do arquivo .ini é usado

CONFIGURAÇÃO DA POLÍTICA	AÇÃO
A configuração não está configurada no Web Studio ou no arquivo .ini	Os arquivos ou pastas excluídos são sincronizados do armazenamento do usuário para um perfil local quando um usuário faz logon.

MANIPULAÇÃO DE ARQUIVOS GRANDES - ARQUIVOS A SEREM CRIADOS COMO LINKS SIMBÓLICOS

Para melhorar o desempenho do logon e processar arquivos grandes, o Profile Management cria um link simbólico em vez de copiar os arquivos desta lista.

Você pode usar curingas em políticas que se referem a arquivos; por exemplo, `!ctx_localappdata!\Microsoft\Outlook*.OST`.

Para processar o arquivo de pasta offline (`*.ost`) do Microsoft Outlook, certifique-se de que a pasta **Outlook** não esteja excluída para o Profile Management.

Esses arquivos não podem ser acessados em várias sessões simultaneamente.

Configurações da política de sincronização

A seção **Sincronização** descreve as configurações de política para especificar quais arquivos e pastas no perfil de um usuário são sincronizados entre o sistema onde o perfil está instalado e o armazenamento de usuário.

DIRETÓRIOS A SEREM SINCRONIZADOS

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema no qual está instalado e o armazenamento de usuário. Se você excluir uma pasta da sincronização, esta política permite incluir as subpastas da pasta excluída de volta à sincronização.

Os caminhos nesta lista devem ser relativos ao perfil do usuário. Curingas em nomes de pastas são suportados, mas não são aplicados recursivamente.

Se esta política não for configurada aqui, o valor do arquivo .ini será usado. Se esta política não for configurada aqui ou no arquivo .ini, somente as pastas não excluídas no perfil do usuário serão sincronizadas.

ARQUIVOS A SEREM SINCRONIZADOS

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema no qual está instalado e o armazenamento de usuário. Se você excluir uma pasta da sincronização, esta política permite incluir os arquivos dentro da pasta excluída de volta à sincronização.

Os caminhos nesta lista devem ser relativos ao perfil do usuário. Curingas são suportados em nomes de arquivos e em nomes de pastas, mas apenas curingas em nomes de arquivos são aplicados recursivamente. Curingas não podem ser aninhados.

Exemplos:

- `AppData\Local\Microsoft\Office\Access.qat` especifica um arquivo abaixo de uma pasta que é excluída na configuração padrão
- `AppData\Local\MyApp*.cfg` especifica todos os arquivos com a extensão `.cfg` na pasta de perfil `AppData\Local\MyApp` e suas subpastas

Desabilitar esta política tem o mesmo efeito que habilitá-la e configurar uma lista vazia.

Se esta política não for configurada aqui, o valor do arquivo .ini será usado. Se esta política não for configurada aqui ou no arquivo .ini, somente os arquivos não excluídos no perfil do usuário serão sincronizados.

PASTAS A SEREM ESPELHADAS

Esta política permite resolver problemas envolvendo qualquer pasta transacional (também conhecida como pasta referencial). Essa pasta contém arquivos interdependentes, onde um arquivo faz referência ao outro.

Espelhar pastas permite que o Profile Management processe uma pasta transacional e seu conteúdo como uma única entidade, evitando o inchaço do perfil. Por exemplo, você pode espelhar a pasta **cookies do Internet Explorer** para que o Index.dat seja sincronizado com os cookies que ele indexa. Nessas situações, a "última gravação vence". Assim, os arquivos em pastas espelhadas que foram modificados em mais de uma sessão são sobrescritos pela última atualização, resultando na perda de alterações do perfil.

Por exemplo, a tabela a seguir descreve como o Index.dat referencia cookies enquanto um usuário navega na Internet:

CENÁRIO	COMO O INDEX.DAT REFERENCIA COOKIES	
Um usuário tem duas sessões do Internet Explorer, cada uma em um servidor diferente, e visita sites diferentes em cada sessão.	Os cookies de cada site são adicionados ao servidor apropriado.	Os cookies de cada site são adicionados ao servidor apropriado.

CENÁRIO	COMO O INDEX.DAT REFERENCIA COOKIES	
O usuário faz logoff da primeira sessão ou no meio de uma sessão (se o recurso de gravação ativa estiver configurado)	Os cookies da segunda sessão devem substituir os cookies da primeira sessão.	
A primeira e a segunda sessões são mescladas e as referências aos cookies no Index.dat ficam desatualizadas	Navegações futuras em novas sessões resultam em mesclagens repetidas e uma pasta de cookies inchada	

Espelhar a pasta de cookies resolve o problema. Nesse caso, os cookies são sobrescritos pelos cookies da última sessão cada vez que o usuário faz logoff. Assim, o Index.dat permanece atualizado.

Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será espelhada.

ACELERAR O ESPELHAMENTO DE PASTAS

Com esta política e a política **Pastas a espelhar** habilitadas, o **Profile Management armazena pastas espelhadas** em um disco virtual baseado em VHDX. Ele anexa o disco virtual durante os logons e o desanexa durante os logoffs. Habilitar esta política elimina a necessidade de copiar as pastas entre o armazenamento do usuário e os perfis locais e acelera o espelhamento de pastas.

Configurações de política de redirecionamento de pasta

Esta seção contém configurações de política que especificam se as pastas que aparecem com frequência em perfis devem ser redirecionadas para um local de rede compartilhado.

Conceder acesso de administrador

Essa configuração permite que um administrador acesse o conteúdo das pastas redirecionadas de um usuário.

> **Observação:**

> Essa configuração concede permissões a administradores que têm acesso completo e irrestrito ao domínio.

> Por padrão, essa configuração está desabilitada e os usuários recebem acesso exclusivo ao conteúdo de suas pastas redirecionadas.

Incluir nome de domínio

Essa configuração permite a inclusão da variável de ambiente `%userdomain%` como parte do caminho UNC. Esse caminho UNC é especificado para pastas redirecionadas.

Por padrão, essa configuração está desabilitada. E a variável de ambiente `%userdomain%` não é incluída como parte do caminho UNC que é especificado para pastas redirecionadas.

Configurações de política do AppData(Roaming)

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **AppData(Roaming)** para um local de rede compartilhado.

CAMINHO DO APPDATA(ROAMING)

Esta configuração especifica o local de rede para o qual o conteúdo da pasta **AppData(Roaming)** é redirecionado.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

CONFIGURAÇÕES DE REDIRECIONAMENTO PARA APPDATA(ROAMING)

Esta configuração especifica como redirecionar o conteúdo da pasta **AppData(Roaming)**.

Por padrão, o conteúdo é redirecionado para um caminho UNC. Para obter mais informações, consulte a seção Caminho para o armazenamento do usuário.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de Documentos

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Documentos** para um local de rede compartilhado.

CAMINHO DOS DOCUMENTOS

Esta configuração especifica o local de rede para o qual os arquivos na pasta **Documentos** são redirecionados.

Por padrão, esta configuração está desabilitada e nenhum local é especificado.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

A configuração **Caminho dos documentos** deve ser habilitada não apenas para redirecionar arquivos para a pasta **Documentos**, mas também para redirecionar arquivos para as pastas **Música**, **Imagens** e **Vídeos**.

CONFIGURAÇÕES DE REDIRECIONAMENTO PARA DOCUMENTOS

Esta configuração especifica como redirecionar o conteúdo da pasta **Documentos**.

Por padrão, o conteúdo é redirecionado para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Documentos**, escolha uma das seguintes opções:

- Redirecionar para o seguinte caminho UNC. Redireciona o conteúdo para o caminho UNC especificado na configuração de política Caminho dos documentos.
- Redirecionar para o diretório inicial do usuário. Redireciona o conteúdo para o diretório inicial do usuário, tipicamente configurado como o atributo #homeDirectory# para um usuário no Active Directory.

Se esta configuração não for configurada aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de log

Esta seção contém configurações de política que configuram o registro do Profile Management.

Ações do Active Directory

Esta configuração habilita ou desabilita o registro detalhado das ações realizadas no Active Directory.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida no Web Studio, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Informações comuns

Esta configuração habilita ou desabilita o registro detalhado de informações comuns.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Avisos comuns

Esta configuração habilita ou desabilita o registro detalhado de avisos comuns.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Habilitar registro

Esta configuração habilita ou desabilita o registro do Profile Management no modo de depuração (registro detalhado). No modo de depuração, informações de status extensas são registradas nos arquivos de log localizados em "%SystemRoot%\System32\Logfiles\UserProfileManager".

Por padrão, esta configuração está desabilitada e apenas erros são registrados.

A Citrix® recomenda habilitar esta configuração apenas se você estiver solucionando problemas do Profile Management.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, somente os erros serão registrados.

Ações do sistema de arquivos

Esta configuração habilita ou desabilita o registro detalhado das ações realizadas no sistema de arquivos.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Notificações do sistema de arquivos

Esta configuração habilita ou desabilita o registro detalhado das notificações do sistema de arquivos.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Logoff

Esta configuração habilita ou desabilita o registro detalhado de logoffs de usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não estiver configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não estiver configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Logon

Esta configuração habilita ou desabilita o registro detalhado de logons de usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Tamanho máximo do arquivo de log

Esta configuração especifica o tamanho máximo permitido para o arquivo de log do Profile Management, em bytes.

Por padrão, este valor é definido como 1048576 bytes (1 MB).

A Citrix recomenda aumentar o tamanho deste arquivo para 5 MB ou mais, se você tiver espaço em disco suficiente. Se o arquivo de log exceder o tamanho máximo:

- Um backup existente do arquivo (.bak) é excluído
- O arquivo de log é renomeado para .bak
- Um novo arquivo de log é criado

O arquivo de log é criado em `%SystemRoot%\System32\Logfiles\UserProfileManager`.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, o valor padrão será usado.

Caminho para o arquivo de log

Esta configuração especifica um caminho alternativo para salvar o arquivo de log do Profile Management.

Por padrão, esta configuração está desabilitada e os arquivos de log são salvos no local padrão: %SystemRoot%\System32\Logfiles\UserProfileManager.

O caminho pode apontar para uma unidade local ou uma unidade de rede remota (caminho UNC). Caminhos remotos podem ser úteis em grandes ambientes distribuídos, mas podem criar um tráfego de rede significativo, o que pode ser inadequado para arquivos de log. Para máquinas virtuais provisionadas com um disco rígido persistente, defina um caminho local para essa unidade. Essa configuração garante que os arquivos de log sejam preservados quando a máquina for reiniciada. Para máquinas virtuais sem um disco rígido persistente, definir um caminho UNC permite reter os arquivos de log. No entanto, a conta do sistema para as máquinas deve ter acesso de gravação ao compartilhamento UNC. Use um caminho local para quaisquer laptops gerenciados pelo recurso de perfis offline.

Se um caminho UNC for usado para arquivos de log, a Citrix recomenda que uma lista de controle de acesso apropriada seja aplicada à pasta de arquivos de log. Essa configuração garante que apenas contas de usuário ou computador autorizadas possam acessar os arquivos armazenados.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, o local padrão %SystemRoot%\System32\Logfiles\UserProfileManager será usado.

Informações personalizadas do usuário

Esta configuração habilita ou desabilita o registro detalhado de informações personalizadas do usuário.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Valores da política no logon e logoff

Esta configuração habilita ou desabilita o registro detalhado de valores de política quando um usuário faz logon e logoff.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Ações do Registro

Esta configuração habilita ou desabilita o registro detalhado de ações realizadas no Registro.

Por padrão, esta configuração está desabilitada.

Ao habilitar esta configuração, certifique-se de que a configuração **Habilitar registro** também esteja habilitada.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Diferenças do Registro no logoff

Essa configuração habilita ou desabilita o registro detalhado de quaisquer diferenças no registro quando um usuário faz logoff.

Por padrão, essa configuração está desabilitada.

Ao habilitar essa configuração, certifique-se de que a configuração **Habilitar log** também esteja habilitada.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida no Web Studio ou no arquivo .ini, o seguinte será registrado:

- Erros
- Informações gerais

Configurações de política de tratamento de perfil

Esta seção inclui configurações de política que especificam como o Profile Management lida com perfis de usuário.

Atraso antes de excluir perfis em cache

Esta configuração especifica uma extensão opcional ao atraso, em minutos, antes que o Profile Management exclua perfis armazenados em cache localmente no logoff.

Um valor de 0 exclui os perfis imediatamente ao final do processo de logoff. O Profile Management verifica os logoffs a cada minuto. Como resultado, um valor de 60 garante que os perfis sejam excluídos entre um e dois minutos após os usuários fazerem logoff. Esta ação depende de quando a última verificação ocorreu. Estender o atraso é útil se você souber que um processo mantém arquivos ou o hive do registro do usuário abertos durante o logoff. Com perfis grandes, este processo também pode acelerar o logoff.

Por padrão, este valor é definido como 0 e o Profile Management exclui os perfis armazenados em cache localmente imediatamente.

Ao habilitar esta configuração, certifique-se de que a opção Excluir perfis armazenados em cache localmente no logoff também esteja habilitada.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, os perfis serão excluídos imediatamente.

Excluir perfis armazenados em cache localmente no logoff

Esta configuração especifica se os perfis armazenados em cache localmente são excluídos depois que um usuário faz logoff.

Quando esta configuração está habilitada, o cache de perfil local de um usuário é excluído depois que ele faz logoff. A Citrix® recomenda habilitar esta configuração para servidores de terminal.

Por padrão, esta configuração está desabilitada e o cache de perfil local de um usuário é retido depois que ele faz logoff.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, os perfis em cache não serão excluídos.

Tratamento de conflitos de perfil local

Essa configuração define como o Profile Management se comporta se um perfil de usuário existir em ambos os seguintes locais:

- Repositório de usuário
- Perfil de usuário local do Windows (não é um perfil de usuário Citrix)

Por padrão, o Profile Management usa o perfil local do Windows, mas não o altera de forma alguma.

Para controlar como o Profile Management se comporta, escolha uma das seguintes opções:

- Usar perfil local. O Profile Management usa o perfil local, mas não o altera de forma alguma.
- Excluir perfil local. O Profile Management exclui o perfil de usuário local do Windows e, em seguida, importa o perfil de usuário Citrix do repositório de usuário.
- Renomear perfil local. O Profile Management renomeia o perfil de usuário local do Windows (para fins de backup) e, em seguida, importa o perfil de usuário Citrix do repositório de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, os perfis locais existentes serão usados.

Migração de perfis existentes

Essa configuração especifica os tipos de perfil migrados para o repositório de usuário durante o logon, se um usuário não tiver um perfil atual no repositório de usuário.

O Profile Management pode migrar perfis existentes "em tempo real" durante o logon, se um usuário não tiver um perfil no repositório de usuário. Depois disso, o perfil do repositório de usuário é usado pelo Profile Management em ambos os seguintes casos:

- Sessão atual
- Qualquer outra sessão configurada com o caminho para o mesmo armazenamento de usuário

Por padrão, ambos os perfis locais e de roaming são migrados para o armazenamento de usuário durante o logon.

Para especificar os tipos de perfil migrados para o armazenamento de usuário durante o logon, escolha uma das seguintes opções:

- Perfis locais e de roaming
- Local
- Roaming
- Nenhum (Desabilitado)

Se você selecionar **Nenhum**, o sistema usa o mecanismo existente do Windows para criar perfis, como se estivesse em um ambiente onde o Profile Management não está instalado.

Se esta configuração não for configurada aqui, o valor do arquivo .ini será usado.

Se esta configuração não for configurada aqui ou no arquivo .ini, os perfis locais e de roaming existentes serão migrados.

Migração automática de perfis de aplicativo existentes

Esta configuração habilita ou desabilita a migração automática de perfis de aplicativo existentes entre diferentes sistemas operacionais. Os perfis de aplicativo incluem tanto os dados do aplicativo na pasta `AppData` quanto as entradas de registro em `HKEY_CURRENT_USER\SOFTWARE`. Esta configuração pode ser útil em casos onde você deseja migrar seus perfis de aplicativo entre diferentes sistemas operacionais.

Por exemplo, suponha que você atualize seu sistema operacional (SO) do Windows 10 versão 1803 para o Windows 10 versão 1809. Se esta configuração estiver habilitada, o Profile Management migra automaticamente as configurações de aplicativo existentes para o Windows

10 versão 1809 na primeira vez que cada usuário faz logon. Como resultado, os dados do aplicativo na pasta `AppData` e as entradas de registro em HKEY_CURRENT_USER\SOFTWARE são migrados.

Se houver vários perfis de aplicativo existentes, o Profile Management realiza a migração na seguinte ordem de prioridade:

1. Perfis do mesmo tipo de SO (SO de sessão única para SO de sessão única e SO de múltiplas sessões para SO de múltiplas sessões).
2. Perfis da mesma família de SO Windows; por exemplo, Windows 10 para Windows 10, ou Windows Server 2016 para Windows Server 2016).
3. Perfis de uma versão anterior do SO; por exemplo, Windows 7 para Windows 10, ou Windows Server 2012 para Windows 2016.
4. Perfis do SO mais próximo.

Nota: Você deve especificar o nome curto do SO incluindo a variável "!CTX_OSNAME!" no caminho do armazenamento do usuário. Isso permite que o Profile Management localize os perfis de aplicativo existentes.

Se esta configuração não for definida aqui, a configuração do arquivo .ini será usada.

Se esta configuração não for definida aqui ou no arquivo .ini, ela será desabilitada por padrão.

Caminho para o perfil de modelo

Esta configuração especifica o caminho para o perfil que você deseja que o Profile Management use como modelo para criar perfis de usuário.

O caminho especificado deve ser o caminho completo para a pasta que contém o arquivo de registro NTUSER.DAT e quaisquer outras pastas e arquivos necessários para o perfil de modelo.

Nota: Não inclua NTUSER.DAT no caminho. Por exemplo, com o arquivo `\\myservername\myprofiles\template\ntuser.dat`, defina o local como `\\myservername\myprofiles\template`.

Use caminhos absolutos, que podem ser caminhos UNC ou caminhos na máquina local. Use este último, por exemplo, para especificar um perfil de modelo permanentemente em uma imagem do Citrix Provisioning™ Services. Caminhos relativos não são suportados.

Nota: Esta configuração não suporta a expansão de atributos do Active Directory, variáveis de ambiente do sistema ou as variáveis `%USERNAME%` e `%USERDOMAIN%`.

Por padrão, esta configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se esta configuração não for definida aqui, o valor do arquivo .ini será usado.

Se esta configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo substitui perfil local

Essa configuração permite que o perfil de modelo substitua o perfil local ao criar perfis de usuário.

Considere que um usuário não tem um perfil de usuário Citrix, mas tem um perfil de usuário local do Windows. Nesse caso, por padrão, o perfil local é usado e migrado para o armazenamento de usuário, se esse valor estiver habilitado. Habilitar essa configuração de política permite que o perfil de modelo substitua o perfil local usado ao criar perfis de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo substitui perfil de roaming

Essa configuração permite que o perfil de modelo substitua um perfil de roaming ao criar perfis de usuário.

Considere que um usuário não tem um perfil de usuário Citrix, mas tem um perfil de usuário de roaming do Windows. Nesse caso, por padrão, o perfil de roaming é usado e migrado para o armazenamento de usuário, se esse valor estiver habilitado. Habilitar essa configuração de política permite que o perfil de modelo substitua o perfil de roaming usado ao criar perfis de usuário.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Perfil de modelo usado como um perfil obrigatório Citrix para todos os logons

Essa configuração permite que o Profile Management use o perfil de modelo como o perfil padrão para criar todos os perfis de usuário.

Por padrão, essa configuração está desabilitada e novos perfis de usuário são criados a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se essa configuração não for definida aqui, o valor do arquivo .ini será usado.

Se essa configuração não for definida aqui ou no arquivo .ini, nenhum modelo será usado.

Configurações de política de contêiner de perfil

Contêiner de perfil

Pastas grandes associadas a um perfil de usuário resultam em um logon lento. O Citrix Profile Management fornece uma solução de perfil baseada em VHDX que permite especificar as pastas a serem contidas no disco de perfil (arquivos VHDX). Essa solução reduz os tempos de logon mapeando as pastas especificadas para o disco de perfil que é armazenado na rede. O contêiner de perfil anexa o disco de perfil contendo essas pastas durante o logon, eliminando assim a necessidade de salvar uma cópia das pastas no perfil local. Isso diminui os tempos de logon.

Habilitar cache local para contêineres de perfil

Esta política habilita o suporte a cache local para contêineres de perfil do Citrix Profile Management. Com a política definida como **Habilitado**, cada perfil local serve como um cache local de seu contêiner de perfil do Citrix Profile Management. Se o streaming de perfil estiver em uso, os arquivos armazenados em cache localmente são criados sob demanda. Caso contrário, eles são criados durante os logons do usuário. Para usar o recurso de cache local, coloque um perfil de usuário inteiro em seu contêiner de perfil do Citrix Profile Management.

Pastas a serem excluídas do contêiner de perfil

Lista de pastas a serem excluídas de um contêiner de perfil do Citrix Profile Management.

Pastas a serem incluídas no contêiner de perfil

Lista de pastas a serem mantidas em um contêiner de perfil do Citrix Profile Management quando suas pastas pai são excluídas.

As pastas nesta lista devem ser subpastas das pastas excluídas. Caso contrário, esta configuração não funciona.

Arquivos a serem incluídos no contêiner de perfil

Lista de arquivos a serem incluídos em um contêiner de perfil do Citrix Profile Management.

Os arquivos nesta lista devem estar dentro das pastas excluídas. Caso contrário, esta configuração não funciona.

Arquivos a serem excluídos do contêiner de perfil

Lista de arquivos a serem excluídos de um contêiner de perfil do Citrix Profile Management.

Habilitar compactação de disco VHD

Permite habilitar a compactação de disco VHD para o Gerenciamento de Perfis. Se habilitado, os discos VHD são compactados automaticamente no logoff do usuário quando certas condições são atendidas. Esta política permite economizar o espaço de armazenamento consumido pelo contêiner de perfil, contêiner do OneDrive e contêiner de pasta espelhada.

Dependendo das suas necessidades e dos recursos disponíveis, você pode ajustar as configurações e o comportamento padrão de compactação de VHD usando as políticas **Taxa de espaço livre para acionar a compactação de disco VHD**, **Número de logoffs para acionar a compactação de disco VHD** e **Desabilitar desfragmentação para compactação de disco VHD** em Configurações avançadas.

Habilitar autoexpansão de VHD para contêiner de perfil

Permite especificar se a autoexpansão de VHD deve ser habilitada para o contêiner de perfil. Quando habilitado, todas as configurações de autoexpansão de VHD se aplicam ao contêiner de perfil.

Precedência de configuração:

- Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
- Se esta política não estiver configurada aqui ou no arquivo .ini, ela será desabilitada.

Habilitar acesso exclusivo a contêineres VHD

Por padrão, os contêineres VHD permitem acesso concorrente. Com esta configuração habilitada, eles permitem apenas um acesso por vez. Este recurso se aplica a contêineres de perfil e contêineres do OneDrive.

> **Observação:**
>
> Habilitar esta configuração para contêineres de perfil em uma solução de perfil baseada em contêiner desabilita automaticamente a configuração *Habilitar gravação de várias sessões para contêineres de perfil*.
>
> Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui ou no arquivo .ini, a configuração será desabilitada.

Fazer logoff de usuários quando o contêiner de perfil não estiver disponível durante o logon

Permite forçar o logoff de usuários quando o contêiner de perfil estiver indisponível durante o logon do usuário e (opcionalmente) personalizar a mensagem de erro que os usuários veem.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado.
2. Se esta política não estiver configurada aqui nem no arquivo .ini, a configuração será desabilitada.

Usuários e grupos para acessar o contêiner de perfil

Permite especificar quais usuários e grupos de domínio AD têm permissão `Read & Execute` em contêineres de perfil. Por padrão, um contêiner de perfil é acessível apenas ao seu proprietário.

Precedência de configuração:

1. Se esta política não estiver configurada aqui, a configuração do arquivo .ini será usada.
2. Se esta política não estiver configurada aqui nem no arquivo .ini, o contêiner de perfil será acessível apenas ao seu proprietário.

Configurações de política de registro

Esta seção contém configurações de política que especificam quais chaves de registro são incluídas ou excluídas do processamento do Profile Management.

Lista de exclusão

Lista de chaves de registro no hive HKCU que são ignoradas durante o logoff.

Exemplo: Software\Policies

Se esta política estiver desabilitada, nenhuma chave de registro será excluída. Se esta política não estiver configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma chave de registro será excluída.

Lista de inclusão

Lista de chaves de registro no hive HKCU que são processadas durante o logoff.

Exemplo: Software\Adobe.

Se esta política estiver habilitada, apenas as chaves desta lista serão processadas. Se esta política estiver desabilitada, o hive HKCU completo será processado. Se esta política não estiver

configurada aqui, o valor do arquivo .ini será usado. Se esta política não estiver configurada aqui ou no arquivo .ini, todo o HKCU será processado.

Habilitar Lista de Exclusão Padrão - Profile Management 5.5

Lista padrão de chaves de registro no hive HKCU que não são sincronizadas com o perfil do usuário. Use esta política para especificar arquivos de exclusão de GPO sem precisar preenchê-los manualmente.

Se você desabilitar esta política, o Profile Management não excluirá nenhuma chave de registro por padrão. Se você não configurar esta política aqui, o Profile Management usará o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não excluirá nenhuma chave de registro por padrão.

Backup de NTUSER.DAT

Permite um backup da última cópia boa conhecida de NTUSER.DAT e reversão em caso de corrupção.

Se você não configurar esta política aqui, o Profile Management usa o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo .ini, o Profile Management não faz backup do NTUSER.DAT.

Configurações da política de controle de acesso a aplicativos

Esta política controla o acesso do usuário a arquivos, pastas e registros. Um caso de uso típico é aplicar regras para controlar o acesso do usuário a aplicativos instalados em máquinas — seja para tornar os aplicativos visíveis aos usuários relevantes.

Habilitar controle de acesso a aplicativos. Se habilitado, o Profile Management controla o acesso do usuário a itens (como arquivos, pastas e registros) com base nas regras que você fornece.

Existem duas maneiras de criar regras de aplicativo:

- Ferramenta baseada em GUI – **WEM Tool Hub > Rule Generator for App Access Control**
- Ferramenta PowerShell – disponível com o pacote de instalação do Profile Management

Configurações de política de personalização do usuário

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.

- Qual o tamanho máximo que os novos discos de camada de usuário podem atingir.

Para fazer isso, estas duas políticas aparecem na lista de políticas disponíveis:

- Caminho do Repositório da Camada de Usuário - Insira um caminho no formato '\\nome ou endereço do servidor\nome da pasta' no campo Valor.
- Tamanho da Camada de Usuário em GB - O tamanho padrão da camada de usuário de 10 GB é o mínimo que a Citrix® recomenda. Uma camada de usuário é um disco de provisionamento dinâmico que se expande até o tamanho definido à medida que o espaço é usado. As camadas de usuário nunca diminuem de tamanho.

> **Observação:**
>
> Aumentar o Tamanho da Camada de Usuário afeta novas camadas de usuário e expande as existentes. Diminuir o tamanho da camada afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

> Para obter mais informações, consulte Camada de personalização do usuário.

Configurações de política do Virtual Delivery Agent

A seção Virtual Delivery Agent (VDA) contém configurações de política que controlam a comunicação entre o VDA e os controladores de um site.

Importante: O VDA requer informações fornecidas por essas configurações para se registrar em um Delivery Controller™, se você não estiver usando o recurso de atualização automática. Como essas informações são necessárias para o registro, você deve configurar as seguintes configurações usando o Editor de Política de Grupo, a menos que forneça essas informações durante a instalação do VDA:

- Máscara de rede IPv6 de registro do controlador
- Porta de registro do controlador
- SIDs do controlador
- Controladores
- Usar apenas registro de controlador IPv6
- GUID do site

Máscara de rede IPv6 de registro do controlador

Essa configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial (em vez de um IP global, se um estiver registrado). Essa configuração especifica o endereço IPv6 e a rede onde o VDA se registra. O VDA se registra apenas no primeiro endereço que corresponde à máscara de rede especificada. Essa configuração é válida apenas se a configuração de política Usar apenas registro de controlador IPv6 estiver habilitada.

Por padrão, essa configuração está em branco.

Porta de registro do controlador

Use essa configuração apenas se a configuração **Habilitar atualização automática de controladores** estiver desabilitada.

Essa configuração especifica o número da porta TCP/IP que o VDA usa para se registrar em um Controlador ao usar o registro baseado em registro.

Por padrão, o número da porta é definido como 80.

SIDs do Controller

Use esta configuração somente se a configuração **Habilitar atualização automática de controladores** estiver desabilitada.

Esta configuração especifica uma lista de identificadores de segurança (SIDs) de controlador separados por espaço que o VDA usa para se registrar em um Controller ao usar o registro baseado em registro. Esta configuração é opcional e pode ser usada com a configuração **Controladores** para restringir a lista de Controllers usados para registro.

Por padrão, esta configuração está em branco.

Controladores

Use esta configuração somente se a configuração **Habilitar atualização automática de controladores** estiver desabilitada.

Esta configuração especifica uma lista de Nomes de Domínio Totalmente Qualificados (FQDNs) de controlador separados por espaço que o VDA usa para se registrar em um Controller ao usar o registro baseado em registro. Esta configuração é opcional e pode ser usada com a configuração **SIDs do Controller**.

Por padrão, esta configuração está em branco.

Habilitar atualização automática de controladores

Esta configuração permite que o VDA se registre em um Controller automaticamente após a instalação.

Após o registro do VDA, o Controller com o qual ele se registrou envia uma lista dos FQDNs e SIDs do controlador atual para o VDA. O VDA grava esta lista em armazenamento persistente. Cada Controller também verifica o banco de dados do Site a cada 90 minutos para obter informações do Controller. O Controller envia listas atualizadas para seus VDAs registrados se um dos seguintes ocorrer:

- Um Controller foi adicionado ou removido desde a última verificação
- Uma alteração de política ocorreu

O VDA aceita conexões de todos os Controllers na lista mais recente que recebeu.

Por padrão, esta configuração está ativada.

Usar apenas registro de controlador IPv6

Esta configuração controla qual forma de endereço o VDA usa para se registrar no Controller:

- Quando ativado, o VDA se registra no Controller usando o endereço IPv6 da máquina. Quando o VDA se comunica com o Controller, ele usa a seguinte ordem de endereços: endereço IP global, Endereço Local Único (ULA), endereço link-local (se nenhum outro endereço IPv6 estiver disponível).
- Quando desativado, o VDA se registra e se comunica com o Controller usando o endereço IPv4 da máquina.

Por padrão, esta configuração está desativada.

GUID do Site

Use esta configuração somente se a configuração **Ativar atualização automática de controladores** estiver desativada.

Esta configuração especifica o Identificador Globalmente Único (GUID) do site que o VDA usa para se registrar em um Controller ao usar o registro baseado no Active Directory.

Por padrão, esta configuração está em branco.

Configurações de política de monitoramento

A seção **Monitoramento** inclui configurações de política para monitoramento de processos, recursos e falhas de aplicativos.

O escopo dessas políticas pode ser definido com base no seguinte:

- Site
- Grupo de entrega
- Tipo de grupo de entrega
- Unidade organizacional
- Tags

Políticas para monitoramento de processos e recursos

Cada ponto de dados para CPU, memória e processos é coletado do VDA e armazenado no banco de dados de Monitoramento. O envio dos pontos de dados do VDA consome largura de banda da rede e o armazenamento deles consome espaço considerável no banco de dados de monitoramento. Considere que você não deseja monitorar dados de recursos ou dados de processos, ou ambos, para um escopo específico. Por exemplo, um grupo de entrega ou unidade organizacional específica. Nesse caso, é recomendável desabilitar a política.

HABILITAR MONITORAMENTO DE PROCESSOS

Habilite esta configuração para permitir o monitoramento de processos em execução em máquinas com VDAs. Estatísticas como uso de CPU e memória são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificações em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Desabilitado.

HABILITAR MONITORAMENTO DE RECURSOS

Habilite esta configuração para permitir o monitoramento de contadores de desempenho críticos em máquinas com VDAs. Estatísticas (como uso de CPU e memória, IOPS e dados de latência de disco) são enviadas para o Serviço de Monitoramento. As estatísticas são usadas para notificação em tempo real e relatórios históricos no Director.

O padrão para esta configuração é Habilitado.

ESCALABILIDADE

Os dados de CPU e memória são enviados para o banco de dados de cada VDA em intervalos de 5 minutos. Os dados de processo (se ativados) são enviados para o banco de dados em intervalos

de 10 minutos. Os dados de IOPS e latência de disco são enviados para o banco de dados em intervalos de 1 hora.

DADOS DE CPU E MEMÓRIA

Os dados de CPU e memória estão **ativados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados de 5 Minutos	1 Dia
Dados de 10 Minutos	7 Dias
Dados Horários	30 Dias
Dados Diários	90 Dias

DADOS DE IOPS E LATÊNCIA DE DISCO

Os dados de IOPS e latência de disco estão **ativados** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados Horários	3 Dias
Dados Diários	90 Dias

Com as configurações de retenção de dados, aproximadamente 276 KB de espaço em disco são necessários para armazenar o seguinte para um VDA durante um período de um ano:

- CPU
- Memória
- IOPS
- Dados de latência de disco

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO
1	276 KB

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO
1K	270 MB
40K	10.6 GB

DADOS DE PROCESSO

Os dados de processo estão **Desativados** por padrão. Recomenda-se habilitar os dados de processo em um subconjunto de máquinas conforme a necessidade. As configurações padrão de retenção de dados para os dados de processo são as seguintes:

GRANULARIDADE DOS DADOS	NÚMERO DE DIAS
Dados de 10 minutos	1 Dia
Dados por Hora	7 Dias

Se os dados de processo forem habilitados com as configurações de retenção padrão, os dados de processo consumiriam aproximadamente 1,5 MB por VDA e 3 MB por VDA de Serviços de Terminal (TS VDA) durante um período de um ano.

NÚMERO DE MÁQUINAS	ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA VDA	ARMAZENAMENTO APROXIMADO NECESSÁRIO PARA TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

Observação:

Os números fornecidos anteriormente não incluem o espaço do Índice. E todos os cálculos são aproximados e variam dependendo da implantação.

CONFIGURAÇÕES OPCIONAIS

Você pode modificar as configurações de retenção padrão para atender às suas necessidades. No entanto, essa configuração consome armazenamento extra. Ao habilitar as configurações abaixo,

você pode obter mais precisão nos dados de utilização do processo. As configurações que podem ser habilitadas são:

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

Essas configurações podem ser habilitadas a partir do cmdlet do PowerShell de Monitoramento: Set-MonitorConfiguration

Políticas para monitoramento de falhas de aplicativos

A guia **Falha de Aplicativo**, por padrão, exibe apenas falhas de aplicativos de VDAs de SO de múltiplas sessões. As configurações de monitoramento de falhas de aplicativos podem ser modificadas com as seguintes políticas de Monitoramento:

HABILITAR MONITORAMENTO DE FALHAS DE APLICATIVOS

Use esta configuração para configurar o monitoramento de falhas de aplicativos para monitorar erros ou falhas de aplicativos (travamentos e exceções não tratadas), ou ambos. Desabilite o monitoramento de falhas de aplicativos definindo o **Valor** como **Nenhum**. O padrão para esta configuração é apenas falhas de aplicativos.

HABILITAR MONITORAMENTO DE FALHAS DE APLICATIVOS EM VDAS DE SO DE SESSÃO ÚNICA

Por padrão, apenas as falhas de aplicativos hospedados em VDAs de SO de múltiplas sessões são monitoradas. Para monitorar VDAs de SO de sessão única, defina a política como **Permitido**. O padrão para esta configuração é **Proibido**.

LISTA DE APLICATIVOS EXCLUÍDOS DO MONITORAMENTO DE FALHAS

Especifique uma lista de aplicativos que não devem ser monitorados quanto a falhas. Por padrão, esta lista está vazia.

Política para coleta de dados para Análise

COLETA DE DADOS VDA PARA ANÁLISE

Use a política para habilitar ou desabilitar o serviço Monitor de coletar métricas relacionadas a desempenho e segurança dos VDAs para Análise de Desempenho e Segurança. Por padrão, a política é **Permitida**. Defina a política como **Proibida** para interromper a coleta de dados dos VDAs.

COLETA DE METADADOS DE LOCAL DA ÁREA DE TRANSFERÊNCIA PARA MONITORAMENTO DE SEGURANÇA

Use a política para habilitar ou desabilitar a coleta de metadados de local da área de transferência pelo serviço Broker para monitoramento de segurança, auditoria e conformidade. Por padrão, a política é **Habilitada**. Defina a política como **Desabilitada** para interromper a coleta de dados dos VDAs.

COLETA DE DADOS DE DIAGNÓSTICO PARA MONITORAMENTO DE DESEMPENHO

Use esta política para habilitar o serviço de monitoramento a coletar dados de diagnóstico, como informações de sessão, estados de serviço UPM/EUEM, otimização do Microsoft Teams e protocolos de conexão. Por padrão, a política é **Habilitada**. Defina a política como **Desabilitada** para interromper a coleta de dados dos VDAs.

Dicas de planejamento de armazenamento

Política de grupo. Se você não estiver interessado em monitorar os Dados de Recurso ou Dados de Processo, um ou ambos podem ser desativados usando a política de grupo. Para obter mais informações, consulte a seção **Política de Grupo** de Criar políticas.

Limpeza de dados. As configurações padrão de retenção de dados podem ser modificadas para limpar os dados mais cedo e liberar espaço de armazenamento. Para obter mais informações sobre as configurações de limpeza, consulte Granularidade e retenção de dados em Acessando dados usando a API.

Configurações de política de IP Virtual

> **Importante:**
>
> - O Windows 10 Enterprise multissessão não oferece suporte à Virtualização de IP de Área de Trabalho Remota (IP Virtual) e não oferecemos suporte à Virtualização de IP de Área de Trabalho Remota ou loopback virtual no Windows 10 Enterprise multissessão.
> - A Virtualização de IP de Área de Trabalho Remota (IP Virtual) não é compatível com máquinas hospedadas na nuvem. Para obter mais informações, consulte a documentação da Microsoft.

A seção **IP Virtual** inclui configurações de política que controlam se as sessões têm seu próprio endereço de loopback virtual.

Suporte a loopback de IP Virtual

Quando esta configuração está ativada, cada sessão tem seu próprio endereço de loopback virtual. Quando desativada, as sessões não têm endereços de loopback individuais.

Por padrão, esta configuração está desativada.

Lista de programas de loopback virtual de IP Virtual

Esta configuração especifica os executáveis de aplicativo que podem usar endereços de loopback virtual. Ao adicionar programas à lista, especifique apenas o nome do executável. Você não precisa especificar o caminho completo.

Por padrão, nenhum executável é especificado.

Exclusão de porta de loopback de IP Virtual

Quando um aplicativo chama o endereço de loopback em qualquer porta especificada nesta configuração, o loopback virtual não altera a chamada para o endereço de loopback específico da sessão

Configurar as configurações de Redirecionamento de Porta COM e Porta LPT usando o registro

Nas versões do VDA de 7.0 a 7.8, as configurações de **Porta COM e Porta LPT** são configuráveis apenas usando o registro. Para versões do VDA anteriores a 7.0 e para versões do VDA 7.9 e posteriores, essas configurações são configuráveis no Web Studio. Para obter mais informações, consulte Configurações de política de redirecionamento de porta e Configurações de política de largura de banda.

As configurações de política para Redirecionamento de Porta COM e Porta LPT estão localizadas em HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated na imagem ou máquina VDA.

Para habilitar o redirecionamento de porta COM e porta LPT, adicione novas chaves de registro do tipo REG_DWORD, da seguinte forma:

Cuidado: Editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

CHAVE DO REGISTRO	DESCRIÇÃO	VALORES PERMITIDOS
AllowComPortRedirection	Permitir ou proibir o redirecionamento da porta COM	1 (Permitir) ou 0 (Proibir)
LimitComBw	Limite de largura de banda para o canal de redirecionamento da porta COM	Valor numérico
LimitComBWPercent	Limite de largura de banda para o canal de redirecionamento da porta COM como uma porcentagem da largura de banda total da sessão	Valor numérico entre 0 e 100
AutoConnectClientComPorts	Conectar automaticamente as portas COM do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)
AllowLptPortRedirection	Permitir ou proibir o redirecionamento de porta LPT	1 (Permitir) ou 0 (Proibir)
LimitLptBw	Limite de largura de banda para o canal de redirecionamento de porta LPT	Valor numérico
LimitLptBwPercent	Limite de largura de banda para o canal de redirecionamento de porta LPT como uma porcentagem da largura de banda total da sessão	Valor numérico entre 0 e 100
AutoConnectClientLptPorts	Conectar automaticamente as portas LPT do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)

Após configurar essas configurações, altere seus catálogos de máquinas para usar a nova imagem mestre ou a máquina física atualizada. Os desktops são atualizados com as novas configurações na próxima vez que os usuários fizerem logoff.

Configurações de política do Connector para Configuration Manager 2012

A seção Connector para Configuration Manager 2012 contém configurações de política para configurar o agente Citrix Connector 7.5.

> **Importante:**
>
> As políticas de mensagem de aviso, logoff e reinicialização aplicam-se apenas a implantações em catálogos de máquinas de SO de múltiplas sessões que são gerenciados manualmente ou por Provisioning Services. Para esses catálogos de máquinas, o serviço Connector alerta os usuários quando há instalações de aplicativos ou atualizações de software pendentes.

> Para catálogos gerenciados por MCS, use o Web Studio para notificar os usuários. Para catálogos de SO de sessão única gerenciados manualmente, use o Configuration Manager para notificar os usuários. Para catálogos de SO de sessão única gerenciados por Provisioning Services, use o Provisioning Services para notificar os usuários.

Intervalo de frequência de aviso

Essa configuração define o intervalo entre as aparições da mensagem de aviso aos usuários.

Os intervalos são definidos usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração do intervalo é de 1 hora (01:00:00).

Texto do corpo da caixa de mensagem de aviso

Essa configuração contém o texto editável da mensagem aos usuários, notificando-os sobre as próximas atualizações de software ou manutenção que exige que eles façam logoff.

Por padrão, a mensagem é: {TIMESTAMP} Salve seu trabalho. O servidor ficará offline para manutenção em {TIMELEFT}.

Título da caixa de mensagem de aviso

Esta configuração contém o texto editável da barra de título da mensagem de aviso aos usuários.

Por padrão, o título é: Manutenção Programada

Período de tempo do aviso

Esta configuração define quanto tempo antes da manutenção a mensagem de aviso aparece pela primeira vez.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração é de 16 horas (16:00:00), indicando que a primeira mensagem de aviso aparece aproximadamente 16 horas antes da manutenção.

Texto do corpo da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da mensagem que alerta os usuários de que um logoff forçado foi iniciado.

Por padrão, a mensagem é: O servidor está atualmente ficando offline para manutenção

Título da caixa de mensagem de logoff forçado final

Esta configuração contém o texto editável da barra de título da mensagem final de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

Período de carência para logoff forçado

Esta configuração define o período entre a notificação aos usuários para fazer logoff e a implementação do logoff forçado para processar a manutenção pendente.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0–999.

- hh são horas com um intervalo de 0–23.
- mm são minutos com um intervalo de 0–59.
- ss são segundos com um intervalo de 0–59.

Por padrão, a configuração do período de carência para logoff forçado é de 5 minutos (00:05:00).

Texto do corpo da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da mensagem que informa aos usuários para salvar seu trabalho e fazer logoff antes de iniciar um logoff forçado.

Por padrão, a mensagem contém o seguinte: {TIMESTAMP} Salve seu trabalho e faça logoff. O servidor ficará offline para manutenção em {TIMELEFT}.

Título da caixa de mensagem de logoff forçado

Esta configuração contém o texto editável da barra de título da mensagem de logoff forçado.

Por padrão, o título é: Notificação da Equipe de TI

Modo gerenciado por imagem

O agente do Connector detecta automaticamente se está sendo executado em um clone de máquina gerenciado pelo Provisioning Services ou MCS. O agente bloqueia as atualizações do Configuration Manager em clones gerenciados por imagem e instala automaticamente as atualizações na imagem mestre do catálogo.

Depois que uma imagem mestre é atualizada, use o Web Studio para orquestrar a reinicialização dos clones do catálogo MCS. O Agente do Connector orquestra automaticamente a reinicialização dos clones do catálogo PVS durante as janelas de manutenção do Configuration Manager. Para substituir esse comportamento, de modo que o software seja instalado nos clones do catálogo pelo Configuration Manager, altere o Modo gerenciado por imagem para Desabilitado.

Texto do corpo da caixa de mensagem de reinicialização

Essa configuração contém o texto editável da mensagem que notifica os usuários quando o servidor está prestes a ser reiniciado.

Por padrão, a mensagem é: O servidor está atualmente ficando offline para manutenção.

Intervalo de tempo regular em que a tarefa do agente deve ser executada

Essa configuração determina a frequência com que a tarefa do agente Citrix Connector™ é executada.

O tempo é definido usando o formato ddd.hh:mm:ss, onde:

- ddd são dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh são horas com um intervalo de 0 a 23.
- mm são minutos com um intervalo de 0 a 59.
- ss são segundos com um intervalo de 0 a 59.

Por padrão, a configuração do intervalo de tempo regular é de 5 minutos (00:05:00).

Alterações de política

A tabela a seguir lista as atualizações de política no Citrix Virtual Apps and Desktops™ 7 2407, incluindo adições, remoções, alterações de nome e alterações de estado padrão.

CONFIGURAÇÃO DE POLÍTICA	ALTERAÇÕES
Geral - Clareza sobre políticas dependentes	Saiba mais.
Geral - Capacidade de selecionar várias políticas	Saiba mais.
Gerenciamento de Perfil > Configurações avançadas > Habilitar failover de contêiner de política em sessão entre armazenamentos de usuário	Nova política para failover de contêiner de perfil em sessão entre armazenamentos de usuário. Saiba mais.
Gerenciamento de Perfil > Registro > Lista de inclusão	Suporte à exclusão e inclusão de registro estendido para solução de perfil baseada em contêiner. Saiba mais.
Gerenciamento de Perfil > Registro > Lista de exclusão	
Gerenciamento de Perfil > Redirecionamento de Pasta	Aprimoramentos nas políticas de Redirecionamento de Pasta. Saiba mais.
Coleta de métricas de sessão	Para obter mais informações, consulte configurações de política ICA.
Configurações de política de impressoras cliente > Impressoras cliente retidas e restauradas	Preterido desde 2402

Observação:

Exclua todas as configurações preteridas antes de atualizar. Se alguma configuração preterida permanecer em uso, a atualização poderá falhar com um erro.

Gerenciar

O gerenciamento de um site Citrix Virtual Apps and Desktops™ abrange vários itens e tarefas.

Licenciamento

É necessária uma conexão válida com o Citrix License Server ao criar um site. Posteriormente, você pode concluir várias tarefas de licenciamento no Studio, incluindo adicionar licenças, alterar tipos ou modelos de licença e gerenciar administradores de licença. Você também pode acessar o Console de Administração de Licenças a partir do Studio.

Aplicativos

Gerencie aplicativos em Delivery Groups e, opcionalmente, em Application Groups.

Zonas

Em uma implantação geograficamente dispersa, você pode usar zonas para manter aplicativos e desktops mais próximos dos usuários finais, o que pode melhorar o desempenho. Ao instalar e configurar um site, todos os Controllers, catálogos de máquinas e conexões de host estão em uma zona primária. Posteriormente, você pode usar o Studio para criar zonas satélites contendo esses itens. Depois que seu site tiver mais de uma zona, você poderá indicar em qual zona quaisquer catálogos de máquinas, conexões de host ou Controllers adicionados recém-criados serão colocados. Você também pode mover itens entre zonas.

Conexões e recursos

Se você estiver usando um hipervisor ou outro serviço para hospedar máquinas que fornecem aplicativos e desktops aos usuários, você cria sua primeira conexão com esse hipervisor ou outro serviço ao criar um site. Os detalhes de armazenamento e rede para essa conexão formam seus recursos. Posteriormente, você pode alterar essa conexão e seus recursos, e criar mais conexões. Você também pode gerenciar as máquinas que usam uma conexão configurada.

Cache de Host Local

O Cache de Host Local permite que as operações de intermediação de conexão em um site continuem quando a conexão entre um Delivery Controller™ e o banco de dados do site falha.

IP virtual e loopback virtual

O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem de comunicações com o localhost para usar um endereço de loopback virtual exclusivo no intervalo do localhost.

Delivery Controllers

Este artigo contém considerações e procedimentos ao adicionar e remover Controllers de um site. Ele também descreve como mover Controllers para outra zona ou site e como mover um VDA para outro site.

Registro de VDA com Controllers

Antes que um VDA possa ajudar a entregar aplicativos e desktops, ele deve se registrar (estabelecer comunicação) com um Controller. Os endereços dos Controllers podem ser especificados de várias maneiras, que são descritas neste artigo. É fundamental que os VDAs tenham informações atualizadas à medida que os Controllers são adicionados, movidos e removidos no site.

Sessões

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência do usuário. Vários recursos podem otimizar a confiabilidade das sessões, reduzir inconvenientes, tempo de inatividade e perda de produtividade.

- Confiabilidade da sessão
- Reconexão Automática do Cliente
- Keep-Alive do ICA®
- Controle de workspace
- Roaming de sessão

Usar pesquisa no Studio

Quando você quiser visualizar informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou Delivery Groups no Studio, use o recurso de pesquisa flexível.

Tags

Use tags para identificar itens como máquinas, aplicativos, grupos e políticas. Você pode então adaptar certas operações para aplicar apenas a itens com uma tag específica.

IPv4/IPv6

O Citrix Virtual Apps and Desktops oferece suporte a implantações IPv4 puro, IPv6 puro e dual-stack que usam redes IPv4 e IPv6 sobrepostas. Este artigo descreve e ilustra essas implantações. Ele também descreve as configurações de política do Citrix que controlam o uso de IPv4 ou IPv6.

Perfis de usuário

Por padrão, o Citrix Profile Management é instalado automaticamente quando você instala um VDA. Se você usa essa solução de perfil, revise este artigo para obter informações gerais. Consulte a documentação do Profile Management para obter detalhes.

Coletar rastreamentos do Citrix Diagnostic Facility (CDF)

O utilitário CDFControl é um controlador ou consumidor de rastreamento de eventos para capturar mensagens de rastreamento do Citrix Diagnostic Facility (CDF) exibidas por vários provedores de rastreamento Citrix. Ele foi criado para solucionar problemas complexos relacionados ao Citrix, analisar o suporte a filtros e coletar dados de desempenho.

Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios.

Citrix Scout

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manutenção proativa em sua implantação do Citrix Virtual Apps and Desktops. A Citrix oferece análise abrangente e automatizada de coleções de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

Aplicativos

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Se sua implantação usa apenas grupos de entrega (e não grupos de aplicativos), você adiciona aplicativos aos grupos de entrega. Se você também tiver grupos de aplicativos, geralmente adiciona aplicativos aos grupos de aplicativos. Esta orientação facilita a administração. Um aplicativo deve sempre pertencer a pelo menos um grupo de entrega ou grupo de aplicativos.

No assistente Adicionar Aplicativos, você pode selecionar um ou mais grupos de entrega, ou um ou mais grupos de aplicativos, mas não ambos. Embora você possa alterar posteriormente a associação de grupo de um aplicativo (por exemplo, mover um aplicativo de um grupo de aplicativos para um grupo de entrega), a melhor prática desencoraja adicionar essa complexidade. Mantenha seus aplicativos em um único tipo de grupo.

Quando você associa um aplicativo a mais de um grupo, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo está associado.

Se você publicar dois aplicativos com o mesmo nome (talvez de grupos diferentes) para os mesmos usuários, altere a propriedade `Application name (for user)` no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace™.

Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Você também pode alterar a pasta do aplicativo onde o aplicativo é colocado, seja ao adicionar o aplicativo ou posteriormente.

Para obter detalhes, consulte:

- Criar grupos de entrega
- Criar grupos de aplicativos
- Tags

Adicionar aplicativos

Você pode adicionar aplicativos ao criar um grupo de entrega ou um grupo de aplicativos. Esses procedimentos são detalhados em Criar grupos de entrega e Criar grupos de aplicativos. O procedimento a seguir descreve como adicionar aplicativos depois de criar um grupo.

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega do Remote PC Access.

- Você não pode usar o assistente Adicionar Aplicativo para remover aplicativos de grupos de entrega ou grupos de aplicativos. Essa é uma operação separada.

Para adicionar um ou mais aplicativos:

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione **Adicionar Aplicativos** na barra de ações.
2. O assistente Adicionar Aplicativos é iniciado com uma página de **Introdução**, que você pode remover de futuras inicializações deste assistente.
3. O assistente o guia pelas páginas **Grupos**, **Aplicativos** e **Resumo**. Ao concluir cada página, clique em **Avançar** até chegar à página **Resumo**.

Alternativas à etapa 1 se você quiser adicionar aplicativos a um único grupo de entrega ou grupo de aplicativos:

- **Para adicionar aplicativos a apenas um grupo de entrega:** Na etapa 1, selecione **Grupos de Entrega** no painel esquerdo do Web Studio, selecione um grupo de entrega no painel central e, em seguida, selecione **Adicionar Aplicativos** na barra de ações. O assistente não exibe a página **Grupos**.
- **Para adicionar aplicativos a apenas um grupo de aplicativos:** Na etapa 1, selecione **Aplicativos** no painel esquerdo do Web Studio, selecione um grupo de aplicativos no painel central e, em seguida, selecione a entrada **Adicionar Aplicativos** sob o nome do grupo de aplicativos na barra de ações. O assistente não exibe a página **Grupos**.

Página Grupos

Esta página lista todos os grupos de entrega no site. Se você também criou grupos de aplicativos, a página lista os grupos de aplicativos e os grupos de entrega. Você pode escolher entre um dos grupos, mas não de ambos. Em outras palavras, você não pode adicionar aplicativos a um grupo de aplicativos e a um grupo de entrega ao mesmo tempo. Geralmente, se você estiver usando grupos de aplicativos, adicione aplicativos a grupos de aplicativos, em vez de grupos de entrega.

Ao adicionar um aplicativo, marque a caixa de seleção ao lado de pelo menos um grupo de entrega (ou grupo de aplicativos, se disponível). Todo aplicativo deve estar sempre associado a pelo menos um grupo.

Página Aplicativos

Clique em **Adicionar** para exibir as fontes de aplicativos.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta fonte não pode ser selecionada se você (1) selecionou grupos de aplicativos sem grupos de entrega associados, (2) selecionou grupos de aplicativos com grupos de entrega associados que não contêm máquinas, ou (3) selecionou um grupo de entrega que não contém máquinas.

- **Manualmente:** Aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. A seleção desta fonte abre uma nova página onde você especifica um aplicativo a ser adicionado das seguintes maneiras:

  - Digite o caminho para o executável, diretório de trabalho, argumentos opcionais da linha de comando e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Procurar**, insira as credenciais para acessar o VDA, aguarde a conexão com o VDA e, em seguida, selecione um aplicativo do VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.

- **Existente:** Aplicativos adicionados anteriormente ao site. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se o site não tiver aplicativos.

- **Pacotes de aplicativos:** Aplicativos em pacotes de aplicativos App-V, MSIX, MSIX app attach ou FlexApp. Ao selecionar esta origem, a página **Adicionar Aplicativos de Pacotes** é aberta. Selecione uma origem de pacote de aplicativos, selecione os aplicativos que deseja adicionar na exibição resultante e, em seguida, selecione **OK**. Para obter mais informações, consulte Implantar e entregar pacotes de aplicativos.

- **Grupo de aplicativos**: Grupos de aplicativos. Ao selecionar esta origem, uma nova página é aberta com uma lista de grupos de aplicativos. (Embora a exibição também liste os aplicativos em cada grupo, você pode selecionar apenas o grupo, não aplicativos individuais.) Todos os aplicativos atuais e futuros nos grupos selecionados são adicionados. Marque as caixas de seleção dos grupos de aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se (1) não houver grupos de aplicativos, ou (2) se os grupos de entrega selecionados não suportarem grupos de aplicativos (por exemplo, grupos de entrega com máquinas atribuídas estaticamente).

Conforme observado na tabela, algumas origens na lista **Adicionar** não podem ser selecionadas se não houver uma origem válida desse tipo. As origens incompatíveis (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos) não são incluídas na lista. Os aplicativos que já foram adicionados aos grupos que você escolheu não podem ser selecionados.

Você pode alterar as propriedades (configurações) de um aplicativo nesta página ou posteriormente.

Por padrão, os aplicativos adicionados são colocados na pasta de aplicativos chamada `Applications`. Você pode alterar o aplicativo nesta página ou posteriormente. Se você tentar adicionar um aplicativo e um com o mesmo nome existir na mesma pasta, será solicitado que você renomeie o aplicativo que está adicionando. Você pode aceitar o novo nome oferecido ou recusar e, em seguida, renomear o aplicativo ou selecionar uma pasta diferente. Por exemplo, se `app` já existe na pasta **Aplicativos** e você tenta adicionar outro aplicativo chamado `app` a essa pasta, o novo nome `app_1` é oferecido.

Página de resumo

Se você estiver adicionando 10 ou menos aplicativos, seus nomes serão listados em **Aplicativos a adicionar**. Se você estiver adicionando mais de 10 aplicativos, o número total será especificado.

Revise as informações de resumo e clique em **Concluir**.

Alterar a associação de grupo de um aplicativo

Depois de adicionar um aplicativo, você pode alterar os grupos de entrega e os grupos de aplicativos aos quais o aplicativo está associado.

Você pode arrastar um aplicativo para um grupo adicional. Esta é uma alternativa ao uso de comandos na barra de ações.

Se um aplicativo estiver associado a mais de um grupo de entrega ou grupo de aplicativos, a prioridade do grupo pode ser usada para especificar a ordem em que vários grupos são verificados para encontrar aplicativos. Por padrão, todos os grupos têm prioridade 0 (a mais alta). Grupos com a mesma prioridade são balanceados por carga.

Um aplicativo pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos. Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam apenas desktops, se (1) o grupo de entrega contiver máquinas compartilhadas e tiver sido criado com uma versão do XenDesktop 7.x anterior a 7.9, e (2) você tiver permissão `Edit delivery group`. O tipo de grupo de entrega é

automaticamente convertido para `desktops and applications` quando a caixa de diálogo de propriedades é confirmada.

1. Faça login no Web Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione o aplicativo.
2. Selecione **Propriedades** na barra de ações.
3. Selecione a página **Grupos**.
    - Para adicionar um grupo, clique em **Adicionar** e selecione **Grupos de Aplicativos** ou **Grupos de Entrega**. (Se você não criou nenhum grupo de aplicativos, a única entrada é **Grupos de Entrega**.) Em seguida, selecione um ou mais grupos disponíveis. Grupos que são incompatíveis com o aplicativo, ou que já estão associados ao aplicativo, não podem ser selecionados.
    - Para remover um grupo, selecione um ou mais grupos e clique em **Remover**. Se a remoção da associação do grupo resultar na não associação do aplicativo a nenhum grupo, você será alertado de que o aplicativo será excluído.
    - Para alterar a prioridade de um grupo, selecione o grupo e clique em **Editar Prioridade**. Selecione um valor de prioridade e clique em **OK**.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações e deixar a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Duplicar, habilitar ou desabilitar, renomear ou excluir um aplicativo

As seguintes ações estão disponíveis:

- **Duplicar:** Você pode querer duplicar um aplicativo para criar uma versão diferente com parâmetros ou propriedades distintas. Ao duplicar um aplicativo, ele é automaticamente renomeado com um sufixo exclusivo e colocado ao lado do original. Você também pode querer duplicar um aplicativo e depois adicioná-lo a um grupo diferente. (Após a duplicação, a maneira mais fácil de mover um aplicativo é arrastando-o.)
- **Habilitar ou desabilitar:** Habilitar e desabilitar um aplicativo é uma ação diferente de habilitar e desabilitar um grupo de entrega ou grupo de aplicativos.
- **Renomear:** Você pode renomear apenas um aplicativo por vez. Se você tentar renomear um aplicativo e já existir um com o mesmo nome na mesma pasta ou grupo, será solicitado que você especifique um nome diferente.
- **Excluir:** A exclusão de um aplicativo o remove dos grupos de entrega e grupos de aplicativos aos quais estava associado, mas não da origem que foi usada para adicionar o aplicativo

originalmente. Excluir um aplicativo é uma ação diferente de removê-lo de um grupo de entrega ou grupo de aplicativos.

Para duplicar, habilitar, desabilitar, renomear ou excluir um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um ou mais aplicativos no painel central e, em seguida, selecione a tarefa apropriada na barra de ações.
3. Confirme a ação, quando solicitado.

Remover aplicativos de um grupo de entrega

Um aplicativo deve estar associado (pertencer) a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de entrega que removeria a associação desse aplicativo com qualquer grupo de entrega ou grupo de aplicativos, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente de uma fonte válida.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo de entrega. No painel central inferior, na guia **Aplicativos**, selecione o aplicativo que deseja remover.
3. Selecione **Remover Aplicativo** na barra de ações.
4. Confirme a remoção.

Remover aplicativos de um grupo de aplicativos

Um aplicativo deve pertencer a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de aplicativos que resultará na não pertencimento desse aplicativo a nenhum grupo, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente de uma fonte válida.

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione o grupo de aplicativos no painel central e, em seguida, selecione um ou mais aplicativos.
3. Selecione **Remover do Grupo de Aplicativos** na barra de ações.
4. Confirme a remoção.

Alterar propriedades do aplicativo

Você pode alterar as propriedades de apenas um aplicativo por vez.

Para alterar as propriedades de um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** na barra de ações.
3. Selecione a página que contém a propriedade que você deseja alterar.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Na lista a seguir, a página é mostrada entre parênteses.

PROPRIEDADE	PÁGINA
Categoria/pasta onde o aplicativo aparece no aplicativo Citrix Workspace	Entrega
Argumentos de linha de comando; consulte Passar parâmetros para aplicativos publicados	Localização
Grupos de entrega e grupos de aplicativos onde o aplicativo está disponível	Grupos
Descrição	Identificação
Extensões de nome de arquivo e associação de tipo de arquivo: quais extensões o aplicativo abre automaticamente	Associação de Tipo de Arquivo
Ícone	Entrega
Palavras-chave para StoreFront™	Identificação
Limites; consulte Configurar limites de aplicativo	Entrega
Nome: Nomes vistos pelo usuário e pelo administrador	Identificação

PROPRIEDADE	PÁGINA
Caminho para o executável; consulte Passar parâmetros para aplicativos publicados	Localização
Atalho na área de trabalho do usuário: habilitar ou desabilitar	Entrega
Visibilidade: Limita quais usuários podem ver o aplicativo no aplicativo Citrix Workspace. Um aplicativo invisível ainda pode ser iniciado. Para torná-lo indisponível e invisível, adicione-o a um grupo diferente.	Limitar Visibilidade
Diretório de trabalho	Localização

As alterações do aplicativo podem não ter efeito para os usuários atuais do aplicativo até que eles saiam de suas sessões.

Configurar limites de aplicativo

Configure limites de aplicativo para ajudar a gerenciar o uso do aplicativo. Por exemplo, você pode usar limites de aplicativo para gerenciar o número de usuários acessando um aplicativo simultaneamente. Da mesma forma, os limites de aplicativo podem ser usados para gerenciar o número de instâncias simultâneas de aplicativos que consomem muitos recursos. Esse limite pode ajudar a manter o desempenho do servidor e evitar a deterioração do serviço.

Este recurso limita o número de inicializações de aplicativos que são intermediadas pelo Controller (por exemplo, do aplicativo Citrix Workspace e do StoreFront), e não o número de aplicativos em execução que podem ser iniciados por outros métodos. Isso significa que os limites de aplicativo auxiliam os administradores no gerenciamento do uso simultâneo, mas não fornecem aplicação em todos os cenários. Por exemplo, os limites de aplicativo não podem ser aplicados quando o Controller está no modo de interrupção.

Por padrão, não há limite para quantas instâncias de aplicativo podem ser executadas ao mesmo tempo. Existem várias configurações de limite de aplicativo. Você pode configurar qualquer uma ou todas elas.

- O número máximo de instâncias simultâneas do aplicativo por todos os usuários no grupo de entrega.
- Uma instância do aplicativo por usuário no grupo de entrega.

- O número máximo de instâncias simultâneas do aplicativo por máquina (somente PowerShell).

Se um limite for configurado, uma mensagem de erro será gerada quando um usuário tentar iniciar uma instância do aplicativo que excederá o limite configurado. Se mais de um limite for configurado, um erro será relatado quando o primeiro limite for atingido.

Exemplos de uso de limites de aplicativo:

- **Limite máximo de instâncias simultâneas:** Em um grupo de entrega, você configura o número máximo de instâncias simultâneas do aplicativo `Alpha` para 15. Mais tarde, os usuários nesse grupo de entrega têm 15 instâncias desse aplicativo em execução ao mesmo tempo. Se qualquer usuário nesse grupo de entrega agora tentar iniciar `Alpha`, uma mensagem de erro será gerada. `Alpha` não é iniciado porque excederia o limite configurado de instâncias simultâneas do aplicativo (15).
- **Limite de uma instância por usuário:** Em outro grupo de entrega, você habilita a opção de uma instância por usuário para o aplicativo `Beta`. O usuário Tony inicia o aplicativo `Beta` com sucesso. Mais tarde no dia, enquanto esse aplicativo ainda está em execução na sessão de Tony, ele tenta iniciar outra instância de `Beta`. Uma mensagem de erro é gerada e `Beta` não é iniciado porque excederia o limite de uma instância por usuário.
- **Número máximo de instâncias simultâneas e limites de uma instância por usuário:** Em outro grupo de entrega, você configura um número máximo de instâncias simultâneas de 10 e habilita a opção de uma instância por usuário para o aplicativo `Delta`. Mais tarde, quando 10 usuários nesse grupo de entrega tiverem cada um uma instância de `Delta` em execução, qualquer outro usuário nesse grupo de entrega que tentar iniciar `Delta` receberá uma mensagem de erro. `Delta` não é iniciado. Se qualquer um dos 10 usuários atuais de `Delta` tentar iniciar uma segunda instância desse aplicativo, eles receberão uma mensagem de erro e a segunda instância não será iniciada.
- **Número máximo de instâncias simultâneas por máquina e uso de restrições de tag:** O aplicativo `Charlie` tem requisitos de licenciamento e desempenho que ditam quantas instâncias podem estar em execução ao mesmo tempo em um servidor específico. Esses requisitos também ditam quantas instâncias podem estar em execução simultaneamente em todos os servidores do site.

  O limite de instâncias de aplicativo por máquina afeta qualquer servidor no site (não apenas máquinas em um grupo de entrega específico). Digamos que seu site tenha três servidores. Para o aplicativo `Charlie`, você configura o limite de instâncias de aplicativo por máquina para 2. Assim, não mais do que seis instâncias do aplicativo `Charlie` são permitidas para

iniciar em todo o site. (Isso é um limite de duas instâncias de Charlie em cada um dos três servidores.)

Para restringir o uso de um aplicativo a apenas certas máquinas dentro de um grupo de entrega (além de limitar as instâncias em todas as máquinas em todo o site):

- Use a funcionalidade de marcação para essas máquinas.
- Configure o limite máximo de instâncias por máquina para essa aplicação.

Se os aplicativos forem iniciados por métodos diferentes da intermediação do Controller (por exemplo, enquanto um Controller estiver em modo de interrupção) e os limites configurados forem excedidos, os usuários não poderão iniciar mais instâncias até que fechem instâncias suficientes para não exceder mais os limites. As instâncias que excederam o limite não são encerradas à força. Elas terão permissão para continuar até que seus usuários as fechem.

Se você desabilitar o roaming de sessão, desabilite o limite de uma instância por usuário da aplicação. Se você habilitar o limite de uma instância por usuário da aplicação, não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos. Para obter informações sobre roaming, consulte Sessões.

Para configurar o limite máximo de instâncias por grupo de entrega e o limite de uma instância por usuário:

1. Selecione **Aplicações** no painel esquerdo e, em seguida, selecione uma aplicação.
2. Selecione **Editar Propriedades da Aplicação** na barra de ações.
3. Na página **Entrega**, escolha uma das seguintes opções.

   - **Permitir uso ilimitado da aplicação**. Não há limite para o número de instâncias em execução ao mesmo tempo. Este é o padrão.
   - **Definir limites para a aplicação**. Existem dois tipos de limite; especifique um ou ambos.
     - Especifique o número máximo de instâncias que podem ser executadas simultaneamente por máquina
     - Limitar a uma instância da aplicação por usuário
4. Clique em **OK** para aplicar a alteração e fechar a caixa de diálogo, ou em **Aplicar** para aplicar a alteração e deixar a caixa de diálogo aberta.

Para configurar o limite máximo de instâncias por máquina (somente PowerShell):

- No PowerShell (usando o Remote PowerShell SDK para implantações do Citrix Cloud™, ou o PowerShell SDK para implantações locais), insira o cmdlet `BrokerApplication` apropriado com o parâmetro `MaxPerMachineInstances`.
- Para orientação, use o `Get-Help` cmdlet. Por exemplo:

```
Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
```

Passar parâmetros para aplicativos publicados

Use a página **Location** das propriedades de um aplicativo para inserir a linha de comando e passar parâmetros para aplicativos publicados.

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos `"%*"` (símbolos de porcentagem e asterisco entre aspas duplas) são anexados ao final da linha de comando do aplicativo. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos de usuário.

Se um aplicativo publicado não iniciar conforme o esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos de usuário são validados quando os símbolos `"%*"` são anexados. Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo de usuário, os símbolos `"%**"` são anexados à linha de comando para ignorar a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como `"C:\Program Files"`), coloque a linha de comando do aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Para fazer isso, adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos `%*`. Certifique-se de incluir um espaço entre as aspas de fechamento do caminho e as aspas de abertura dos símbolos `%*`.

Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **Observação:**

> O número máximo de caracteres, incluindo argumentos, na linha de comando para iniciar aplicativos publicados é 203.

Solução de problemas de encerramento de sessão com Aplicativos Publicados

Ao publicar aplicativos, apenas o arquivo executável principal do aplicativo publicado é especificado. No entanto, alguns aplicativos podem produzir processos adicionais (filhos) que são executados em segundo plano e não são fechados pelo arquivo executável principal correspondente quando o aplicativo publicado principal é fechado. Processos adicionais também podem ser criados a partir de scripts executados ou de chaves de registro específicas, como `Run` e `RunOnceKey`. Esses aplicativos podem impedir um encerramento de sessão adequado, resultando em sessões persistentes ou travadas e podem fazer com que a sessão não seja fechada e o usuário seja desconectado.

Nesse caso, você precisa redefinir ou encerrar essas sessões usando o Citrix Director.

Para ajudar a identificar e solucionar problemas de sessões que não estão sendo encerradas corretamente, a Citrix disponibilizou três entradas de registro. A identificação e solução de problemas de sessões que não estão sendo desconectadas corretamente devido a esses problemas é um processo de três etapas:

1. Identificar quais sessões com aplicativos publicados estão impedindo um encerramento de sessão adequado
2. Identificar para esses aplicativos publicados se eles produzem quaisquer processos adicionais (filhos)
3. Adicionar esses processos a uma entrada de registro especificada para evitar que eles impeçam o encerramento da sessão

Passo 2: Identificar se essas aplicações publicadas produzem quaisquer processos adicionais (filhos)

Uma vez que uma aplicação publicada é identificada como impedindo um logoff gracioso, o próximo passo é determinar se esta aplicação produz processos adicionais quando em execução.

Você pode ler `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` para determinar se algum processo está bloqueando um logoff gracioso quando uma aplicação publicada é fechada.

No exemplo a seguir, a chave `LogoffCheckerBlockingProcess` contém as seguintes entradas:

```
PhoneExperienceHost.exe

SkypeApp.exe
```

```
SkypeBackgroundHost.exe
```

Esses processos impediram o logoff gracioso.

Observação:

Substitua o pelo ID de sessão correto para a sessão que você deseja verificar.

Passo 3: Adicionar esses processos a uma entrada de registro especificada para evitar que eles impeçam o logoff

Você pode adicionar esses processos às seguintes chaves de registro para evitar que eles impeçam o logoff em sessões futuras:

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

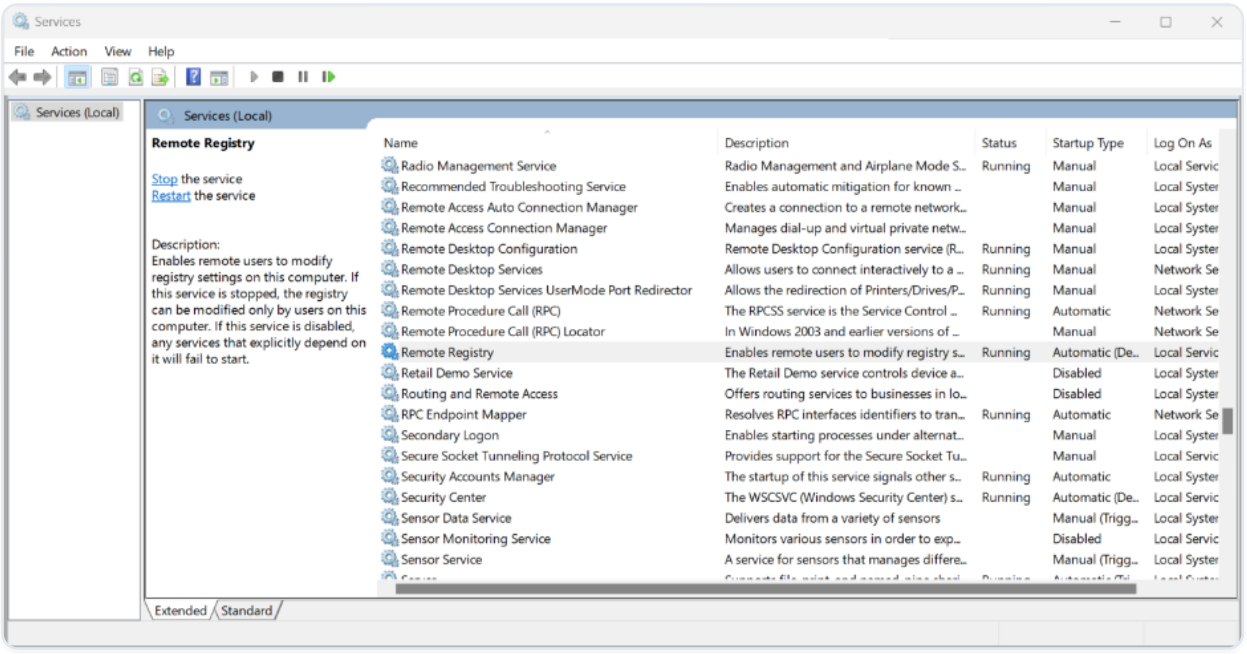
Type:REG_SZ

String:MyAppName.exe
```

Para mais informações sobre `LogoffCheckSysModules`, consulte Logoff gracioso de uma aplicação publicada deixa a sessão em estado ativo.

Guia de solução de problemas passo a passo

1. Inicie o serviço de registro remoto no VDA em teste:
    a. No Painel de Controle, selecione **Ferramentas Administrativas > Serviços**.
    b. Clique com o botão direito em **Serviço de Registro Remoto** e selecione **Propriedades**.
    c. Em **Tipo de Inicialização**, selecione **Automático** no menu suspenso.



2. Desative o Firewall do Windows no VDA em teste ou crie uma regra de firewall de entrada para habilitar a porta 455:

   a. No Painel de Controle, selecione **Firewall do Windows Defender > Configurações Avançadas**.

   b. Clique com o botão direito em **Regras de Entrada** e selecione **Nova Regra**.

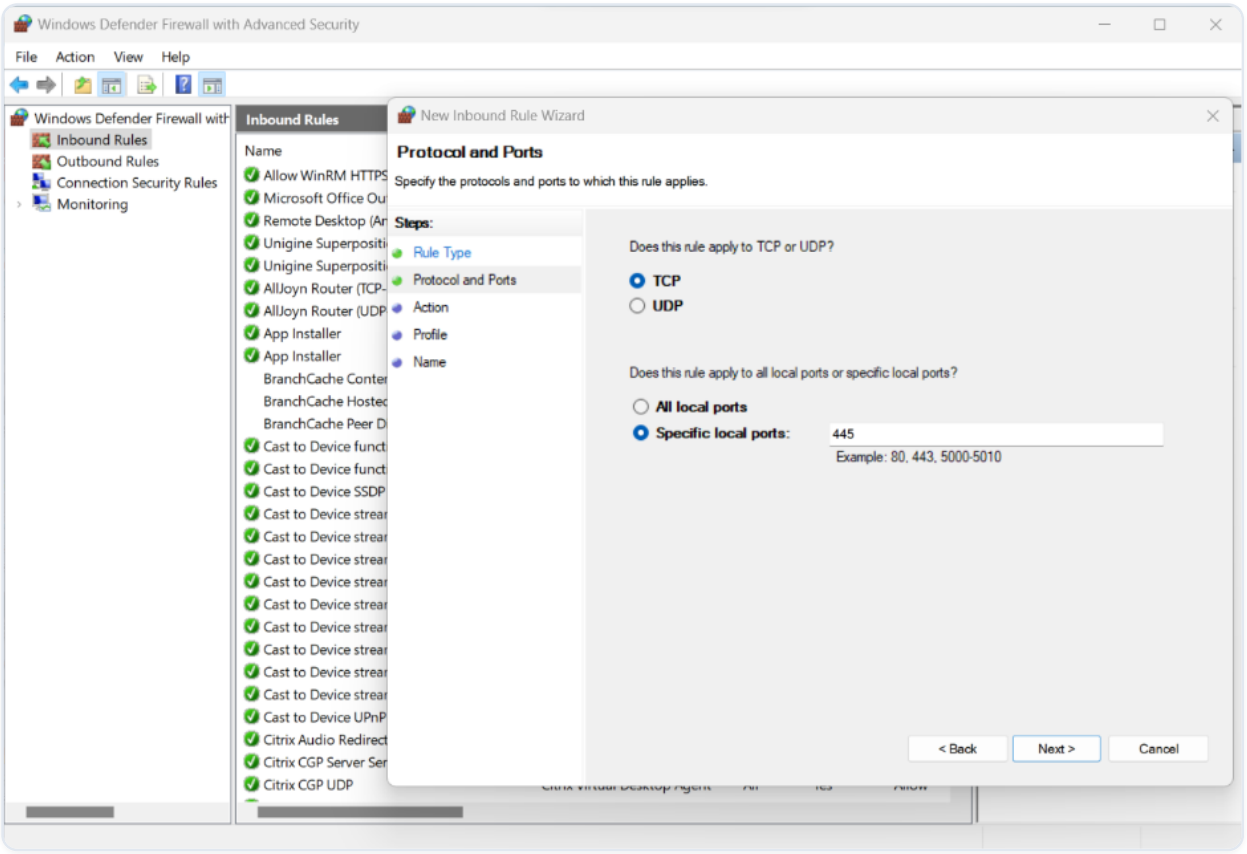
   c. No **Assistente de Nova Regra de Entrada**, selecione **Porta**.

   d. Na página **Protocolos e Portas**, selecione **TCP e Portas Locais Específicas**. Insira `445` como a porta local.

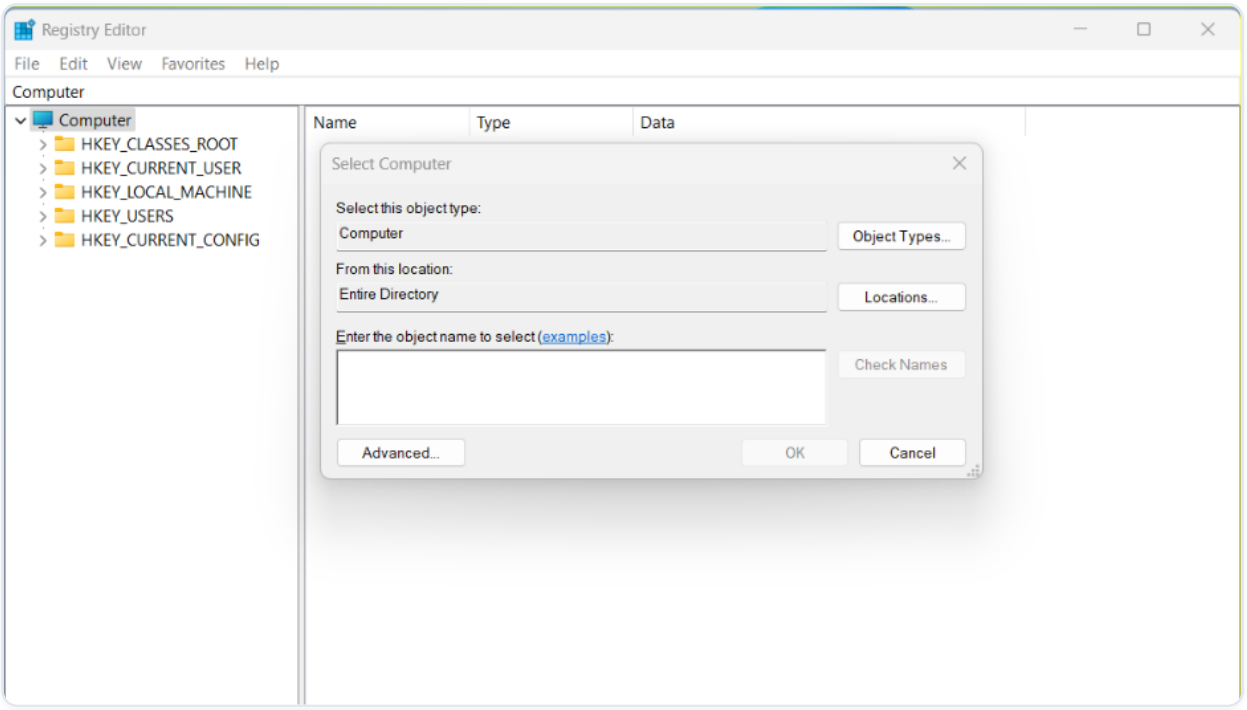
   e. Selecione **Permitir Conexão** na página **Ação**.

   f. Selecione os perfis de firewall aos quais você deseja aplicar a nova regra de entrada.

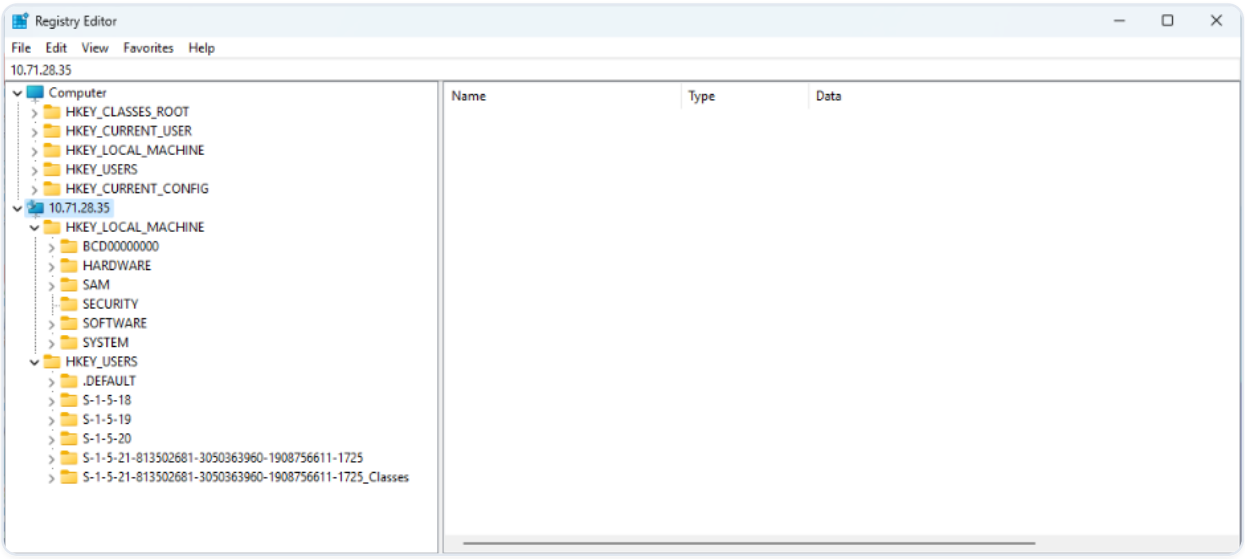
   g. Nomeie a regra de firewall e selecione **Concluir** para sair do **Assistente de Nova Regra de Entrada**.



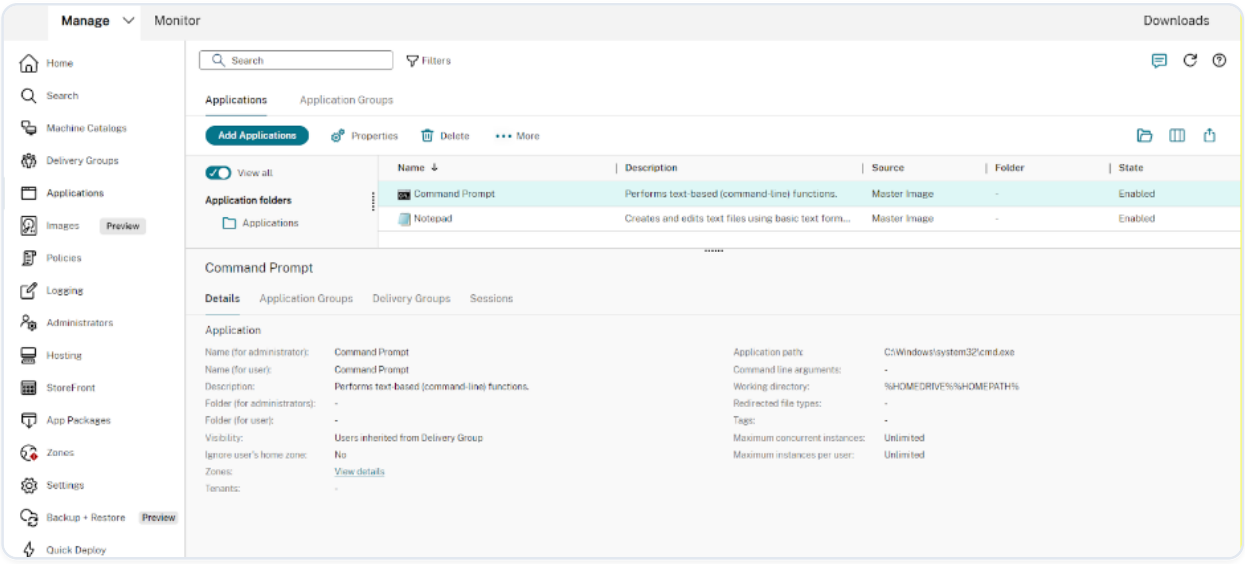
3. De outra VM no mesmo domínio (pode ser DC, DDC ou outro VDA), execute `Regedit` e conecte-se a um registro remoto.



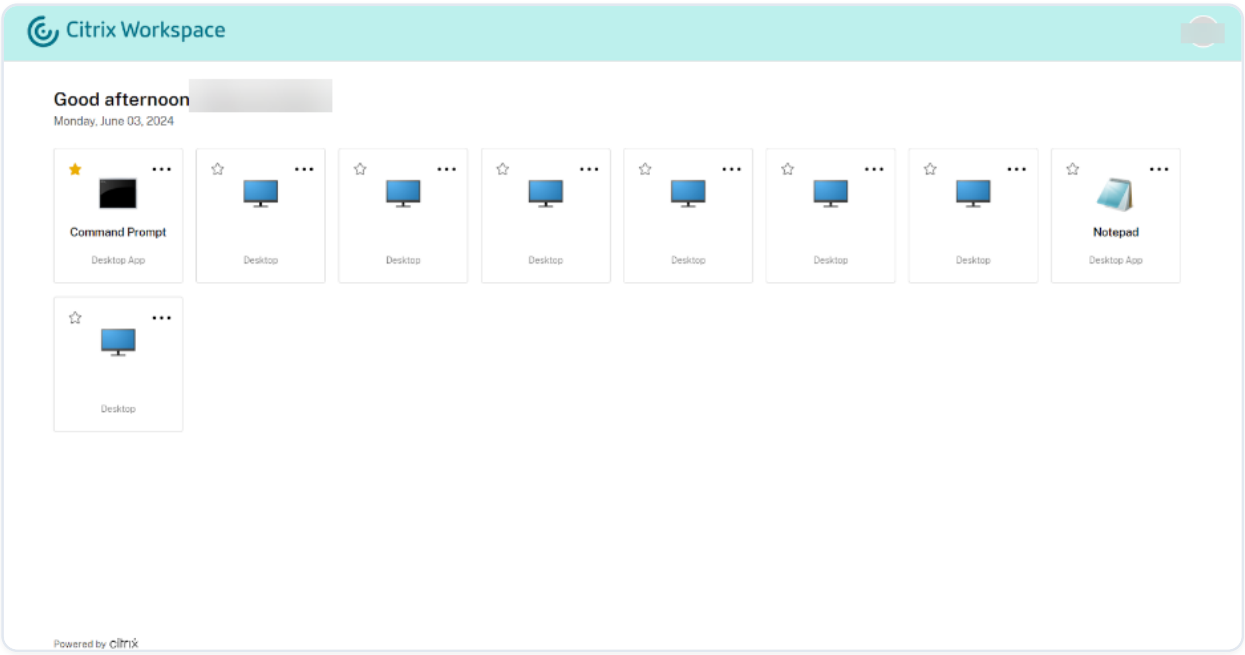
4. Insira o endereço IP do VDA em teste e clique em **OK**. A árvore `regedit` deve exibir ramificações para o VDA em teste.



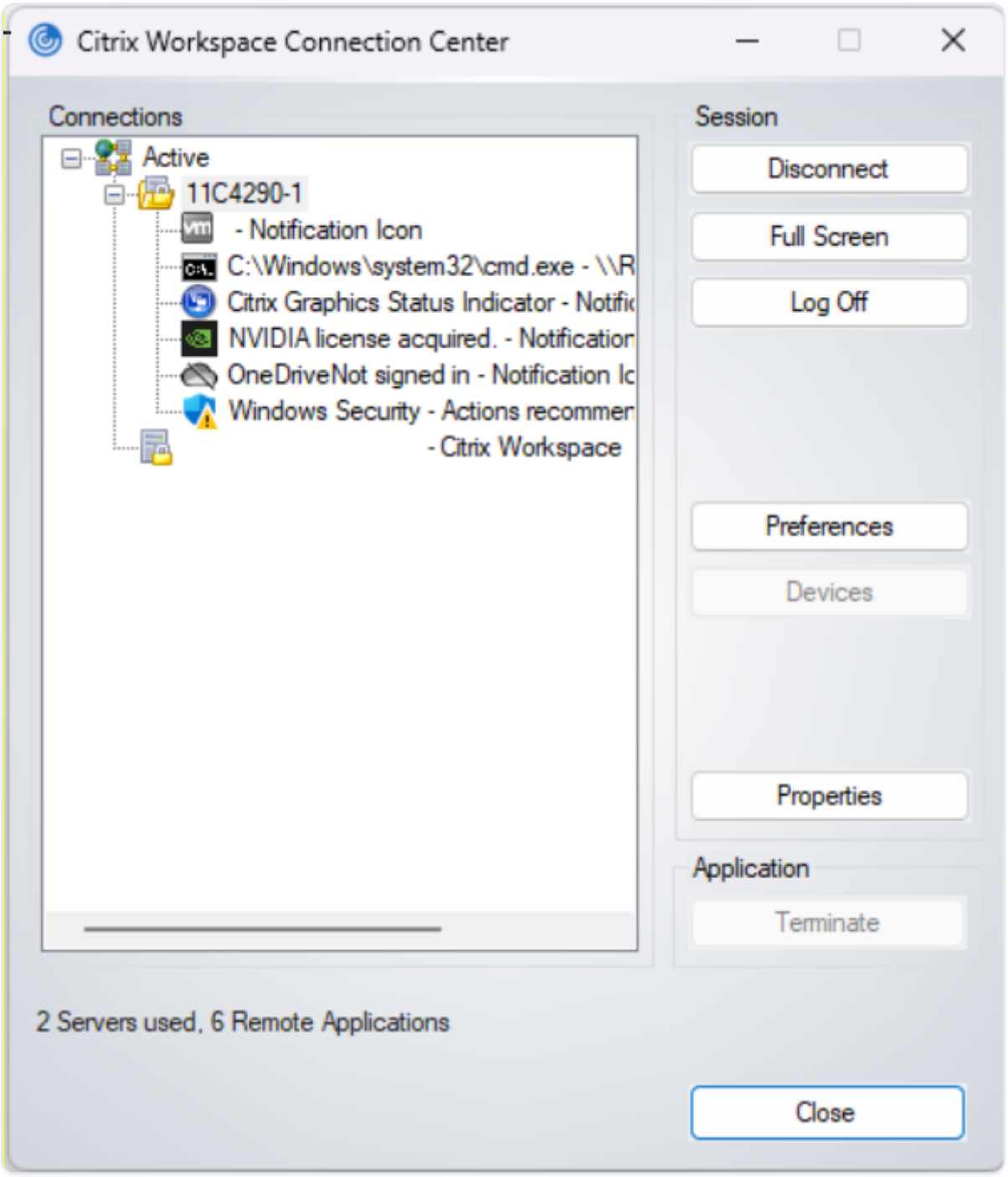
5. Abra o aplicativo publicado **Prompt de Comando**.



O aplicativo **Prompt de Comando** é exibido no Citrix Workspace.



6. Abra o **Centro de Conexão** no cliente. Isso é usado para monitorar quando uma sessão é encerrada, após fechar um aplicativo contínuo aberto. Podemos ver na imagem a seguir que o processo do Prompt de Comando `c:\Windows\system32\cmd.exe` está ativo no VDI remoto.



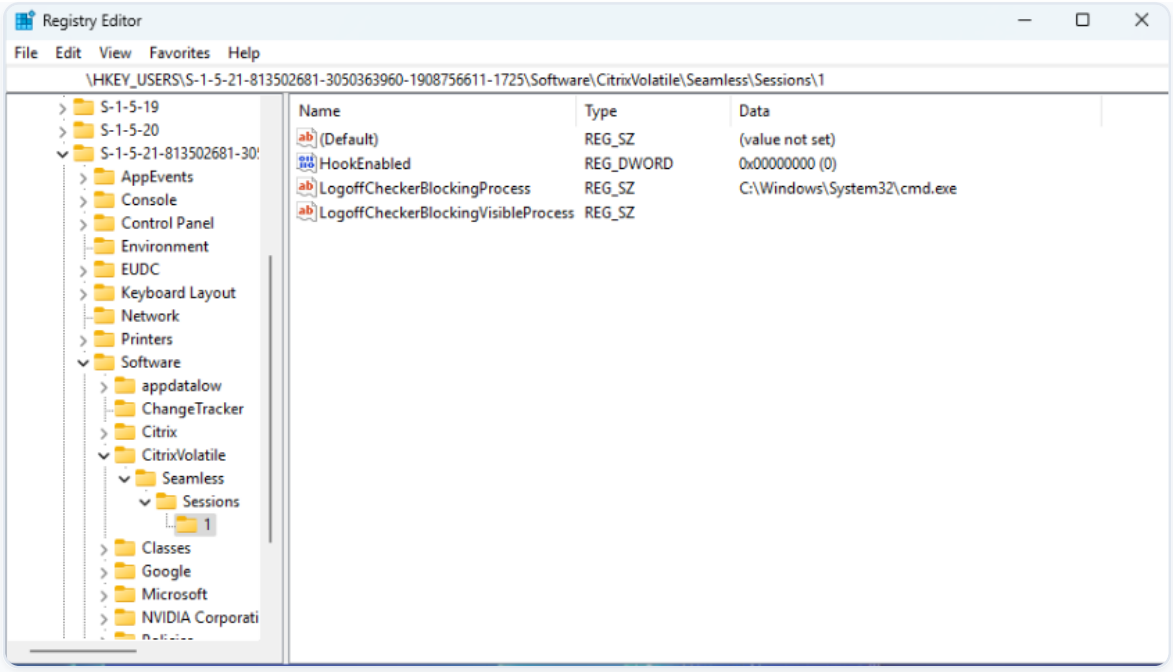
7. No VDA onde o **regedit** está em execução, vá para o seguinte local de IP remoto: `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **Observação:**

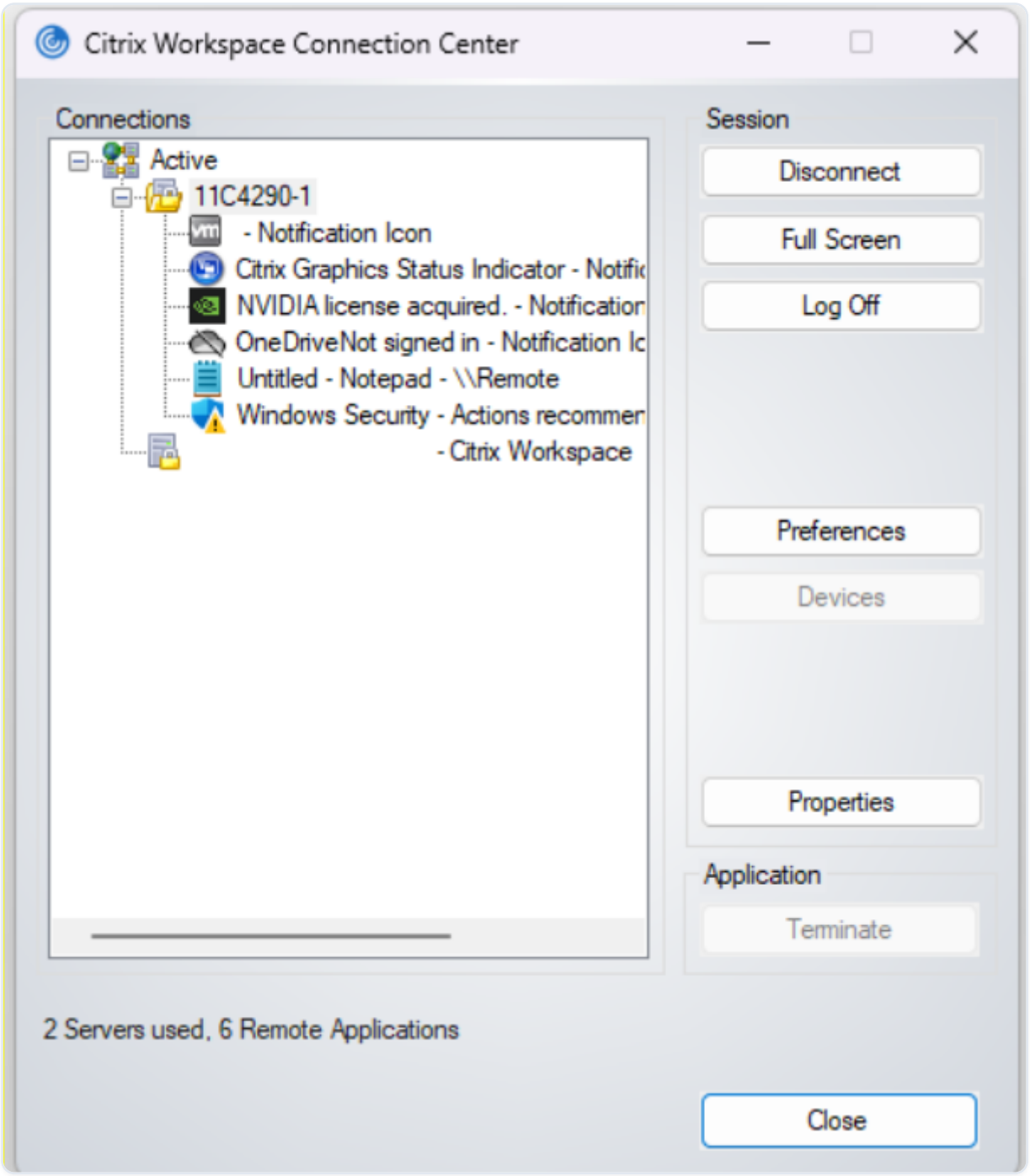
> Este caminho muda toda vez que você abre uma nova sessão.

8. Existem duas chaves para ler aqui (não as altere aqui): **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess**. Essas chaves exibem quaisquer programas que estejam bloqueando o logoff. A primeira deve exibir `C:\Windows\System32\cmd.exe`, pois estava aberta e ainda não foi fechada.

> **Observação:**
>
> **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess** não devem ser editados manualmente. A edição manual desses valores de registro pode levar a sessões instáveis.

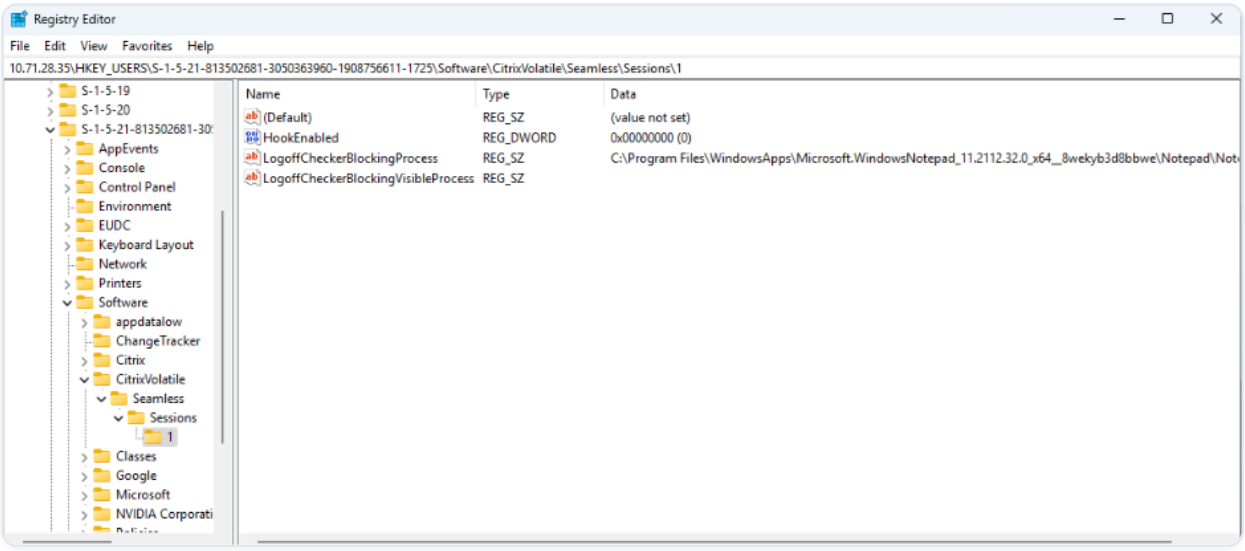


9. Clique em **X** no canto superior direito para sair do **CMD Contínuo**.
10. Verifique o centro de conexão para ver se a sessão é encerrada. Pode levar até 30 segundos para fechar. Se fechar, não houve aplicativos ou processos que impediram um logoff normal.



11. Se a sessão não fechou, atualize a saída do **regedit** com F5.
12. Verifique novamente o conteúdo de **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess**. O CMD não deve mais estar presente, mas deve haver outro processo listado. Qualquer processo que esteja atualmente bloqueando o logoff da sessão deve ser exibido aqui.

    Neste caso, o **Notepad.exe** está aberto a partir do prompt de comando publicado antes que o prompt de comando fosse fechado, e este processo remoto do Notepad está impedindo um logoff normal.



13. Anote o caminho para este executável e em qual chave ele apareceu, e insira-o na seguinte chave de registro, sob a árvore remota:

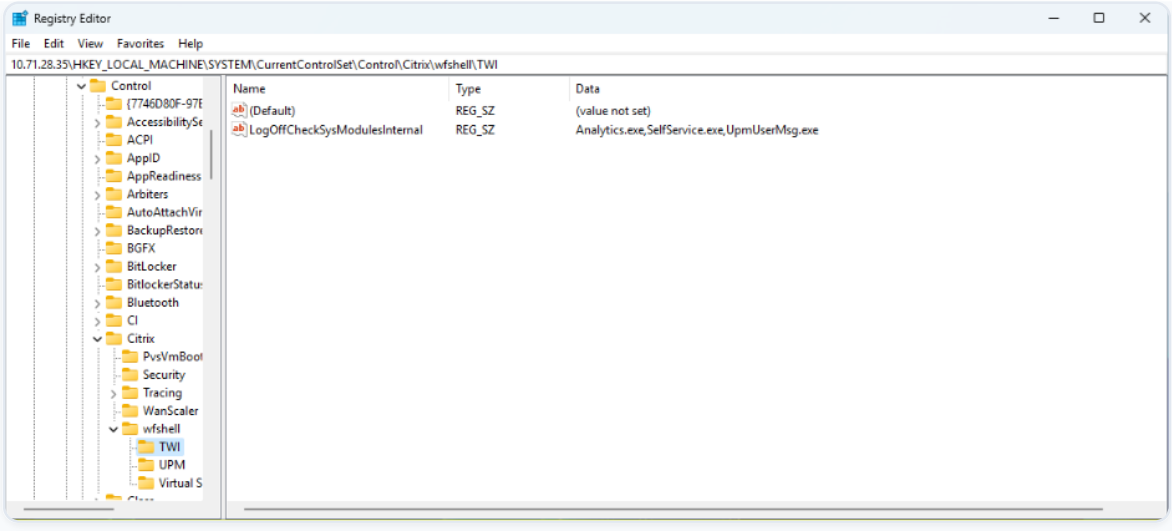
    - Se aparecer em **LogoffCheckBlockingProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - Se aparecer em **LogoffCheckerBlockingVisibleProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **Observação:**
>
> Se já houver uma ou mais entradas na chave, adicione uma vírgula no final e coloque a nova entrada após a vírgula.



14. Saia da sessão do centro de conexão no cliente e reabra o Aplicativo Remoto.

15. Repita os passos 9-16 até que a sessão seja encerrada automaticamente dentro de 30 segundos após fechar o Aplicativo Remoto.

> **Observação:**
>
> Após a solução de problemas, reverta as alterações temporárias do Firewall para permitir o acesso remoto ao registro, se necessário.

Como modificar o LogonUI para visualizar a mensagem de isenção de responsabilidade do Windows em tamanho real ao abrir aplicativos publicados

O escalonamento da janela **LogonUI** é aprimorado para cenários onde a autenticação pass-through não ocorre. A janela **LogonUI** é escalonada com base na resolução do monitor e nas configurações de DPI usadas, o que garante que a janela **LogonUI** completa seja visível sem nenhum corte.

O tamanho da janela em pixels também pode ser definido manualmente no registro.

1. Abra o **Editor do Registro** usando `regedit` no comando **Executar**.
2. Vá para `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Crie duas novas chaves DWORD: **LogonUIWidth** e **LogonUIHeight**.
4. Defina o valor das chaves para a largura e altura necessárias em pixels para a janela **LogonUI**.

   Ao definir manualmente o tamanho da janela **LogonUI**, o dimensionamento automático é desativado.

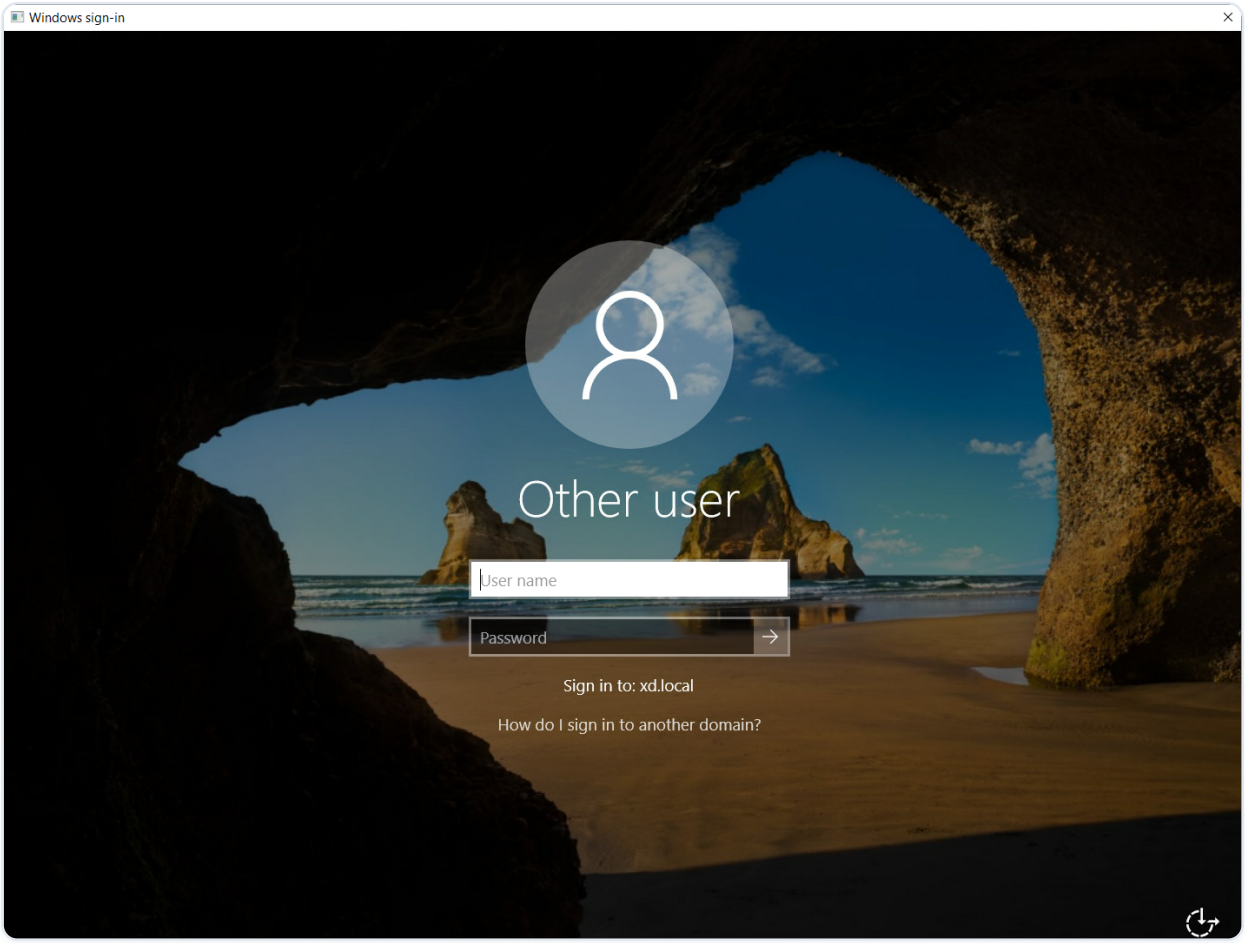
> **Observação:**
>
> Esses caminhos de registro foram alterados a partir da versão 2407 e posteriores. Os valores de registro antigos são ignorados e preteridos.

> Por padrão, a janela **LogonUI** inclui uma barra de título com um botão de fechar que permite ao usuário final desconectar-se da sessão, se necessário.

Desativar uma barra de título

Você pode desativar a barra de título na janela **LogonUI** com a seguinte chave de registro:

1. Abra o Editor do Registro usando `regedit` no comando **Executar**.
2. Vá para `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\SeamlessHook\`.
3. Crie novas chaves DWORD: **LogonUICaption** e defina o valor da chave como `0`.



Gerenciar pastas de aplicativos

Por padrão, os novos aplicativos que você adiciona aos grupos de entrega são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente ao criar o grupo de entrega, ao adicionar um aplicativo ou posteriormente.

É bom saber:

- Você não pode renomear ou excluir a pasta Aplicativos, mas pode mover todos os aplicativos que ela contém para outras pastas que você criar.
- Um nome de pasta pode conter de 1 a 64 caracteres. Espaços são permitidos.

- As pastas podem ser aninhadas em até cinco níveis.
- As pastas não precisam conter aplicativos. Pastas vazias são permitidas.
- As pastas são listadas em ordem alfabética no Web Studio, a menos que você as mova ou especifique um local diferente ao criá-las.
- Você pode ter mais de uma pasta com o mesmo nome, desde que cada uma tenha uma pasta pai diferente. Da mesma forma, você pode ter mais de um aplicativo com o mesmo nome, desde que cada um esteja em uma pasta diferente.
- Você deve ter a permissão `View Applications` para ver os aplicativos nas pastas, e deve ter a permissão `Edit Application Properties` para todos os aplicativos na pasta para remover, renomear ou excluir uma pasta que contém aplicativos.
- A maioria dos procedimentos a seguir solicita ações usando a barra de ações no Web Studio. Alternativamente, você pode usar menus de clique com o botão direito ou arrastar o item. Por exemplo, se você criar ou mover uma pasta para um local que não pretendia, pode arrastá-la/soltá-la para o local correto.

Para gerenciar pastas de aplicativos, selecione **Aplicativos** no painel esquerdo. Use a lista a seguir como guia.

- **Para visualizar todas as pastas (excluindo pastas aninhadas):** Clique em **Mostrar tudo** acima da lista de pastas.
- **Para criar uma pasta no nível mais alto (não aninhada):** Selecione a pasta **Aplicativos**. Para colocar a nova pasta sob uma pasta existente que não seja **Aplicativos**, selecione essa pasta. Em seguida, selecione **Criar Pasta** na barra de ações. Digite um nome.
- **Para mover uma pasta:** Selecione a pasta e, em seguida, selecione **Mover Pasta** na barra de ações. Você pode mover apenas uma pasta por vez, a menos que a pasta contenha pastas aninhadas. (A maneira mais fácil de mover uma pasta é arrastá-la.)
- **Para renomear uma pasta:** Selecione a pasta e, em seguida, selecione **Renomear Pasta** na barra de ações. Digite um nome.
- **Para excluir uma pasta:** Selecione a pasta e, em seguida, selecione **Excluir Pasta** na barra de ações. Ao excluir uma pasta que contém aplicativos e outras pastas, esses objetos também são excluídos. A exclusão de um aplicativo remove a atribuição do aplicativo do grupo de entrega. Isso não o remove da máquina.
- **Para mover aplicativos para uma pasta:** Selecione um ou mais aplicativos. Em seguida, selecione **Mover Aplicativo** na barra de ações. Selecione a pasta.

Você também pode colocar os aplicativos que está adicionando em uma pasta na página **Aplicativo** ao criar um grupo de entrega ou um grupo de aplicativos. Por padrão, os aplicativos adicionados vão para a pasta **Aplicativos**. Clique em **Alterar** para selecionar ou criar uma pasta.

Controlar o lançamento local de aplicativos em desktops publicados

Quando os usuários iniciam um aplicativo publicado de dentro de um desktop publicado, você pode controlar se o aplicativo é iniciado nessa sessão de desktop ou como um aplicativo publicado. O aplicativo Citrix Workspace procura o caminho de instalação do aplicativo no registro do Windows no VDA e, se presente, inicia a instância local do aplicativo. Caso contrário, uma instância hospedada do aplicativo é iniciada. Se você iniciar um aplicativo que não está instalado no VDA, o aplicativo hospedado será iniciado. Para obter mais informações, consulte início vPrefer.

No PowerShell (usando o SDK do PowerShell Remoto em implantações do Citrix Cloud ou o SDK do PowerShell em implantações locais), você pode alterar essa ação.

No cmdlet `New-Broker` Application ou `Set-BrokerApplication`, use a opção `LocalLaunchDisabled`. Por exemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Por padrão, o valor desta opção é falso (`-LocalLaunchDisabled $false`). Ao iniciar um aplicativo publicado de dentro de um desktop publicado, o aplicativo é iniciado nessa sessão de desktop.

Se você definir o valor da opção como verdadeiro (`-LocalLaunchDisabled $true`), o aplicativo publicado será iniciado. Isso cria uma sessão separada e adicional do desktop publicado (usando o aplicativo Citrix Workspace para Windows) para o aplicativo publicado.

Requisitos e limites:

- O valor `ApplicationType` do aplicativo deve ser `HostedOnDesktop`.
- Esta opção está disponível apenas através do SDK do PowerShell apropriado. Atualmente, não está disponível na interface gráfica do Web Studio.
- Esta opção requer no mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 e Delivery Controller 7.17.

Pacotes de aplicativos

Observação:

- Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente em Citrix Virtual Apps and Desktops 7 2212 ou anterior.
- Não recomendamos usar o Web Studio e o Citrix Studio de forma intercambiável para implantar e entregar pacotes de aplicativos. Cada um usa mecanismos diferentes, o que pode levar a discrepâncias, como informações do servidor App-V aparecendo corretamente em um, mas não no outro.

A Microsoft oferece três tecnologias de empacotamento para entregar aplicativos aos usuários: App-V, MSIX e MSIX app attach. Este artigo o guiará sobre como implantar e entregar esses aplicativos empacotados usando **Web Studio > App Packages**:

- Implantar e entregar aplicativos App-V
- Implantar e entregar aplicativos MSIX e MSIX app attach

Implantar e entregar aplicativos App-V

Esta seção aborda as seguintes informações:

- Visão geral. Descreve os métodos de gerenciamento para entregar e gerenciar os pacotes App-V.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

Esta seção descreve os métodos de gerenciamento para entregar e gerenciar os pacotes App-V. Para obter mais informações sobre os componentes e conceitos com os quais você interage ao entregar aplicativos empacotados App-V, consulte a documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/application-management/app-v/appv-for-windows>`.

Você pode usar os seguintes métodos para entregar e gerenciar pacotes App-V:

- **Administração Dupla**. Os pacotes de aplicativos são configurados e gerenciados em servidores App-V. O Citrix Virtual Apps and Desktops e os servidores App-V trabalham juntos para entregar e gerenciar pacotes.

Este método exige que o Citrix Virtual Apps and Desktops atualize periodicamente a visualização instantânea do estado do servidor App-V. Isso acarreta custos de hardware, infraestrutura e administração. O Citrix Virtual Apps and Desktops e os servidores App-V devem permanecer sincronizados, particularmente para permissões de usuário.

A Administração Dupla funciona melhor em implantações onde o App-V e seu ambiente estão intimamente acoplados:

- **Servidor de gerenciamento App-V**. Publica e gerencia o ciclo de vida dos pacotes App-V e dos Arquivos de Configuração Dinâmica.
- **Componente de Personalização Citrix** instalado em máquinas VDA. Gerencia o registro do servidor de publicação App-V apropriado necessário para o lançamento de aplicativos.

Este 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 atualização no logon e grupos de conexão.

- **Administrador Único**. Os pacotes de aplicativos são armazenados em compartilhamentos de rede. O Citrix Virtual Apps and Desktops entrega e gerencia pacotes de forma independente.

  Este método reduz a sobrecarga porque os servidores App-V e a infraestrutura de banco de dados não são necessários na implantação.

  Neste método, você armazena pacotes App-V em um compartilhamento de rede e carrega seus metadados desse local para o seu ambiente. O componente de Personalização Citrix instalado nas máquinas VDA então gerencia e entrega aplicativos da seguinte forma:

  - Processar os Arquivos de Configuração de Implantação e os Arquivos de Configuração do Usuário quando um aplicativo é iniciado.
  - Gerenciar todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Você pode usar ambos os métodos de gerenciamento simultaneamente. Em outras palavras, ao adicionar aplicativos a grupos de entrega, os aplicativos podem vir de pacotes App-V presentes em servidores App-V ou em compartilhamentos de rede.

> **Observação:**
>
> Se você estiver usando ambos os métodos de gerenciamento simultaneamente e o pacote App-V tiver um Arquivo de Configuração Dinâmica em ambos os locais, o arquivo no servidor App-V (Administrador Duplo) será usado.

Procedimentos

Para oferecer suporte à entrega de aplicativos App-V, você deve instalar o componente de Personalização Citrix nas máquinas VDA. Consulte Instalar o componente de Personalização Citrix nas máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados App-V aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.
4. Para habilitar a entrega automática de pacotes App-V interdependentes, crie grupos de isolamento.

Para que o Citrix Virtual Apps and Desktops reconheça e aplique Arquivos de Configuração Dinâmica App-V no método de Administrador Único, consulte este blog da Citrix.

Implantar e entregar aplicativos MSIX e MSIX app attach

Esta seção aborda as seguintes informações:

- Visão geral. Descreve como os pacotes MSIX e MSIX app attach são entregues e gerenciados.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

O Citrix Virtual Apps and Desktops entrega aplicativos MSIX e MSIX app attach aos usuários por meio do componente de Personalização Citrix instalado nas máquinas VDA. Este componente gerencia todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Para obter mais informações sobre MSIX e MSIX app attach, consulte a documentação da Microsoft: `<https://docs.microsoft.com/pt-br/windows/msix/>` e `<https://docs.microsoft.com/pt-br/azure/virtual-desktop/what-is-app-attach>`, respectivamente.

Procedimentos

Para oferecer suporte à entrega de pacotes MSIX e MSIX app attach, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization nas máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados MSIX e MSIX app attach aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.

Instalar o componente Citrix Personalization nas máquinas VDA

O componente Citrix Personalization gerencia o processo de publicação de pacotes de aplicativos nos formatos App-V, MSIX e MSIX app attach. 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 maneiras:

- No assistente de instalação, vá para a página **Additional Components** e selecione a caixa de seleção **Citrix Personalization for App-V - VDA**.
- Na interface de linha de comando, use a opção **/includeadditional "Citrix Personalization for App-V – VDA"**.

Para instalar o componente após a instalação do VDA, siga estas etapas:

1. Na máquina VDA, vá para **Painel de Controle > Programas > Programas e Recursos**, clique com o botão direito em **Citrix Virtual Delivery Agent** e selecione **Alterar**.
2. No assistente que aparece, prossiga para a página **Additional Components** e, em seguida, habilite a caixa de seleção **Citrix Personalization for App-V - VDA**.

> **Observação:**
>
> O Microsoft App-V Desktop Client é o componente que executa aplicativos virtuais de pacotes App-V em dispositivos de usuário. O Windows 10 (1607 ou posterior) e o Windows Server 2019 já incluem este 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/pt-br/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 **App-V Single Admin**: Armazene os pacotes e os arquivos de configuração dinâmica correspondentes (App-V) em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
    - Para **App-V Dual Admin**: Publique os pacotes no servidor de gerenciamento App-V a partir de um caminho UNC. (A publicação a partir de URLs HTTP não é suportada.)
    - Para **MSIX ou MSIX app attach**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
3. Certifique-se de que o VDA tenha permissão de leitura no caminho de armazenamento do pacote:
    - Se você armazenar pacotes em um compartilhamento de rede UNC ou SMB em seu domínio AD, conceda à máquina VDA permissão de leitura para o caminho de armazenamento. Para fazer isso, você pode dar à conta AD da máquina permissão de leitura para o compartilhamento explicitamente, ou incluir a conta em um grupo AD que tenha essa permissão.
    - Se você armazenar pacotes em um Azure File Share, primeiro conceda a uma conta de usuário permissão de leitura para o caminho de armazenamento no Azure. Em seguida, configure `ctxAppVService` em execução na máquina VDA para usar essa conta de usuário para acessar o caminho de armazenamento do pacote. Consulte a seção a seguir para obter etapas detalhadas.

Alterar a conta de logon do usuário

O VDA chama `ctxAppVService` para acessar os caminhos de armazenamento de pacotes. 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 AD. No entanto, não funciona nos cenários de integração AD e Azure AD, que exigem autenticação baseada em conta de usuário.

Se você armazenar pacotes em um Azure File Share, altere a conta de logon para `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 **Serviços**, clique com o botão direito em **ctxAppVService** e selecione **Propriedades**.
2. Na guia **Log on**, selecione **Esta conta**, insira uma conta de usuário que tenha permissão de leitura para o caminho de armazenamento do pacote e, em seguida, insira a senha do usuário duas vezes.
3. Clique em **OK**.

Carregar pacotes de aplicativos para o seu ambiente

Depois de armazenar os pacotes de aplicativos em um local de rede conforme necessário, carregue-os para o seu ambiente para entrega. Use um dos seguintes métodos conforme necessário:

- Carregar em massa
- Carregar um por um

Preparações

O Citrix Virtual Apps and Desktops usa uma máquina VDA para configurar a conexão com o local de rede para descoberta de pacotes. Portanto, crie um grupo de entrega com antecedência e certifique-se de que pelo menos um VDA no grupo atenda aos seguintes requisitos:

- Versão do VDA:
  - Para descobrir pacotes App-V: 2203 ou posterior
  - Para descobrir pacotes MSIX e MSIX app attach: 2209 ou posterior
- Componente Citrix Personalization for App-V: Instalado
- Permissão no local do pacote: Leitura (Consulte Etapa 2: Armazenar pacotes de aplicativos em compartilhamentos de rede para obter detalhes.)
- Energia: Ligado
- Estado: Registrado

Carregar pacotes de aplicativos em massa

Carregue pacotes em um local de rede para o seu ambiente. Certifique-se de ter os seguintes itens prontos antes do carregamento:

- Um grupo de entrega que atenda aos requisitos de Preparação

- O caminho do local de rede

Para carregar pacotes em massa, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **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 indicados em Preparation 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, conclua as configurações correspondentes:
   - Se você selecionar **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 **Compartilhamento de rede**, especifique as seguintes informações:
     - Insira o caminho UNC do compartilhamento de rede. Exemplo: `\\Package-Server\apps\`
     - Selecione os tipos de pacote que você deseja carregar. As opções incluem App-V, MSIX e MSIX app attach.
     - Especifique se deseja pesquisar subpastas por pacotes.
6. Clique em **Add Source**.

   A página Add Source é fechada e a origem recém-adicionada aparece na lista de origens. O Citrix Virtual Apps and Desktops carrega os pacotes para o seu ambiente usando um VDA no grupo de entrega. Após a conclusão do upload, o campo Status mostra *Import successful*. Os pacotes correspondentes aparecem na guia **Packages**.

   > **Observação:**

> Para verificar se há atualizações de pacote em um local de origem e importá-las para o seu ambiente, selecione o local na lista de origens e clique em **Check for Package Updates**.

Carregar pacotes de aplicativos um por um

Carregue um pacote de aplicativo de um compartilhamento de rede para seu ambiente. Antes do upload, certifique-se de ter os seguintes itens prontos:

- Um grupo de entrega que atende aos requisitos declarados em Preparação
- O caminho do local de rede.

Para carregar um pacote para seu ambiente, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Pacotes**, clique no botão **Adicionar pacote**. A página **Adicionar pacote** é exibida.
3. No campo **Grupo de entrega**, clique em **Selecionar um grupo de entrega**. Em seguida, selecione um grupo de entrega que atenda aos requisitos declarados em Preparação e clique em **OK**.
4. No campo **Caminho completo do pacote**, insira um caminho conforme necessário:
   - Para carregar vários pacotes de uma vez, insira seus caminhos completos, separados por ponto e vírgula (`;`). Exemplo: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Para carregar todos os pacotes presentes em um compartilhamento de rede, insira o caminho de armazenamento. Exemplo: `\\package-Server\apps\`
5. Clique em **Adicionar Pacote**.

   O pacote de aplicativos aparece na guia **Pacotes**.

Adicionar aplicativos a grupos de entrega

Depois que um pacote de aplicativos é totalmente carregado, 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.

Para adicionar um ou mais aplicativos em um pacote a vários grupos de entrega, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.

2. Na guia **Pacotes**, selecione um pacote conforme necessário.
3. Na barra de ações, clique em **Adicionar Grupos de Entrega**. A página Adicionar Grupos de Entrega é exibida.
4. Selecione um ou mais aplicativos no pacote conforme necessário e clique em **Avançar**.
5. Na lista de grupos de entrega, selecione os grupos aos quais você deseja atribuir os aplicativos e clique em **Avançar**. **Nota:** Se você selecionou um pacote MSIX ou MSIX app attach, apenas os grupos de entrega cujo nível funcional é 2106 ou posterior são mostrados na lista.
6. Clique em **Concluir**.

Você também pode adicionar aplicativos empacotados a um grupo de entrega quando:

- Criar um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.
- Editar grupos de entrega ou grupos de aplicativos existentes. Para obter mais informações, consulte Adicionar aplicativos.

(Opcional) Criar grupos de isolamento para pacotes App-V

Você pode criar grupos de isolamento para permitir a entrega automática de pacotes App-V interdependentes.

> **Observação:**
>
> Grupos de isolamento são suportados para o método App-V Single Admin. Se você estiver usando o método App-V Dual Admin, poderá atingir o mesmo objetivo criando *grupos de conexão* na infraestrutura do Microsoft App-V. Para obter mais informações, consulte este artigo da documentação da Microsoft: `<https://docs.microsoft.com/pt-br/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 idênticos, aos grupos de conexão do App-V. Um grupo de isolamento inclui dois tipos de pacotes:

- Pacotes de aplicativos **explícitos**. Aplicativos com requisitos de licenciamento específicos. Você pode restringir esses aplicativos a um intervalo específico de usuários adicionando-os a grupos de entrega.
- Pacotes de aplicativos **automáticos**. Aplicativos que estão sempre disponíveis para todos os usuários, independentemente de serem adicionados a grupos de entrega.

Por exemplo, o aplicativo `app-a` requer JRE 1.7 para ser executado. Você pode criar um grupo de isolamento que contenha app-a (marcado como *Explícito*) e JRE 1.7 (marcado como *Automático*). Em seguida, adicione o pacote App-V para `app-a` a um ou mais grupos de entrega. Quando um usuário inicia o app-a, o JRE 1.7 é implantado automaticamente com ele.

Quando um usuário inicia um aplicativo App-V marcado como *Explícito* em um grupo de isolamento, o Citrix Virtual Apps and Desktops verifica a permissão de acesso do usuário ao aplicativo nos grupos de entrega. Se o usuário tiver permissão para acessar o aplicativo, quaisquer pacotes de aplicativos *Automáticos* no mesmo grupo de isolamento serão disponibilizados ao usuário.

Você não precisa adicionar os pacotes *Automáticos* a nenhum grupo de entrega. Se houver outro pacote de aplicativo *Explícito* no grupo de isolamento, esse pacote será disponibilizado ao usuário somente se estiver no mesmo grupo de entrega.

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 **Grupos de Isolamento**, clique em **Adicionar Grupo de Isolamento**.
2. Insira um nome e uma descrição para o grupo de isolamento. Todos os pacotes de aplicativos em seu ambiente aparecem na lista **Pacotes Disponíveis**.
3. Na lista **Pacotes Disponíveis**, selecione um aplicativo conforme necessário e clique na seta para a direita. O aplicativo selecionado aparece na lista **Pacotes no Grupo de Isolamento**.
4. No campo **Implantação**, selecione **Explícito** ou **Automático** para o aplicativo.
5. Repita os passos 2–3 para adicionar mais pacotes.
6. Para ajustar a ordem dos pacotes na lista, clique na seta para cima ou para baixo.
7. Clique em **Salvar**.

> **Observação:**

> As configurações do Grupo de Isolamento resultam na criação de Grupos de Conexão App-V no VDA. Os cenários de implantação podem se tornar complexos e o cliente App-V suporta pacotes que estão em apenas um Grupo de Conexão ativo por vez. Recomendamos que você evite adicionar o mesmo pacote a dois grupos de isolamento diferentes que são adicionados ao mesmo grupo de entrega.

Publicar aplicativos empacotados em VDAs de sessão única ou de desktop compartilhado

Agora você pode entregar pacotes App-V, MSIX e MSIX app attach para suas sessões VDA de sessão única ou de desktop compartilhado diretamente por meio de grupos de entrega. Você pode acessar os aplicativos empacotados em seu VDA de desktop no momento do login, com base nas permissões de acessibilidade definidas nos aplicativos.

Benefícios

- Aplicativos disponíveis no VDA no momento do login e não preparados sob demanda via Workspace ou StoreFront.
- Tempo de inicialização aprimorado ao acessar os aplicativos empacotados.
- Facilita a manutenção dos aplicativos empacotados de forma independente, separadamente da imagem base do VDA.

Considerações

- Esta opção está disponível para VDAs de sessão única apenas através do SDK do PowerShell apropriado. Atualmente, não está disponível no fluxo de trabalho do Web Studio. A publicação em desktops compartilhados pode ser feita com o SDK do PowerShell ou da maneira existente através do fluxo de trabalho do Web Studio. Para obter mais informações sobre o procedimento existente, consulte Adicionar aplicativos a grupos de entrega.
- Os aplicativos devem fazer parte de um grupo de entrega.

Antes de começar

- Certifique-se de que os aplicativos empacotados estejam assinados e disponíveis no compartilhamento de arquivos ou local UNC. Para obter mais informações, consulte Armazenar pacotes de aplicativos em compartilhamentos de rede.
- Instale o componente Citrix Personalization nas máquinas VDA.

Procedimento

Para entregar aplicativos empacotados a VDAs de desktop, siga estas etapas:

1. Importar pacotes de aplicativos para o Web Studio.
2. Publicar o BrokerApplication empacotado.
3. Limitar a visibilidade de aplicativos no Web Studio.

Importar pacotes de aplicativos para o Web Studio

1. Abra um navegador da web. Digite `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Crie um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.
3. Importe os pacotes de aplicativos para o Web Studio. Para obter mais informações, consulte Carregar pacotes de aplicativos em massa.

Publicar o aplicativo empacotado no BrokerApplication

Se você estiver publicando em um VDA multi-sessão (compartilhado) ou em um VDA de aplicativo de sessão única, o procedimento de publicação permanece inalterado. Para obter mais informações, consulte Adicionar aplicativos a grupos de entrega. Se você estiver publicando em um VDA de desktop de sessão única, faça o seguinte:

No Delivery Controller™, execute os seguintes comandos PowerShell:

1. Para recuperar os comandos presentes no pacote:

   `Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"`

   > **Observação:**
   >
   > A versão do `App-V package discovery module` que oferece suporte a essa funcionalidade pode ser encontrada no ISO do Citrix Virtual Apps and Desktops (versões 2311 ou superiores) no caminho acima.

2. Para recuperar os IDs de grupo de entrega e os IDs de aplicativos empacotados relevantes:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. Para publicar os pacotes e criar as BrokerMachineConfigurations apropriadas:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid
   <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Para sincronizar as configurações do Broker, que são posteriormente enviadas para o agente Broker no VDA:

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>
   ```

   > **Observação:**
   >
   > Certifique-se de executar o comando PowerShell `Update-DesktopGroupMachineConfigurations` depois de publicar ou remover aplicativos empacotados de um VDA.

Limitar a visibilidade de aplicativos no Web Studio

Por padrão, os usuários têm todos os aplicativos empacotados atribuídos ao grupo de entrega que atende ao seu VDA disponíveis em sua sessão de desktop. Você pode controlar a visibilidade de aplicativos empacotados nos VDAs de desktop definindo a visibilidade dos aplicativos para usuários ou grupos específicos no Web Studio. Para gerenciar a visibilidade de aplicativos empacotados, consulte Alterar Propriedades do Aplicativo.

Aplicativos da Plataforma Universal do Windows

Para obter informações sobre aplicativos da Plataforma Universal do Windows (UWP), consulte a seguinte documentação da Microsoft:

- O que é um aplicativo da Plataforma Universal do Windows (UWP)?
- Gerenciador de Pacotes do Windows

Requisitos e limitações

O Citrix Virtual Apps and Desktops™ oferece suporte ao uso de aplicativos UWP com VDAs nas seguintes máquinas Windows:

- Windows 10 e versões posteriores
- Windows Server 2016 e versões posteriores

Os VDAs devem ser no mínimo da versão 7.11.

Os seguintes recursos do Citrix Virtual Apps and Desktops não são suportados ou são limitados ao usar aplicativos UWP:

- A associação de tipo de arquivo não é suportada.
- O Acesso a Aplicativos Locais não é suportado.
- Visualização dinâmica: Se os aplicativos em execução na sessão se sobrepuserem, a visualização mostrará o ícone padrão. As APIs Win32 usadas para Visualização Dinâmica não são suportadas em aplicativos UWP.
- Remoting do Centro de Ações: Aplicativos UWP podem usar o Centro de Ações para exibir as mensagens na sessão. Essas mensagens atualmente não são redirecionadas para o endpoint para serem exibidas ao usuário.

O lançamento de aplicativos UWP e aplicativos não-UWP do mesmo servidor não é suportado. Em vez disso, coloque aplicativos UWP e aplicativos não-UWP em grupos de entrega ou grupos de aplicativos separados.

Como todos os aplicativos UWP instalados na máquina são enumerados, a Citrix® recomenda desabilitar o acesso do usuário à Windows Store. Isso impede que os aplicativos UWP instalados por um usuário sejam acessados por um usuário diferente.

Durante o sideload, o aplicativo UWP é instalado na máquina e fica disponível para uso por outros usuários. Quando outro usuário inicia o aplicativo, ele é instalado e o sistema operacional atualiza seu banco de dados AppX para indicar "como instalado" por esse usuário.

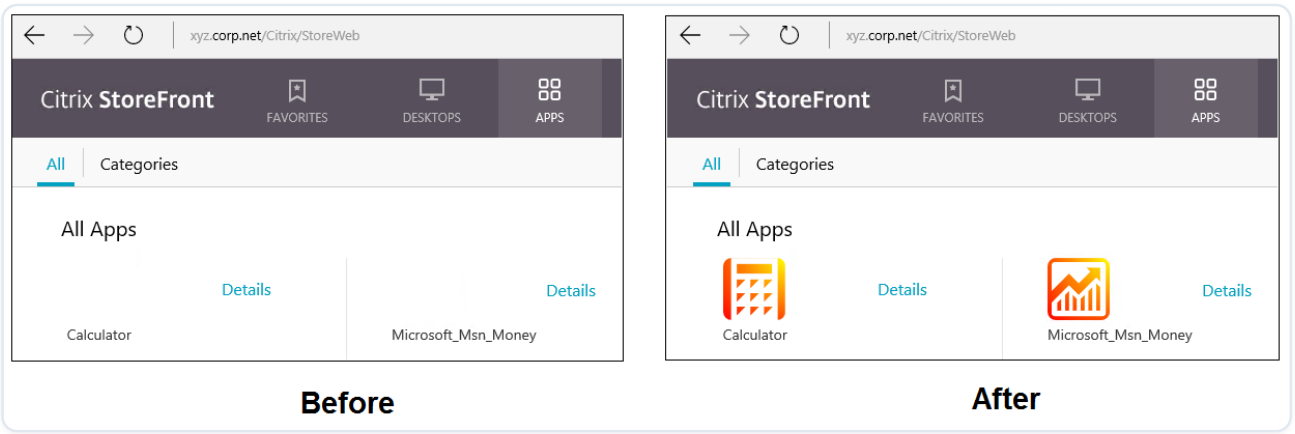
Um logoff normal iniciado a partir de um aplicativo UWP publicado que foi lançado em uma janela fixa ou contínua pode impedir que a sessão VDA seja encerrada e forçar o logoff do usuário. Quando isso ocorre, vários processos que permanecem na sessão VDA impedem que ela seja encerrada corretamente. Para resolver isso, determine qual processo está impedindo o encerramento da sessão VDA e, em seguida, adicione-o ao valor da chave de registro "LogoffCheckSysModules", seguindo as orientações em CTX891671.

Os nomes de exibição e descrições de aplicativos para aplicativos UWP podem não ter os nomes corretos. Edite e corrija essas propriedades ao adicionar os aplicativos ao grupo de entrega.

Verifique Problemas conhecidos para quaisquer problemas adicionais.

Atualmente, vários aplicativos UWP têm ícones brancos com transparência ativada, o que faz com que o ícone não seja visível contra o fundo branco da exibição do StoreFront. Para evitar esse problema, você pode alterar o plano de fundo. Por exemplo, na máquina StoreFront, edite o arquivo `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. No final do arquivo,

adicione `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`. O gráfico a seguir ilustra o antes e o depois para este exemplo.



No Windows Server 2016 e versões posteriores, o Gerenciador do Servidor também pode ser iniciado quando um aplicativo UWP é iniciado. Para evitar que isso ocorra, você pode desabilitar o início automático do Gerenciador do Servidor durante o logon com a chave de registro `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Para obter detalhes, consulte `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`.

Instalar e publicar aplicativos UWP

O suporte para aplicativos UWP é habilitado por padrão.

Para instalar um ou mais aplicativos UWP em VDAs (ou uma imagem mestre), use um dos seguintes métodos:

- Conclua uma instalação offline da Windows Store for Business, usando uma ferramenta como Deployment Image Servicing and Management (DISM) para implantar os aplicativos na imagem da área de trabalho. Para obter mais informações, consulte Windows Package Manager.
- Faça o sideload dos aplicativos. Para obter mais informações, consulte Sideload line of business (LOB) apps in Windows client devices.
- Instale os aplicativos UWP para cada usuário pretendido diretamente da Windows Store for Business.

Para adicionar (publicar) um ou mais aplicativos UWP no Citrix Virtual Apps ou Citrix Virtual Desktops™:

1. Depois que os aplicativos UWP forem instalados na máquina, adicione os aplicativos UWP a um grupo de entrega ou grupo de aplicativos. Você pode fazer isso ao criar um grupo ou mais tarde. Na página **Aplicativos**, no menu **Adicionar**, selecione **Do menu Iniciar**.

2. Quando a lista de aplicativos aparecer, selecione os aplicativos UWP que deseja publicar.
3. Continue com o assistente ou feche a caixa de diálogo de edição.

Para desabilitar o uso de Aplicativos Universais em um VDA, adicione a configuração de registro **EnableUWASeamlessSupport** em `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` e defina como **0**.

Desinstalar aplicativos UWP

Quando você desinstala um aplicativo UWP com um comando como `Remove-AppXPackage`, o item é desinstalado apenas para administradores. Para remover o aplicativo das máquinas dos usuários que podem ter iniciado e usado o aplicativo, execute o comando de remoção em cada máquina. Você não pode desinstalar o pacote AppX das máquinas de todos os usuários com um único comando.

Autoscale™

> **Observação:**

> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este recurso está disponível apenas no Web Studio.

> O Autoscale é um recurso que fornece uma solução consistente e de alto desempenho para gerenciar proativamente a energia de suas máquinas. Ele visa equilibrar custos e experiência do usuário.

O Autoscale permite o gerenciamento proativo de energia de todas as máquinas OS de sessão única e multissessão registradas em um grupo de entrega.

Os recursos do Autoscale incluem:

- Configurações baseadas em agendamento e em carga
- Tempos limite de sessão dinâmicos
- Máquinas marcadas pelo Autoscale (burst de nuvem)
- Notificações de logoff do usuário

Plataformas de hospedagem de VDA suportadas

O Autoscale oferece suporte a todas as plataformas que o Citrix Virtual Apps and Desktops oferece suporte. Isso inclui várias plataformas de infraestrutura, como XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e muitas outras. Para obter uma lista completa das plataformas compatíveis, consulte Requisitos do sistema para Citrix Virtual Apps and Desktops.

> **Observação:**
>
> Ao adicionar conexões de host de nuvem pública à sua implantação, você precisa da Licença de Direitos Híbridos. Para obter informações sobre a Licença de Direitos Híbridos, consulte Transição e Troca (TTU) com Direitos Híbridos. Para obter informações sobre como adicionar uma licença, consulte Criar um site.

Cargas de trabalho suportadas

O Autoscale suporta grupos de entrega de SO multi-sessão e SO de sessão única. Existem três interfaces de usuário a serem consideradas:

- Interface de usuário do Autoscale para grupos de entrega de SO multi-sessão (anteriormente grupos de entrega RDS)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única aleatórios (agrupados) (anteriormente grupos de entrega VDI agrupados)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única estáticos (anteriormente grupos de entrega VDI estáticos)

Para obter mais informações sobre as interfaces de usuário para diferentes grupos de entrega, consulte Interfaces de usuário do Autoscale.

Benefícios

O recurso Autoscale oferece os seguintes benefícios:

- Fornecer um mecanismo único e consistente para gerenciar o consumo de energia das máquinas em um grupo de entrega.
- Garantir a disponibilidade e controlar os custos, ligando as máquinas com gerenciamento de energia baseado em carga ou baseado em agendamento, ou uma combinação de ambos.

- Para monitorar métricas como economia de custos e utilização da capacidade, e para habilitar notificações, use Director.

Assista a um vídeo de 2 minutos

O vídeo a seguir oferece um tour rápido pelo Autoscale.

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Introdução ao Autoscale™

O Autoscale funciona no nível do grupo de entrega. Ele gerencia proativamente a energia das máquinas em um grupo de entrega com base nos agendamentos que você define.

Autoscale aplica-se a todos os tipos de grupos de entrega:

- SO estático de sessão única
- SO aleatório de sessão única
- SO aleatório de múltiplas sessões

Este artigo descreve conceitos básicos relacionados ao Autoscale e fornece orientação sobre como habilitar e configurar o Autoscale para um grupo de entrega.

Conceitos básicos

Antes de começar, saiba mais sobre os seguintes conceitos básicos no Autoscale:

- Agendamentos
- Buffer de capacidade
- Índice de carga

Agendamentos

O Autoscale liga e desliga máquinas em um grupo de entrega com base em um agendamento que você define.

Um agendamento inclui o número de máquinas ativas para cada slot de tempo, com horários de pico e fora de pico definidos.

As configurações de agendamento variam com o tipo de grupo de entrega. Para mais informações, consulte:

- Grupos de entrega de SO multi-sessão
- Grupos de entrega aleatórios de SO de sessão única
- Grupos de entrega estáticos de SO de sessão única

Buffer de capacidade

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem observados:

- Para grupos de entrega de SO de várias sessões, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga.
- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem do número total de máquinas no grupo de entrega.

Índice de carga

> **IMPORTANTE:**

> O índice de carga aplica-se apenas a grupos de entrega de várias sessões.

> A métrica do índice de carga determina a probabilidade de uma máquina receber solicitações de logon de usuário. Ela é calculada usando as configurações da **política de Gerenciamento de Carga do Citrix** configuradas para logon simultâneo, sessão, CPU, disco e uso de memória.

O índice de carga varia de 0 a 10.000. Por padrão, uma máquina é considerada em carga total quando hospeda 250 sessões:

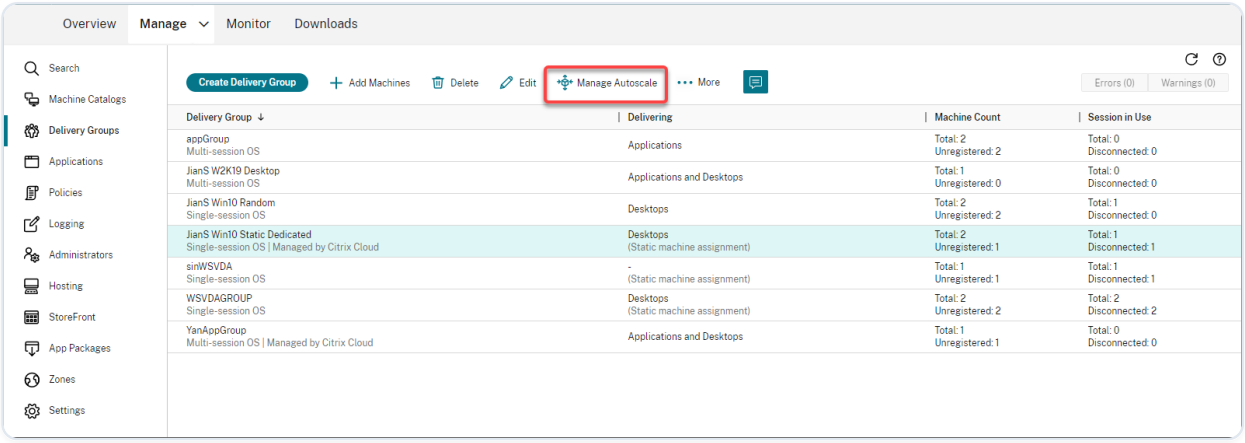
- O dígito "0" indica uma máquina descarregada. Uma máquina com um valor de índice de carga de 0 está em uma carga de linha de base.
- O dígito "10.000" indica uma máquina totalmente carregada que não pode executar mais sessões.

Habilitar o Autoscale para um grupo de entrega

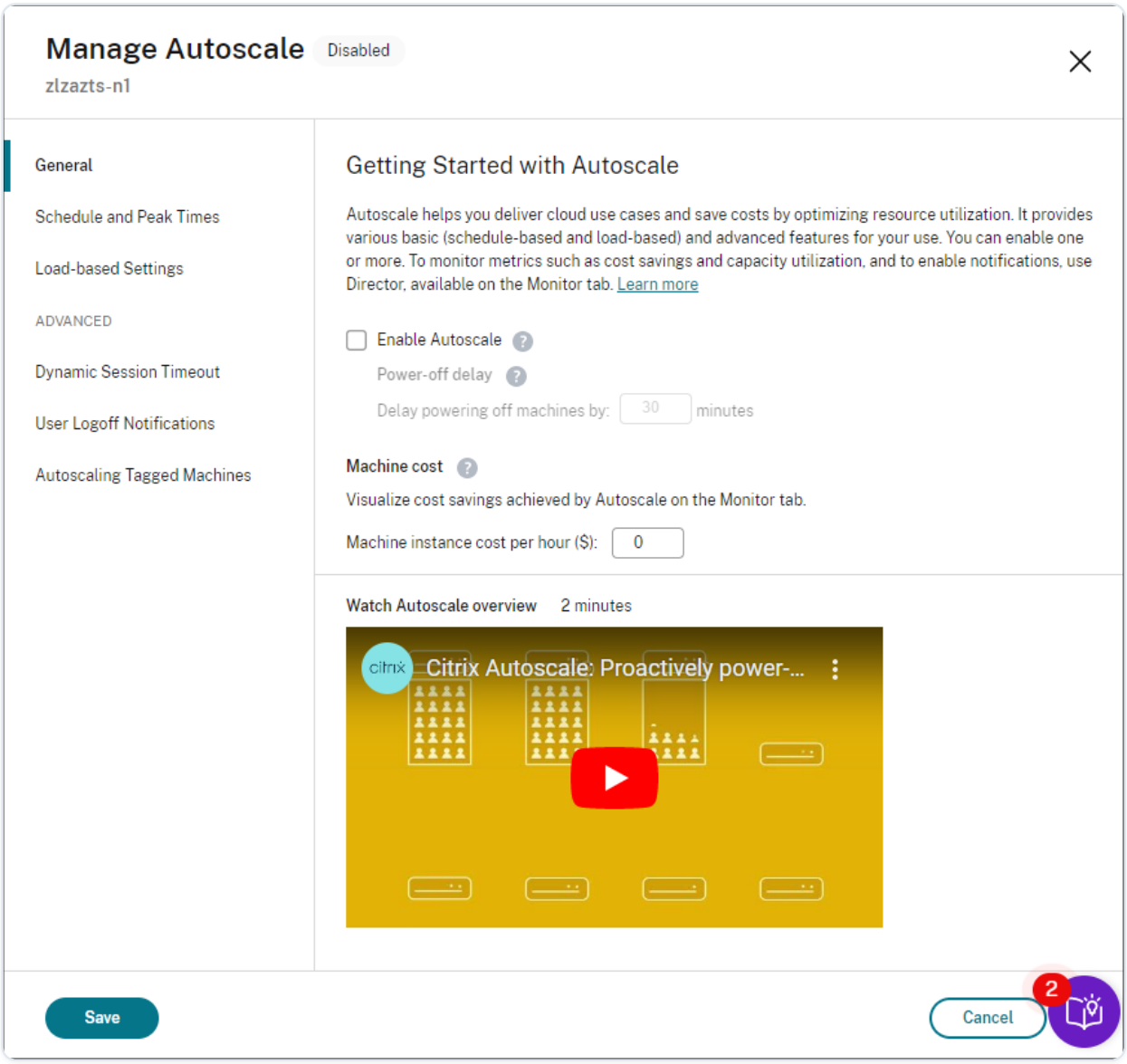
O Autoscale é desabilitado por padrão ao criar um grupo de entrega. Para habilitar e configurar o Autoscale para um grupo de entrega usando o Web Studio, siga estas etapas:

Você também pode usar comandos do PowerShell para habilitar e configurar o Autoscale para um grupo de entrega. Para obter mais informações, consulte comandos do SDK do PowerShell do Broker.

1. Selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo de entrega que você deseja gerenciar e clique em **Gerenciar Autoscale**.



3. Na página **Gerenciar Autoscale**, selecione a caixa de seleção **Habilitar Autoscale** para habilitar o Autoscale. Depois de habilitar o Autoscale, as opções na página são habilitadas.



4. Para alterar as configurações padrão com base nas necessidades da sua organização, conclua as seguintes configurações:

   - Configurar agendamentos
   - Para desligar máquinas inativas de forma mais eficiente, use Tempos limite de sessão dinâmicos e Notificações de logoff do usuário
   - Para gerenciar o consumo de energia de um subconjunto de máquinas no grupo de entrega, use Máquinas marcadas com dimensionamento automático

Para desabilitar o Autoscale, desmarque a caixa de seleção **Autoscale**. As opções na página ficam cinzas para indicar que o Autoscale está desabilitado para o grupo de entrega selecionado.

> **Importante:**

- Se você desabilitar o Autoscale, todas as máquinas gerenciadas pelo Autoscale permanecem em seus estados no momento da desabilitação.
- Depois de desabilitar o Autoscale, as máquinas em estado de drenagem são retiradas do estado de drenagem. Para obter mais informações sobre o estado de drenagem, consulte Estado de drenagem.

Monitorar métricas

Depois de habilitar o Autoscale para um grupo de entrega, você pode monitorar as seguintes métricas de máquinas gerenciadas pelo Autoscale a partir do Director.

- Uso da máquina
- Economias estimadas
- Notificações de alerta para máquinas e sessões
- Status da máquina
- Tendências de avaliação de carga

Observação:

Quando você habilita o Autoscale inicialmente para um grupo de entrega, pode levar alguns minutos para exibir os dados de monitoramento desse grupo de entrega. Os dados de monitoramento permanecem disponíveis se o Autoscale for habilitado e depois desabilitado para o grupo de entrega. O Autoscale coleta dados de monitoramento em intervalos de 5 minutos.

Para obter mais informações sobre as métricas, consulte Monitorar máquinas gerenciadas pelo Autoscale.

É bom saber

O Autoscale funciona no nível do grupo de entrega. Ele é configurado por grupo de entrega. Ele gerencia a energia apenas das máquinas no grupo de entrega selecionado.

Capacidade e registro de máquinas

O Autoscale inclui apenas máquinas que estão registradas no site ao determinar a capacidade. Máquinas ligadas que não estão registradas não podem aceitar solicitações de sessão. Como resultado, elas não são incluídas na capacidade geral do grupo de entrega.

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 máquinas aleatoriamente de cada catálogo para atender aos requisitos de agendamento ou demanda de sessão.

Por exemplo, um grupo de entrega tem dois catálogos de máquinas: o Catálogo A tem três máquinas ligadas e o Catálogo B tem uma máquina ligada. Se o Autoscale precisar ligar uma máquina extra, ele poderá ligar uma máquina do Catálogo A ou do Catálogo B.

Provisionamento de máquinas e demanda de sessão

O catálogo de máquinas associado ao grupo de entrega deve ter máquinas suficientes para ligar e desligar conforme a demanda aumenta e diminui. Se a demanda de sessão exceder o número total de máquinas registradas no grupo de entrega, o Autoscale garante que todas as máquinas registradas sejam ligadas. No entanto, **o Autoscale não provisiona máquinas adicionais**.

Considerações sobre o tamanho da instância

Você pode otimizar seus custos se dimensionar adequadamente suas instâncias em nuvens públicas. Recomendamos que você provisione instâncias menores, desde que elas correspondam ao desempenho da sua carga de trabalho e aos requisitos de capacidade.

Instâncias menores hospedam menos sessões de usuário do que instâncias maiores. Portanto, o Autoscale coloca as máquinas em estado de drenagem muito mais rapidamente porque leva menos tempo para a última sessão de usuário ser desconectada. Como resultado, o Autoscale desliga instâncias menores mais cedo, reduzindo assim os custos.

Estado de drenagem

O Autoscale tenta reduzir o número de máquinas ligadas no grupo de entrega para o tamanho do pool configurado e o buffer de capacidade.

Para atingir esse objetivo, o Autoscale coloca as máquinas em excesso com o menor número de sessões em "estado de drenagem" e as desliga quando todas as sessões são encerradas. Esse comportamento ocorre quando a demanda por sessões diminui e o agendamento exige menos máquinas do que as que estão ligadas.

O Autoscale coloca máquinas em excesso em "estado de drenagem" uma a uma:

- Se duas ou mais máquinas tiverem o mesmo número de sessões ativas, o Autoscale drena a máquina que esteve ligada pelo atraso de desligamento especificado.

  Fazer isso evita colocar máquinas recém-ligadas em estado de drenagem, pois essas máquinas são mais propensas a ter o menor número de sessões.
- Se duas ou mais máquinas estiveram ligadas pelo atraso de desligamento especificado, o Autoscale drena essas máquinas uma a uma aleatoriamente.

Máquinas em estado de drenagem não hospedam mais novos inícios de sessão e estão aguardando que as sessões existentes sejam encerradas. Uma máquina se torna candidata a desligamento somente quando todas as sessões são encerradas. No entanto, se não houver máquinas imediatamente disponíveis para inícios de sessão, o Autoscale prefere direcionar os inícios de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina.

Uma máquina é retirada do estado de drenagem quando uma das seguintes condições é atendida:

- A máquina é desligada.
- O Autoscale está desabilitado para o grupo de entrega ao qual a máquina pertence.
- O Autoscale usa a máquina para atender aos requisitos de agendamento ou demanda de carga. Este caso ocorre quando o agendamento (escalonamento baseado em agendamento) ou a demanda atual (escalonamento baseado em carga) exige mais máquinas do que o número de máquinas atualmente ligadas.

> **Importante:**

> Se nenhuma máquina estiver imediatamente disponível para inicializações de sessão, o Autoscale prefere direcionar as inicializações de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina. Uma máquina em estado de drenagem que hospeda uma inicialização de sessão permanece em estado de drenagem.

> Para descobrir quais máquinas estão em estado de drenagem, use o comando PowerShell `Get-BrokerMachine`. Por exemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternativamente, você pode usar o console Gerenciar. Consulte Exibir máquinas em estado de drenagem.

EXIBIR MÁQUINAS EM ESTADO DE DRENAGEM

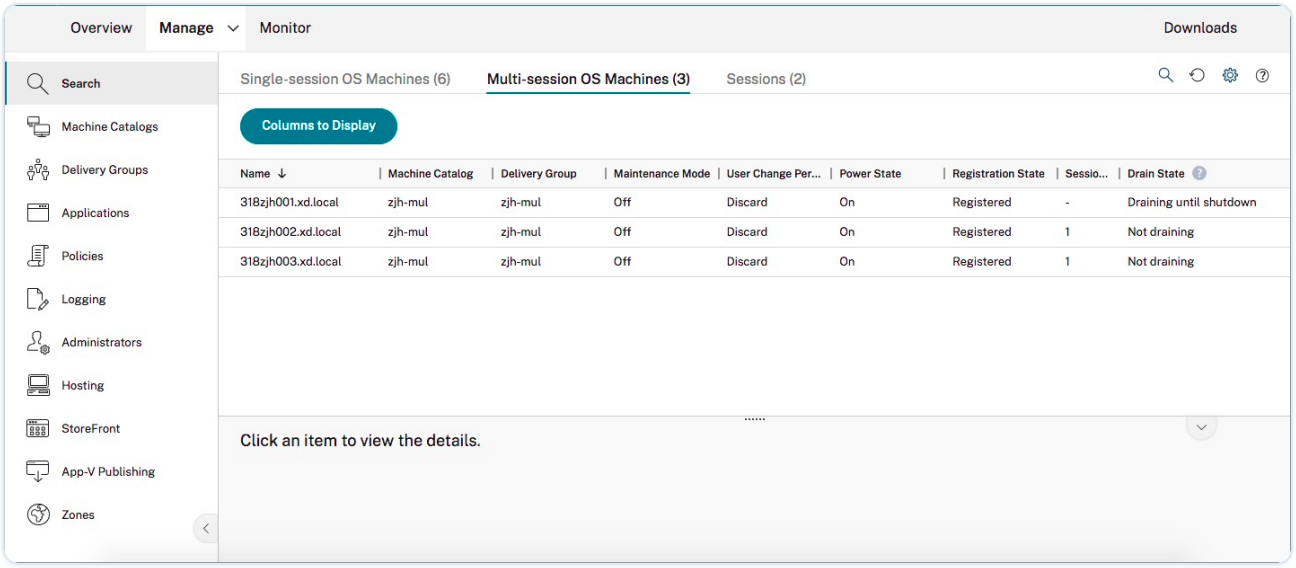
> **Observação:**
>
> Este recurso se aplica apenas a máquinas de várias sessões.

No Web Studio, você pode exibir máquinas que estão em estado de drenagem, informando quais máquinas estão prestes a ser desligadas. Conclua as seguintes etapas:

1. navegar para o nó **Pesquisar** e, em seguida, clique em **Colunas a Exibir**.
2. Na janela **Colunas a Exibir**, selecione a caixa de seleção ao lado de **Estado de Drenagem**.
3. Clique em **Salvar** para sair da janela **Colunas a Exibir**.

A coluna **Estado de Drenagem** pode exibir as seguintes informações:

- **Drenando até o desligamento.** Aparece quando as máquinas estão no estado de drenagem até serem desligadas.
- **Não drenando.** Aparece quando as máquinas ainda não estão em estado de drenagem.



Mais informações

Para obter mais informações sobre o Autoscale, consulte Citrix Autoscale na Tech Zone.

Configurações baseadas em agendamento e baseadas em carga

Como o Autoscale™ gerencia a energia das máquinas

O Autoscale liga e desliga as máquinas com base no agendamento selecionado. O Autoscale permite que você defina vários agendamentos que incluem dias específicos da semana e ajuste o número de máquinas disponíveis durante esses períodos. Se você espera que um conjunto de

usuários consuma os recursos da máquina em um horário específico em dias específicos, o Autoscale ajuda a fornecer uma experiência otimizada. Observe que essas máquinas serão ligadas durante o agendamento, independentemente de haver sessões em execução nelas.

> **Observação:**
>
> O Autoscale oferece suporte a qualquer máquina com gerenciamento de energia.

> O agendamento é baseado no **fuso horário** do grupo de entrega. Para alterar o fuso horário, você pode alterar as configurações do usuário em um grupo de entrega. Para obter mais informações, consulte Gerenciar Grupos de Entrega.

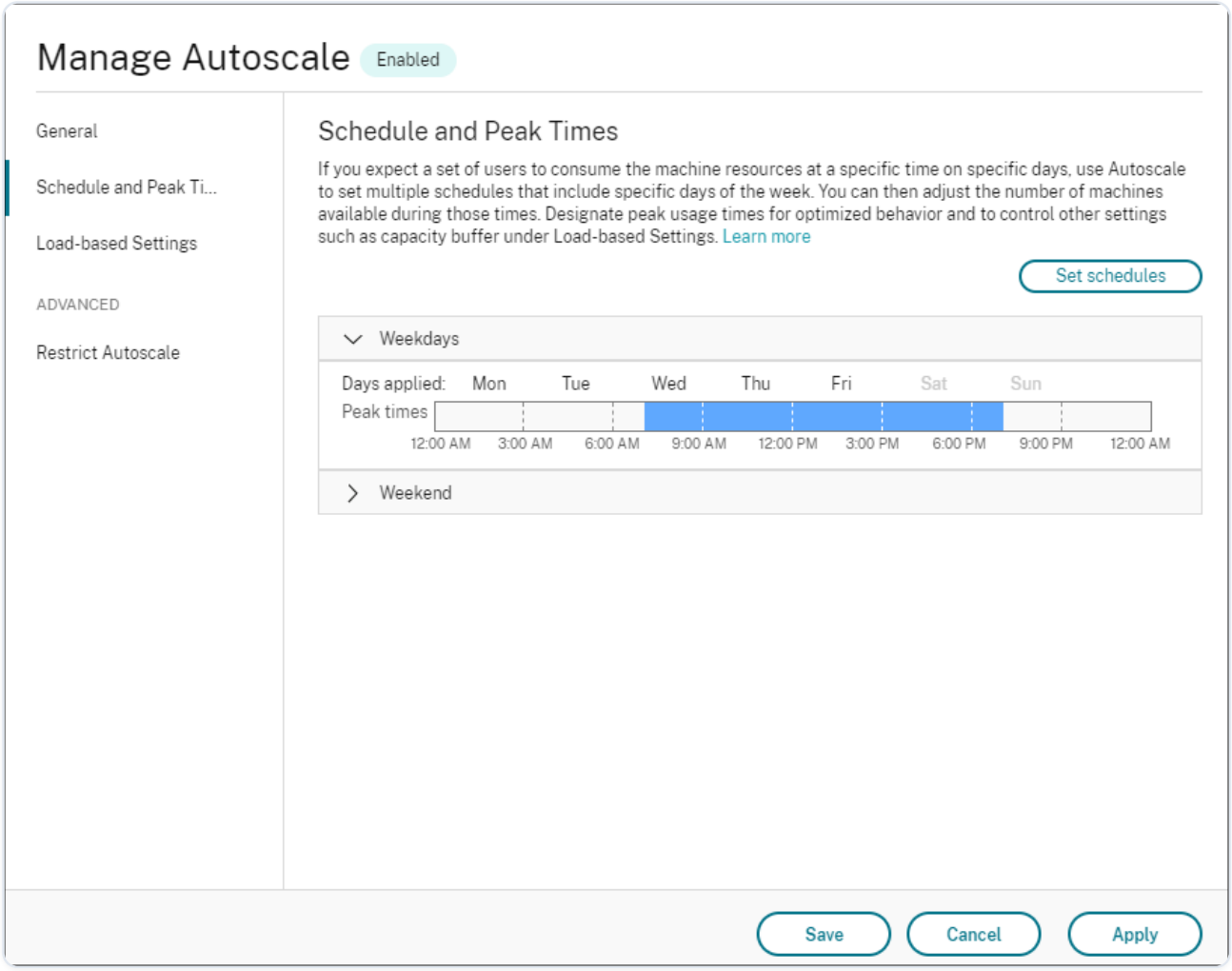
O Autoscale possui dois agendamentos padrão: *Dias da semana* (de segunda a sexta-feira) e *Fim de semana* (sábado e domingo). Por padrão, o agendamento **Dias da semana** mantém uma máquina ligada das 07:00 AM às 06:30 PM durante os horários de pico e nenhuma durante os horários de menor movimento. O buffer de capacidade padrão é definido como 10% durante os horários de pico e de menor movimento. Por padrão, o agendamento **Fim de semana** não mantém nenhuma máquina ligada.

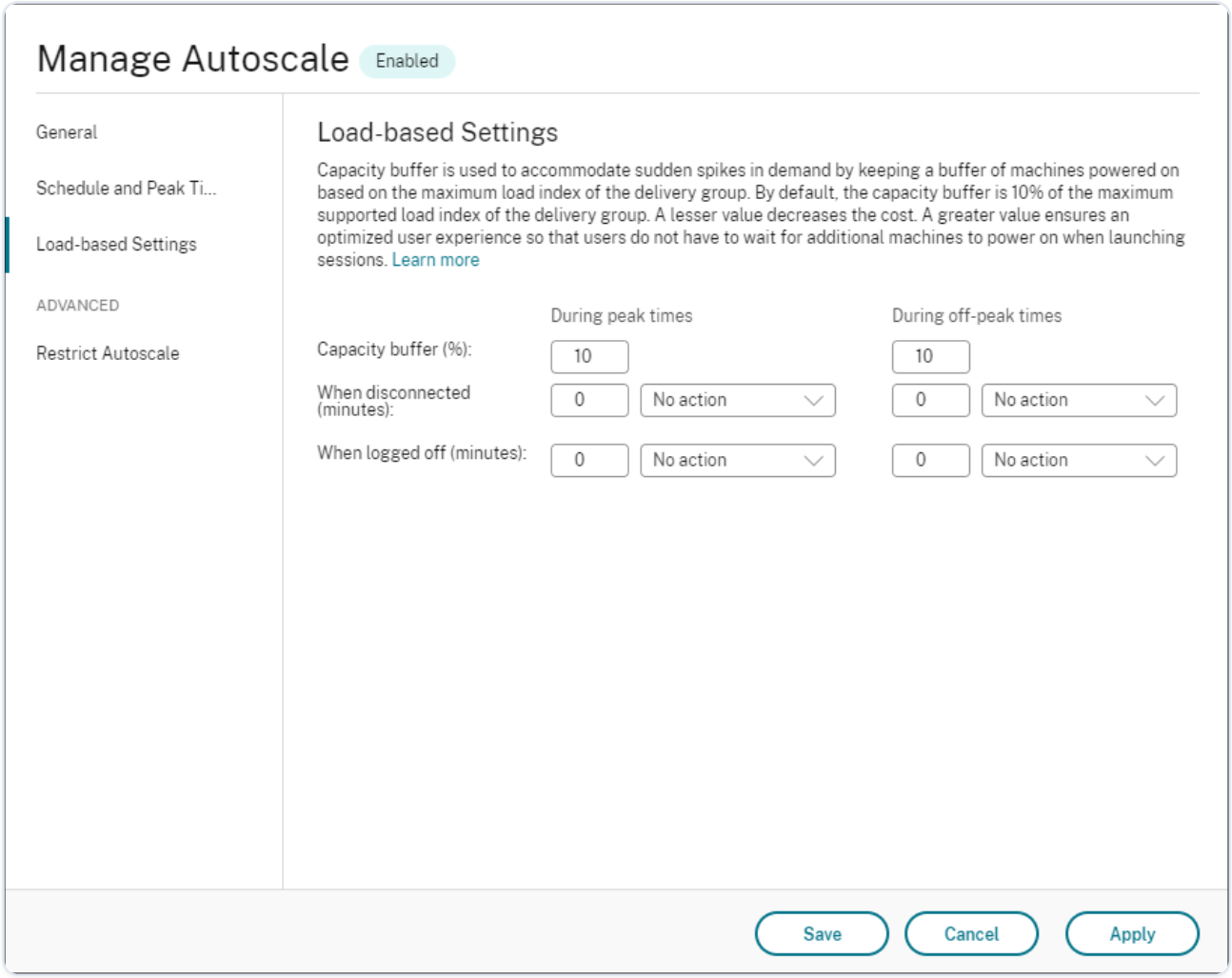
> **Observação:**
>
> O Autoscale considera apenas as máquinas registradas no site como parte da capacidade disponível nos cálculos que realiza. "Registrada" significa que a máquina está disponível para uso ou já em uso. Isso garante que apenas as máquinas que podem aceitar sessões de usuário sejam incluídas na capacidade do grupo de entrega.

Interfaces de usuário

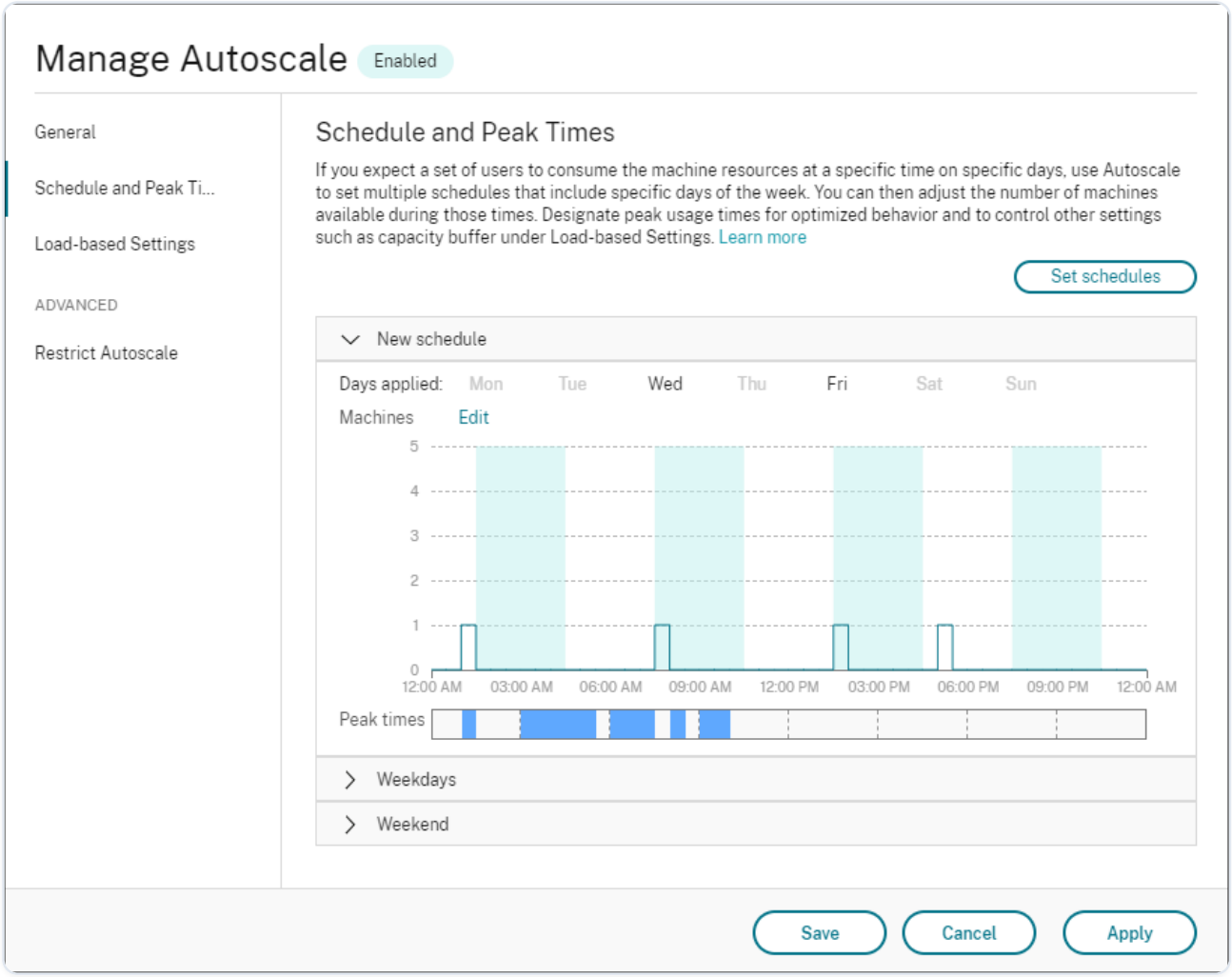
Existem três tipos de interfaces de usuário a serem consideradas.

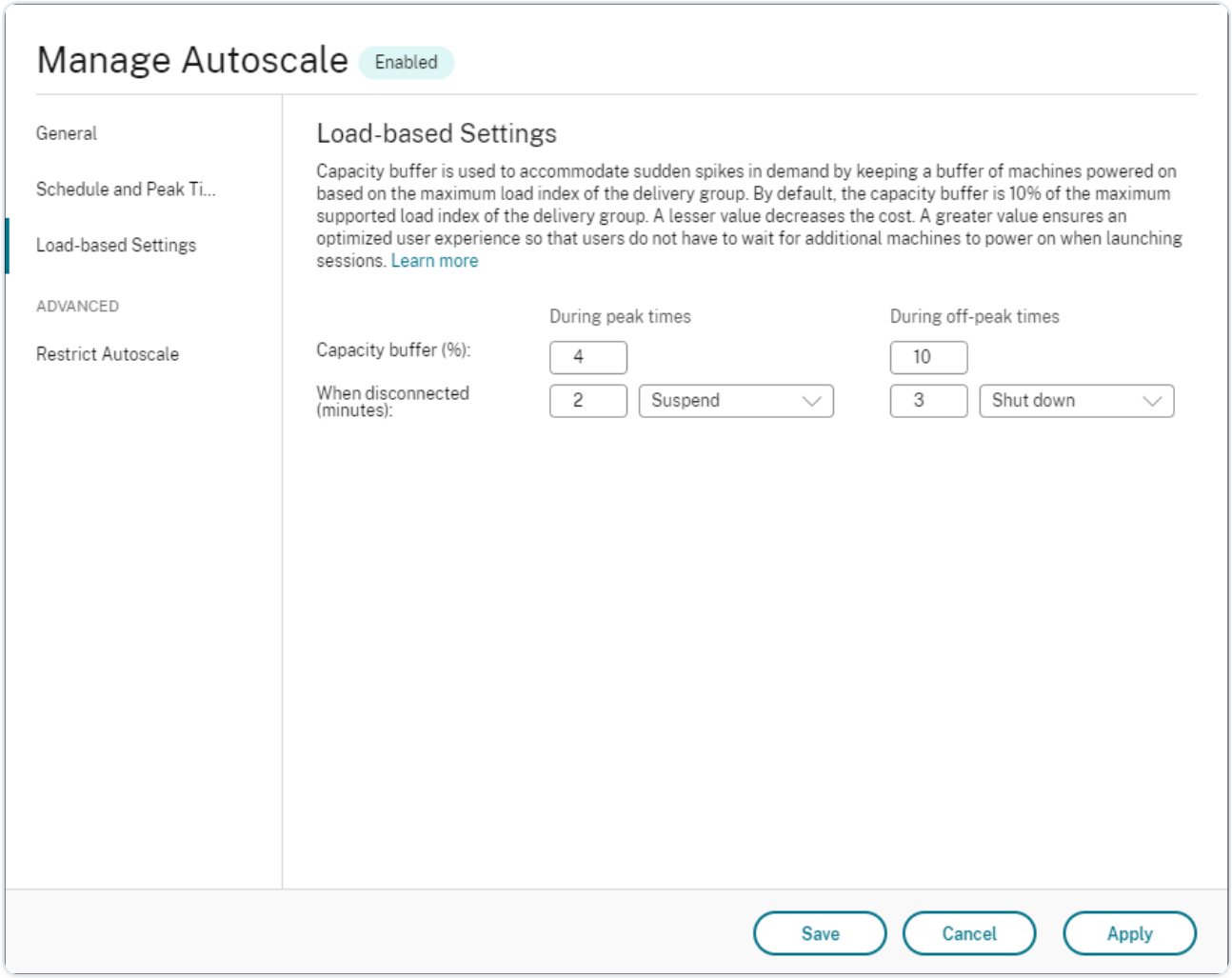
Interface de usuário para *grupos de entrega estáticos de SO de sessão única*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

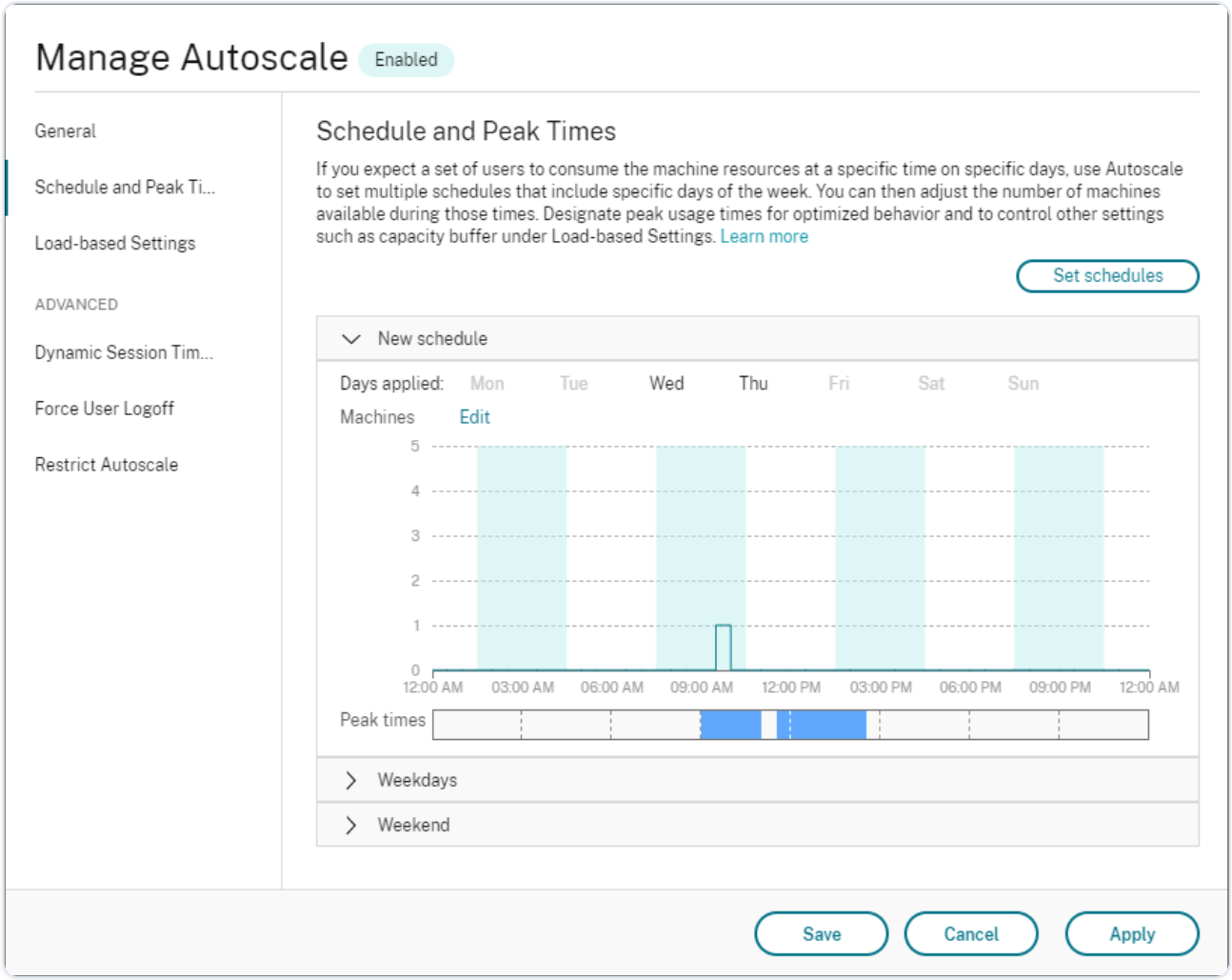


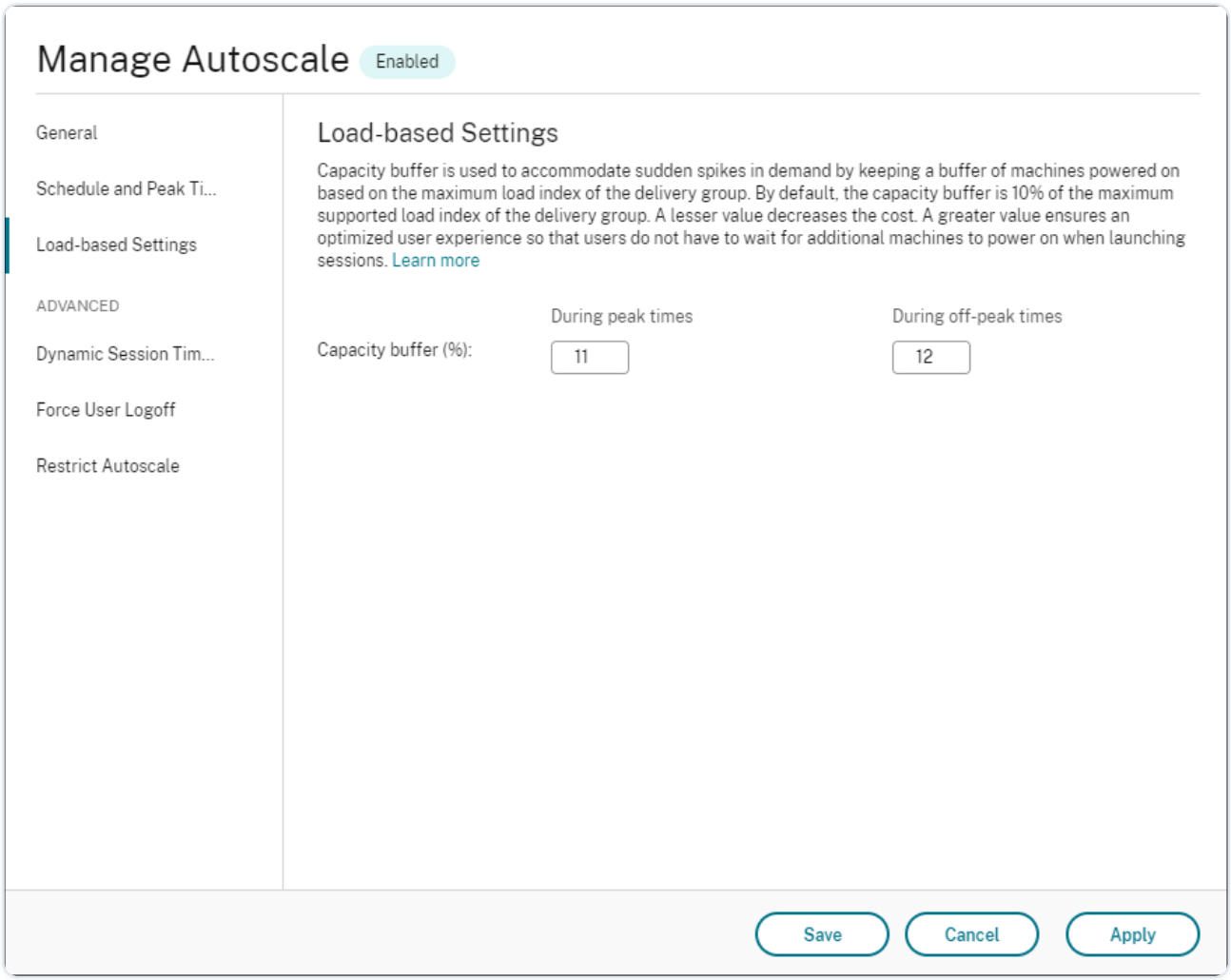
Interface de usuário do Autoscale para *grupos de entrega aleatórios de SO de sessão única*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Interface de usuário do Autoscale para *grupos de entrega de SO multi-sessão*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Configurações baseadas em agendamento

Agendamento do Autoscale. Permite adicionar, editar, selecionar e excluir agendamentos.

Dias aplicados. Destaca os dias que você aplicou ao agendamento selecionado. Os dias restantes ficam esmaecidos.

Editar. Permite atribuir as máquinas a cada hora ou a cada meia hora. Você pode atribuir as máquinas por números e por porcentagens.

Observação:

- Esta opção está disponível apenas nas interfaces de usuário do Autoscale para grupos de entrega aleatórios de SO multi-sessão e SO de sessão única.
- O histograma ao lado de **Editar** plota o número ou a porcentagem de máquinas que estão em execução em diferentes intervalos de tempo.

- Você pode **atribuir máquinas** a cada intervalo de tempo clicando em **Editar** acima de **Horários de pico**. Dependendo da opção selecionada no menu na janela **Máquinas para iniciar**, você pode atribuir as máquinas por números ou por porcentagens.
- Para grupos de entrega de SO multi-sessão, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 30 minutos durante cada dia. Para grupos de entrega aleatórios de SO de sessão única, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 60 minutos durante cada dia.

Para definir seus próprios agendamentos, siga estas etapas:

1. Na página **Agendamento e Horários de Pico** da janela **Gerenciar Autoscale**, clique em **Definir agendamentos**.
2. Na janela **Editar Agendamentos do Autoscale**, selecione os dias que deseja aplicar a cada agendamento. Você também pode excluir agendamentos, conforme aplicável.
3. Clique em **Concluído** para salvar os agendamentos e retornar à página **Agendamento e Horários de Pico**.
4. Selecione o agendamento aplicável e configure-o conforme necessário.
5. Clique em **Aplicar** para sair da janela **Gerenciar Autoscale** ou configurar as definições em outras páginas.

Importante:

- O Autoscale não permite que o mesmo dia se sobreponha em agendamentos diferentes. Por exemplo, se você selecionar segunda-feira no agendamento2 depois de selecionar segunda-feira no agendamento1, a segunda-feira será automaticamente desmarcada no agendamento1.
- Um nome de agendamento não diferencia maiúsculas de minúsculas.
- Um nome de agendamento não deve estar em branco ou conter apenas espaços.
- O Autoscale permite espaços em branco entre caracteres.
- Um nome de agendamento não deve conter os seguintes caracteres: \ / ; : # . * ? = < > \| ( ) { } " ' `.

- O Autoscale não oferece suporte a nomes de agendamento duplicados. Insira um nome diferente para cada agendamento.
- O Autoscale não oferece suporte a agendamentos vazios. Isso significa que agendamentos sem dias selecionados não são salvos.

Observação:

Os dias incluídos no agendamento selecionado são destacados, enquanto os não incluídos ficam esmaecidos.

Configurações baseadas em carga

Horários de pico. Permite definir os horários de pico para os dias aplicados no agendamento selecionado. Você pode fazer isso clicando com o botão direito do mouse no gráfico de barras horizontal. Depois de definir os horários de pico, os horários restantes e não definidos são padronizados para horários fora de pico. Por **padrão**, o período das 7:00 AM às 7:00 PM é definido como horários de pico para os dias incluídos no agendamento selecionado.

Importante:

- Para grupos de entrega de SO de várias sessões, o gráfico de barras de horários de pico é usado para o buffer de capacidade.
- Para grupos de entrega de SO de sessão única, o gráfico de barras de horários de pico é usado para o buffer de capacidade e controla as ações a serem acionadas após o logoff e/ou desconexão.
- Você pode definir os horários de pico para os dias incluídos em um agendamento em um nível granular de 30 minutos para grupos de entrega de SO de várias sessões e de sessão única. Alternativamente, você pode usar o comando `New-BrokerPowerTimeScheme PowerShell`. Para obter mais informações, consulte comandos do SDK do Broker PowerShell.

Buffer de capacidade. Permite manter um buffer de máquinas ligadas. Um valor menor diminui o custo. Um valor maior garante uma experiência de usuário otimizada para que, ao iniciar sessões, os usuários não precisem esperar que máquinas adicionais liguem. Por

padrão, o buffer de capacidade é de 10% para horários de pico e fora de pico. Se você definir o buffer de capacidade como 0 (zero), os usuários podem ter que esperar que máquinas adicionais liguem ao iniciar sessões. O Autoscale permite que você determine o buffer de capacidade separadamente para horários de pico e fora de pico.

Configurações diversas

Dica:

- Você pode optar por configurar as configurações diversas usando o SDK do Broker PowerShell. Para obter mais informações, consulte comandos do SDK do Broker PowerShell.
- Para entender os comandos do SDK associados às configurações de quando desconectado e quando desconectado (logoff), consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`.

Quando desconectado. Permite especificar por quanto tempo uma máquina desconectada e bloqueada permanece ligada após a desconexão da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de desconexão especificado expira, dependendo da ação que você configurou. Por padrão, nenhuma ação é atribuída a máquinas desconectadas. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina após a desconexão da sessão permanece ligada. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de desconexão especificado expira. A seguinte opção fica disponível depois que você seleciona **Suspender**.
  - **Quando não houver reconexão em (minutos)**. Máquinas suspensas permanecem disponíveis para usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Para tornar as máquinas disponíveis novamente para manipular todas as cargas de trabalho, desligue-as. Especifique o tempo limite, em minutos, após o qual o Autoscale as desliga.

- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de desconexão especificado expira.

Observação:

Esta opção está disponível apenas nas interfaces de usuário do Autoscale para grupos de entrega aleatórios e estáticos de SO de sessão única.

Quando desconectado (logoff). Permite especificar por quanto tempo uma máquina permanece ligada após o logoff da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de logoff especificado expira, dependendo das ações que você configurou. Por padrão, nenhuma ação é atribuída a máquinas com logoff. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina após o logoff da sessão permanece ligada. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de logoff especificado expira.
- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de logoff especificado expira.

Observação:

Esta opção está disponível apenas na interface de usuário do Autoscale para grupos de entrega estáticos de SO de sessão única.

Gerenciar energia de máquinas OS de sessão única em transição para um período de tempo diferente com sessões desconectadas

Importante:

- Este aprimoramento se aplica apenas a máquinas OS de sessão única com sessões desconectadas. Não se aplica a máquinas OS de sessão única com sessões encerradas.
- Para que este aprimoramento entre em vigor, você precisa habilitar o Autoscale para o grupo de entrega aplicável. Caso contrário, as ações da política de energia de desconexão não são acionadas na transição de período.

Em versões anteriores, uma máquina OS de sessão única em transição para um período de tempo onde uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Este cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) onde nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir desta versão, o Autoscale suspende ou desliga a máquina quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega OS de sessão única:

- Defina `PeakDisconnectAction` como "Nada"
- Defina `OffPeakDisconnectAction` como "Desligar"
- Defina 'OffPeakDisconnectTimeout' como "10"

Observação:

Para obter mais informações sobre a política de energia de ação de desconexão, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` e `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

Em versões anteriores, uma máquina OS de sessão única com uma sessão desconectada durante os horários de pico permanecia ligada ao fazer a transição do pico para fora do pico. A partir desta versão, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina OS de sessão única na transição

> de período. Como resultado, a máquina é desligada 10 minutos após a transição para fora do pico.

Caso você queira reverter para o comportamento anterior (ou seja, não tomar nenhuma ação em máquinas que fazem a transição do pico para fora do pico ou do fora do pico para o pico com sessões desconectadas), faça o seguinte:

- Defina o valor do registro "LegacyPeakTransitionDisconnectedBehaviour" como 1 (verdadeiro; habilita o comportamento anterior). Por padrão, o valor é 0 (falso; aciona as ações da política de energia de desconexão na transição de período).
  - Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dados: 0x00000001 (1)
- Configure a definição usando o comando PowerShell `Set-BrokerServiceConfigurationData`. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações da política de energia possam ser aplicadas a ela na transição de período:

- Tem uma sessão desconectada.
- Não tem ações de energia pendentes.
- Pertence a um grupo de entrega de SO de sessão única que faz a transição para um período de tempo diferente.
- Tem uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e faz a transição para um período onde uma ação de energia é atribuída.

Como o buffer de capacidade funciona

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem observados:

- Para grupos de entrega de SO de várias sessões, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga. Para obter mais informações sobre o índice de carga, consulte Índice de carga.
- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos do número de máquinas.

Observação:

Em cenários onde você restringe o Autoscale a máquinas marcadas, o buffer de capacidade é definido como uma porcentagem da capacidade total das máquinas marcadas no grupo de entrega em termos de índice de carga.

O Autoscale permite que você defina o buffer de capacidade separadamente para horários de pico e fora de pico. Um valor menor no campo do buffer de capacidade diminui o custo porque o Autoscale liga menos capacidade sobressalente. Um valor maior garante uma experiência de usuário otimizada para que os usuários não precisem esperar que máquinas adicionais liguem ao iniciar sessões. Por padrão, o buffer de capacidade é de 10%.

Importante:

O buffer de capacidade resulta em máquinas sendo ligadas quando a capacidade sobressalente total cai para um nível abaixo de "X" por cento da capacidade total do grupo de entrega. Fazer isso reserva a porcentagem necessária de capacidade sobressalente.

Grupos de entrega de SO de várias sessões

Quando as máquinas são ligadas?

Importante:

Se um agendamento for selecionado, o Autoscale liga todas as máquinas configuradas para serem ligadas no agendamento. O Autoscale mantém esse número especificado de máquinas ligadas durante o agendamento, independentemente da carga.

Quando o número de máquinas ligadas no grupo de entrega não consegue mais atender ao buffer necessário para honrar a capacidade do buffer em termos de índice de carga, o Autoscale liga máquinas extras. Por exemplo, digamos que seu grupo de entrega tenha 20 máquinas e 3 máquinas estejam agendadas para serem ligadas como parte do dimensionamento baseado em agendamento com um buffer de capacidade de 20%. Eventualmente, 4 máquinas serão ligadas quando não houver carga. Isso ocorre porque um índice de carga de 4 x 10k é necessário como buffer; portanto, pelo menos 4 máquinas precisam ser ligadas. Este caso pode ocorrer durante horários de pico, aumento da carga nas máquinas, novos inícios de sessão e quando você adiciona novas máquinas ao grupo de entrega. Observe que o Autoscale liga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas não estão em modo de manutenção.
- O hipervisor no qual as máquinas estão sendo executadas não está em modo de manutenção.
- As máquinas estão atualmente desligadas.
- As máquinas não têm ações de energia pendentes.

Quando as máquinas são desligadas?

Importante:

- Se um agendamento for selecionado, o Autoscale desliga as máquinas com base no agendamento.
- O Autoscale não desliga as máquinas configuradas no agendamento para serem ligadas durante o agendamento.

Quando há máquinas mais do que suficientes para suportar o número alvo de máquinas ligadas (incluindo o buffer) para o grupo de entrega, o Autoscale desliga máquinas extras. Este caso pode ocorrer durante horários de menor movimento, diminuição da carga nas máquinas e logoffs de sessão, e quando você remove máquinas do grupo de entrega. O Autoscale desliga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas e o hipervisor no qual as máquinas estão sendo executadas não estão em modo de manutenção.
- As máquinas estão atualmente ligadas.

- As máquinas estão registradas como disponíveis ou aguardando registro após a inicialização.
- As máquinas não têm sessões ativas.
- As máquinas não têm ações de energia pendentes.
- As máquinas satisfazem o atraso de desligamento especificado. Isso significa que as máquinas estiveram ligadas por pelo menos "X" minutos, onde "X" é o atraso de desligamento especificado para o grupo de entrega.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - Uma máquina (por exemplo, M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina é ligada.
  - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base (índice de carga igual a 0).
- O primeiro usuário faz logon

  - A sessão é direcionada para ser hospedada na máquina M1.
  - O índice de carga da máquina ligada M1 aumenta e a máquina M1 não está mais em uma carga de linha de base.
  - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.
  - O valor do índice de carga da máquina M2 está em uma carga de linha de base.

- Usuários aumentam a carga
  - As sessões são balanceadas entre as máquinas M1 e M2. Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta.
  - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
  - O valor do índice de carga da máquina M2 não está mais em uma carga de linha de base.
- Mais sessões de usuário são iniciadas
  - As sessões são balanceadas entre as máquinas (M1 e M2). Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta ainda mais.
  - Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.
  - O valor do índice de carga da máquina M3 está em uma carga de linha de base.
- Ainda mais sessões de usuário são iniciadas
  - As sessões são balanceadas por carga entre as máquinas (M1 a M3). Como resultado, o índice de carga das máquinas ligadas (M1 a M3) aumenta.
  - A capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
  - O valor do índice de carga da máquina M3 não está mais em uma carga de linha de base.
- A carga da sessão do usuário diminui devido ao encerramento da sessão
  - Depois que os usuários saem de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M3 é reutilizada para hospedar sessões iniciadas por outros usuários.

    - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M3) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina, a menos que novas alterações ocorram. Por exemplo, a carga do usuário final aumenta novamente ou outras máquinas se tornam menos carregadas.

- A carga da sessão do usuário continua a diminuir
    - Depois que todas as sessões na máquina M3 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M3.
    - Depois que mais usuários encerram suas sessões, a capacidade liberada nas máquinas ligadas (M1 e M2) é reutilizada para hospedar sessões iniciadas por outros usuários.
    - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M2) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina.
- A carga da sessão do usuário continua a diminuir até que não haja sessões
    - Depois que todas as sessões na máquina M2 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M2.
    - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base. O Autoscale não coloca a máquina M1 em estado de drenagem devido ao buffer de capacidade configurado.

> **Observação:**
>
> Para grupos de entrega de SO multi-sessão, todas as alterações na área de trabalho são perdidas quando os usuários encerram as sessões. No entanto, se configurado, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

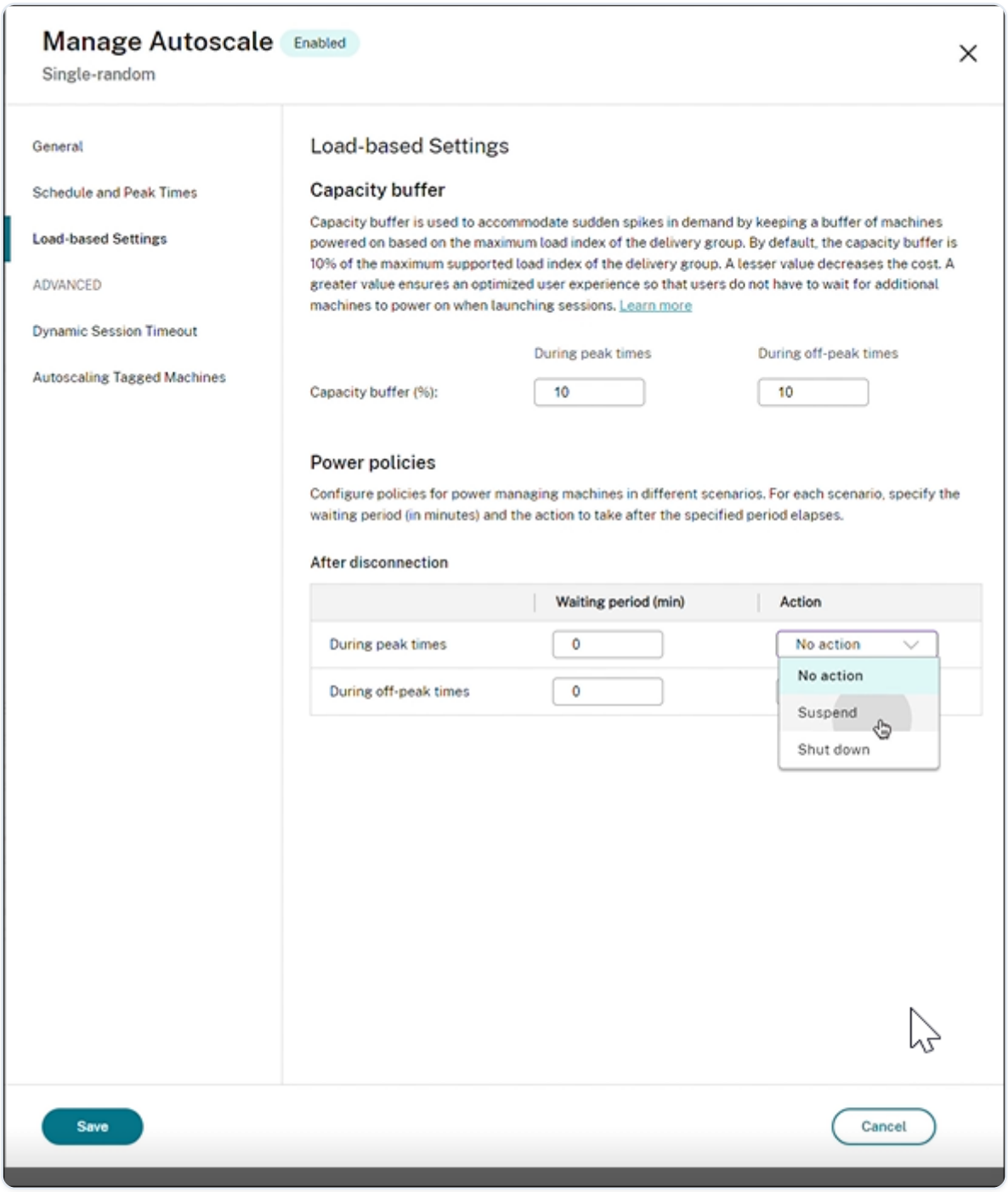
Grupos de entrega aleatórios de SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas ligadas com base no número total de máquinas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas no grupo de entrega.

Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

Políticas de energia

Configure políticas para gerenciar a energia das máquinas para diferentes cenários. Para cada cenário, você pode especificar o tempo de espera (em minutos) e a ação a ser tomada após o término do tempo especificado. As políticas de energia são aplicáveis a grupos de entrega aleatórios de SO de sessão única e grupos de entrega estáticos de SO de sessão única.

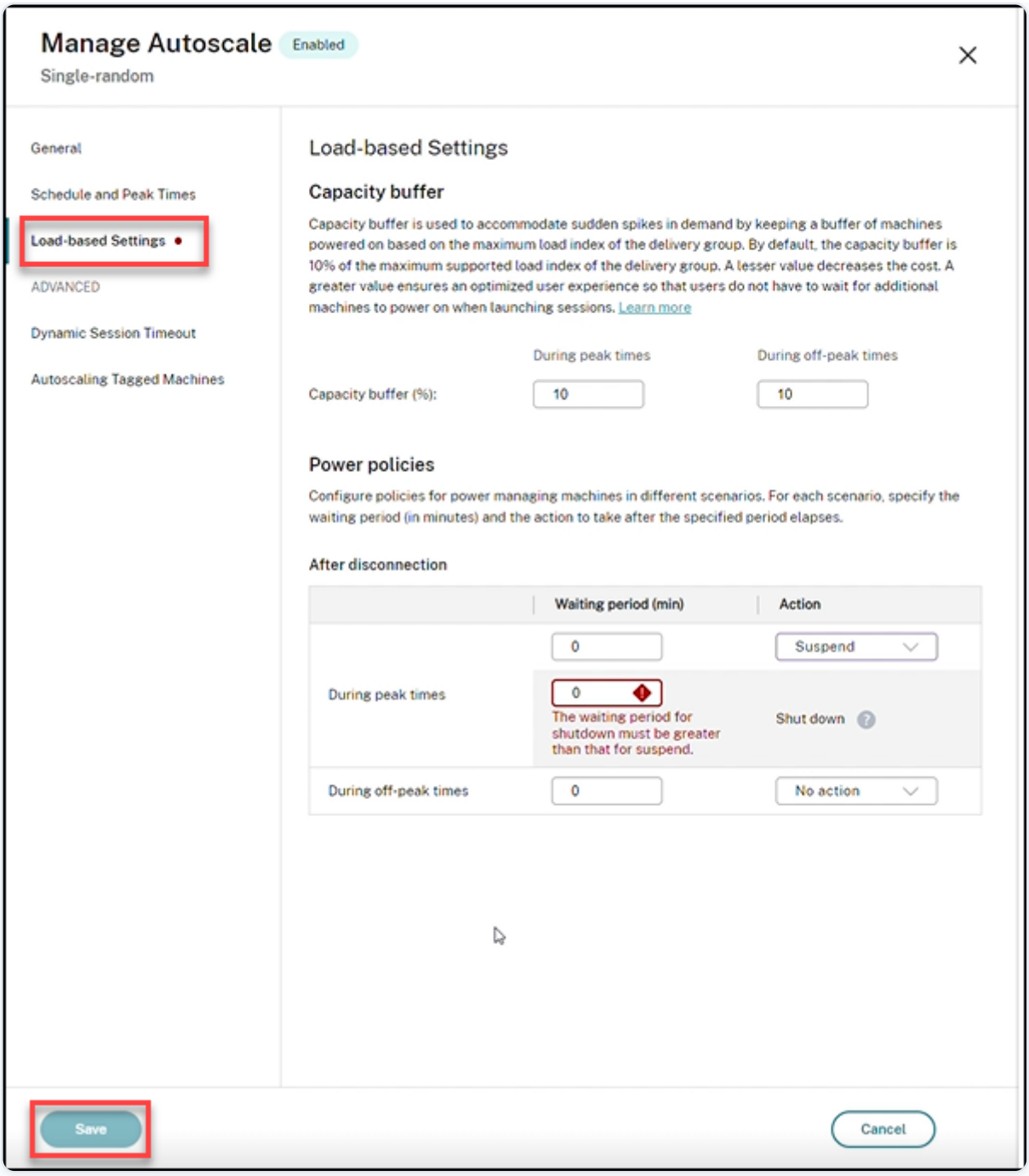


Após a desconexão, as seguintes configurações são aplicáveis tanto durante os horários de pico quanto durante os horários de folga:

- Você pode definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar no menu suspenso.
- Se você selecionar a ação de suspender, configure um tempo de espera adicional para desligar a máquina.

> **Observação:**

- Durante os horários de pico e de folga, o tempo de espera para a ação de desligamento deve ser maior do que o tempo de espera para suspender.
- Máquinas suspensas são acessíveis apenas a usuários desconectados quando eles se reconectam. Para tornar as máquinas suspensas disponíveis para novos usuários, desligue-as.
- Se as configurações de tempo estiverem incorretamente configuradas para os campos de suspender e desligar, a opção **Salvar** é desabilitada e um ponto vermelho também aparece ao lado dos itens de navegação, indicando erros de configuração.



Por exemplo

- Se você definir o tempo de espera para 12 minutos e escolher a primeira ação como nenhuma ação, então, após o término dos 12 minutos, a máquina continuará no estado ligado.
- Se você definir o tempo de espera para 15 minutos e escolher a primeira ação como suspender, e o segundo tempo de espera para 20 minutos, após o término dos 15 minutos, a máquina será suspensa. Após o término do segundo tempo de espera, a máquina será desligada.
- Se você definir o tempo de espera para 18 minutos e escolher a primeira ação como desligar, então, após o término dos 18 minutos, a máquina será desligada.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - Uma máquina (M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10% (buffer de capacidade configurado) é igual a 1. Portanto, uma máquina é ligada.
- Um primeiro usuário faz logon

  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas ligadas. Neste caso, o usuário recebe um desktop da máquina M1.
  - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.

- Um segundo usuário faz logon
  - O usuário recebe um desktop da máquina M2.
  - O Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.

- Um terceiro usuário faz logon
  - O usuário recebe um desktop da máquina M3.
  - O Autoscale começa a ligar uma máquina adicional (M4) para atender à demanda devido ao buffer de capacidade configurado.

- Um usuário faz logoff
  - Depois que um usuário faz logoff ou o desktop do usuário expira, a capacidade liberada (por exemplo, M3) fica disponível como buffer. Como resultado, o Autoscale começa a desligar a máquina M4 porque o buffer de capacidade está configurado para 10%.

- Mais usuários fazem logoff até que não haja 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 está reservada como capacidade sobressalente.

> **Observação:**

> Para grupos de entrega aleatórios de SO de sessão única, todas as alterações na área de trabalho são perdidas quando os usuários fazem logoff das sessões. No entanto, se configuradas, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

Grupos de entrega estáticos de SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas não atribuídas ligadas com base no número total de máquinas não atribuídas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas não atribuídas no grupo de entrega.

> **Importante:**

> Depois que todas as máquinas no grupo de entrega são atribuídas, o buffer de capacidade não desempenha um papel no ligar ou desligar das máquinas.

> Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais não atribuídas são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

Para grupos de entrega estáticos de SO de sessão única, o Autoscale:

- Liga as máquinas atribuídas durante os horários de pico e as desliga durante os horários de menor movimento somente quando a propriedade `AutomaticPowerOnForAssigned` do grupo de entrega de SO de sessão única aplicável está 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.

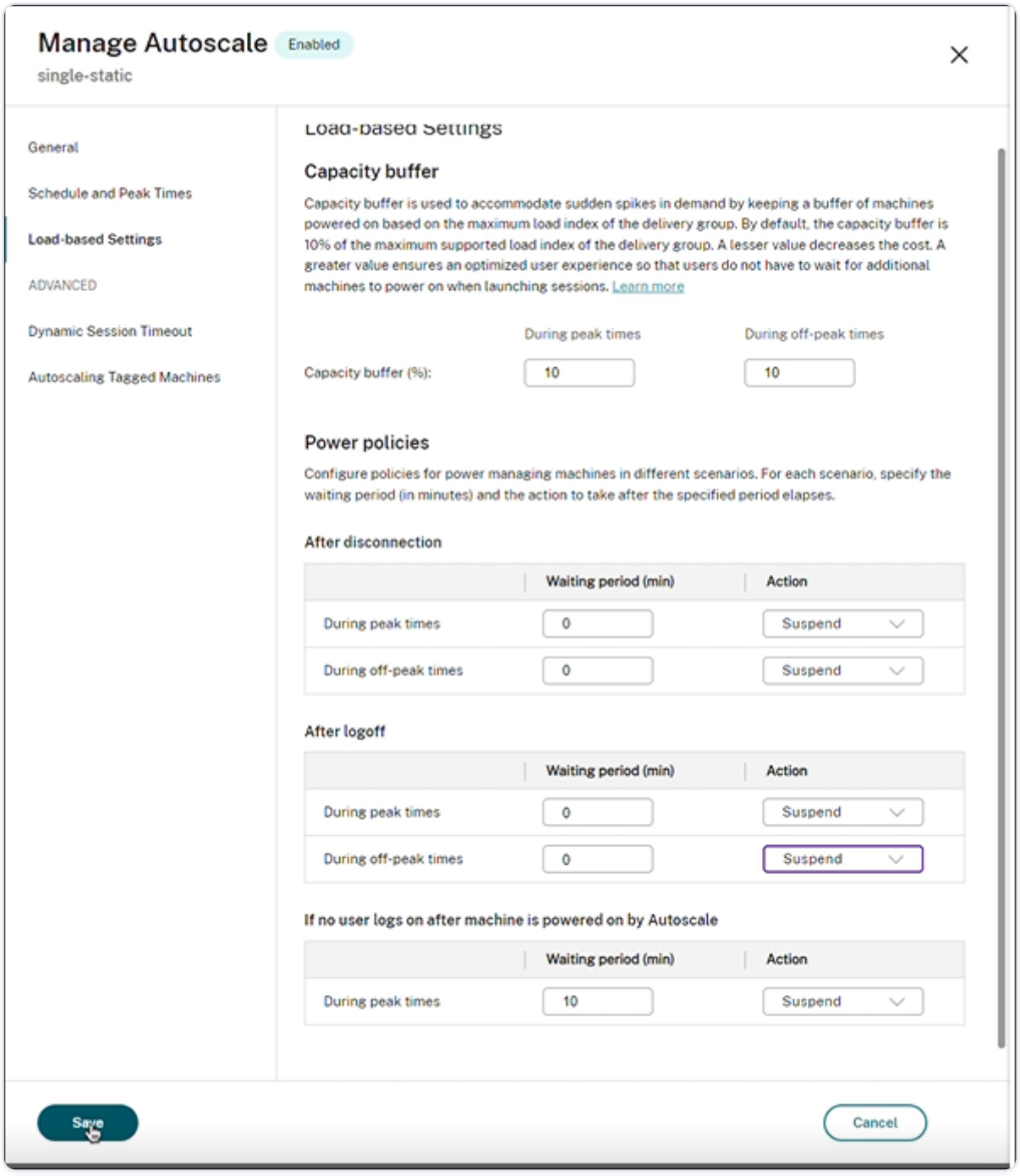
Para entender como o buffer de capacidade funciona com máquinas atribuídas, considere o seguinte:

- O buffer de capacidade funciona somente quando o grupo de entrega tem uma ou mais máquinas não atribuídas.
- Se o grupo de entrega não tiver máquinas não atribuídas (todas as máquinas no grupo de entrega estão atribuídas), o buffer de capacidade não desempenha um papel no ligar ou desligar 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 mesmo que estejam desligadas.

Políticas de energia

Configure políticas para gerenciar a energia das máquinas para diferentes cenários. Para cada cenário, você pode especificar o tempo de espera (em minutos) e a ação a ser tomada após o término do tempo especificado. As políticas de energia são aplicáveis a grupos de entrega aleatórios de SO de sessão única e grupos de entrega estáticos de SO de sessão única.



Para **Após desconexão** e **Após logoff**, as seguintes configurações são aplicáveis tanto durante os horários de pico quanto durante os horários de folga: Você pode definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar no menu suspenso.

Se nenhum usuário fizer logon depois que a máquina for ligada pelo Autoscale, as seguintes configurações são aplicáveis apenas 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.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - As máquinas M1 a M3 são atribuídas, e as máquinas M4 a M10 não são atribuídas.
  - Buffer de capacidade definido para 10% para horários de pico e de folga.
  - De acordo com o agendamento selecionado, o Autoscale gerencia a energia das máquinas entre 09:00 e 18:00.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Início do agendamento – 09:00
  - O Autoscale liga as máquinas M1 a M3.
  - O Autoscale liga uma máquina adicional (por exemplo, M4) devido ao buffer de capacidade configurado. A máquina M4 não é atribuída.
- Um primeiro usuário faz logon
  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas não atribuídas e ligadas. Neste caso, o usuário recebe um desktop da máquina M4. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - O Autoscale começa a ligar uma máquina adicional (por exemplo, M5) para atender à demanda devido ao buffer de capacidade configurado.
- Um segundo usuário faz logon

    - O usuário recebe um desktop das máquinas não atribuídas e ligadas. Neste caso, o usuário recebe um desktop da máquina M5. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
    - O Autoscale começa a ligar uma máquina adicional (por exemplo, M6) para atender à demanda devido ao buffer de capacidade configurado.

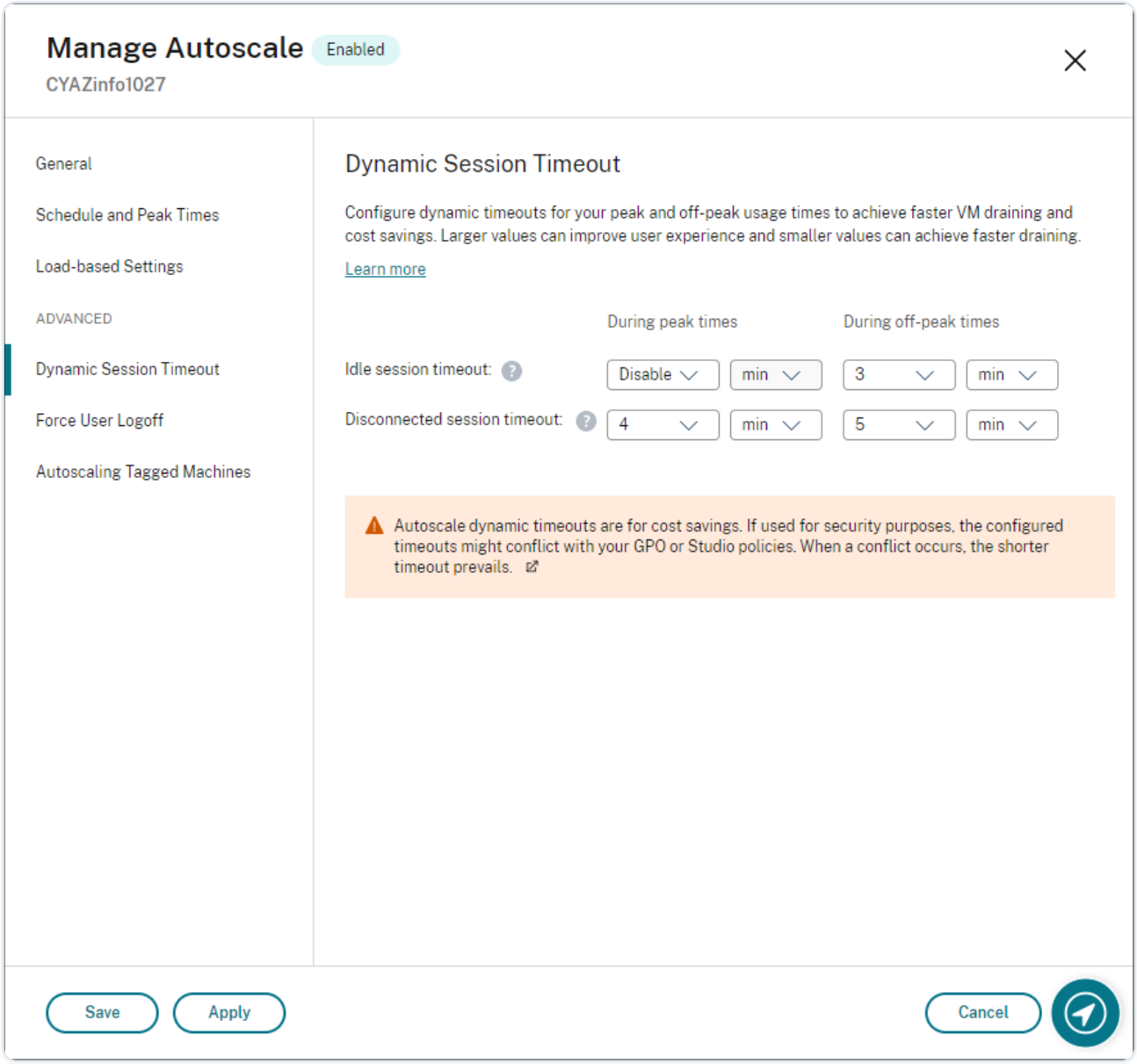
- Usuários fazem logoff
    - À medida que os usuários fazem logoff de seus desktops ou os desktops expiram, o Autoscale mantém as máquinas M1 a M5 ligadas durante as 09:00 AM – 06:00 PM. Quando esses usuários fizerem logon na próxima vez, eles se conectarão ao mesmo desktop que foi atribuído no primeiro uso.
    - A máquina não atribuída M6 está aguardando para servir um desktop a um usuário não atribuído e que está chegando.
- Fim do agendamento – 06:00 PM
    - Às 06:00 PM, o Autoscale desliga as máquinas M1 a M5.
    - O Autoscale mantém a máquina não atribuída M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário não atribuído e que está chegando.
    - No grupo de entrega, as máquinas M6 a M10 são máquinas não atribuídas.

Tempos limite de sessão dinâmicos

Este recurso permite configurar tempos limite de sessão desconectada e ociosa para seus horários de pico e fora de pico, a fim de obter um esvaziamento mais rápido da máquina e economia de custos. Este recurso se aplica a:

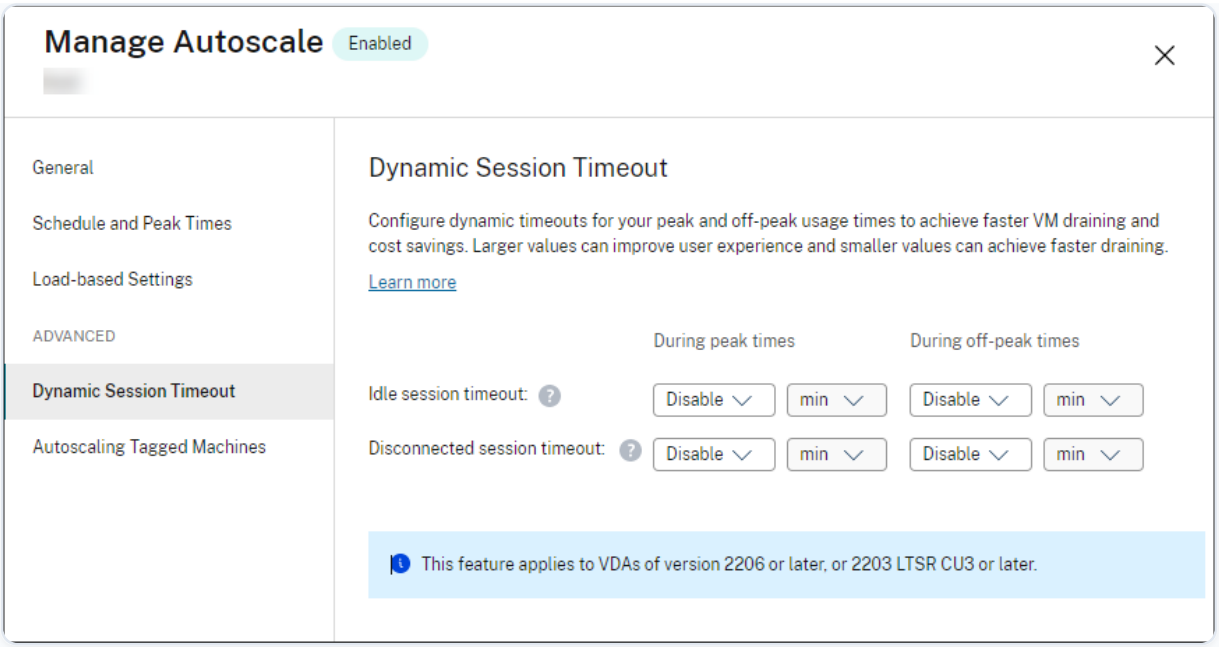
- Máquinas de SO de sessão única e multi-sessão.
- Todas as máquinas no Grupo de Entrega, independentemente de estarem marcadas para dimensionamento automático.

Um VDA relata tempos ociosos para sessões que estiveram ociosas por mais de 10 minutos, portanto, os tempos limite de sessão dinâmicos não conseguem desconectar sessões ociosas dentro de 10 minutos de inatividade. Um valor menor remove sessões persistentes mais cedo, reduzindo assim os custos.



Observação:

- Este recurso está sempre disponível para grupos de entrega de SO multi-sessão.
- Para grupos de entrega de SO de sessão única, este recurso se aplica a VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Certifique-se de que esses VDAs tenham se registrado no Citrix Cloud™ pelo menos uma vez. Quando indisponível, a seguinte interface de usuário aparece:



- Os tempos limite dinâmicos do Autoscale™ são para economia de custos. Se usados para fins de segurança, os tempos limite configurados podem entrar em conflito com suas políticas de GPO ou do console de Gerenciamento. Quando ocorre um conflito, o tempo limite mais curto prevalece.

Tempo limite de sessão ociosa. Ativa ou desativa um temporizador que especifica por quanto tempo uma conexão de usuário ininterrupta é mantida se não houver entrada do usuário. Quando o temporizador expira, a sessão é colocada no estado desconectado e o **Tempo limite de sessão desconectada** se aplica. Se o **Tempo limite de sessão desconectada** estiver desativado, a sessão não é encerrada.

Importante:

- Se você especificar um valor menor ou igual a 10 minutos (600 segundos), o Autoscale desconecta as sessões relevantes depois que elas estiverem ociosas por 10 minutos. Isso ocorre porque o Autoscale depende dos tempos ociosos de sessão que os VDAs relatam. Os VDAs relatam tempos ociosos apenas para sessões que estiveram ociosas por mais de 10 minutos.
- Uma sessão ociosa ainda pode ser colocada em um estado desconectado se o usuário interagir com ela nos últimos 5 minutos antes de atingir o tempo limite de sessão ociosa.

> **Tempo limite de sessão desconectada**. Ativa ou desativa um temporizador que especifica por quanto tempo uma área de trabalho desconectada permanece bloqueada antes que a sessão seja encerrada. Se ativado, a sessão desconectada é encerrada quando o temporizador expira.

Perguntas Frequentes

O recurso de tempo limite de sessão dinâmico se aplica apenas a máquinas marcadas para Autoscaling?

O recurso de tempo limite de sessão dinâmico se aplica a todas as máquinas no grupo de entrega, independentemente de estarem marcadas para autoscaling.

Quando uma sessão é desconectada devido ao tempo limite de sessão dinâmico, as máquinas não marcadas também são incluídas no destino do Autoscale de máquinas marcadas?

O recurso de tempo limite de sessão dinâmico não está relacionado ao recurso de marcação do Autoscale. Se os tempos limite de sessão dinâmicos resultarem no encerramento de sessões, as máquinas não marcadas também poderão ser desligadas durante o processo, desde que as máquinas estejam esvaziando até o desligamento.

Dimensionamento automático de máquinas marcadas (expansão para a nuvem)

> **Observação:**
>
> Este recurso era anteriormente Restringir Dimensionamento Automático.

Introdução

O Autoscale oferece a flexibilidade para gerenciar a energia de apenas um subconjunto de máquinas em um grupo de entrega. Para conseguir isso, aplique uma tag a uma ou mais máquinas e então configure o Autoscale para gerenciar a energia apenas das máquinas marcadas.

Esse recurso pode ser útil em casos de uso de expansão para a nuvem, onde você deseja usar recursos locais (ou instâncias de nuvem pública reservadas) para manipular cargas de trabalho antes que os recursos baseados em nuvem atendam à demanda adicional (ou seja, cargas de

trabalho de expansão). Para permitir que as máquinas locais (ou instâncias reservadas) atendam às cargas de trabalho primeiro, você deve usar a restrição de tag junto com a preferência de zona.

A restrição de tag especifica as máquinas a serem gerenciadas por energia pelo Dimensionamento Automático. A preferência de zona especifica as máquinas na zona preferencial para manipular as solicitações de inicialização do usuário. Para obter mais informações, consulte Tags e Preferência de zona.

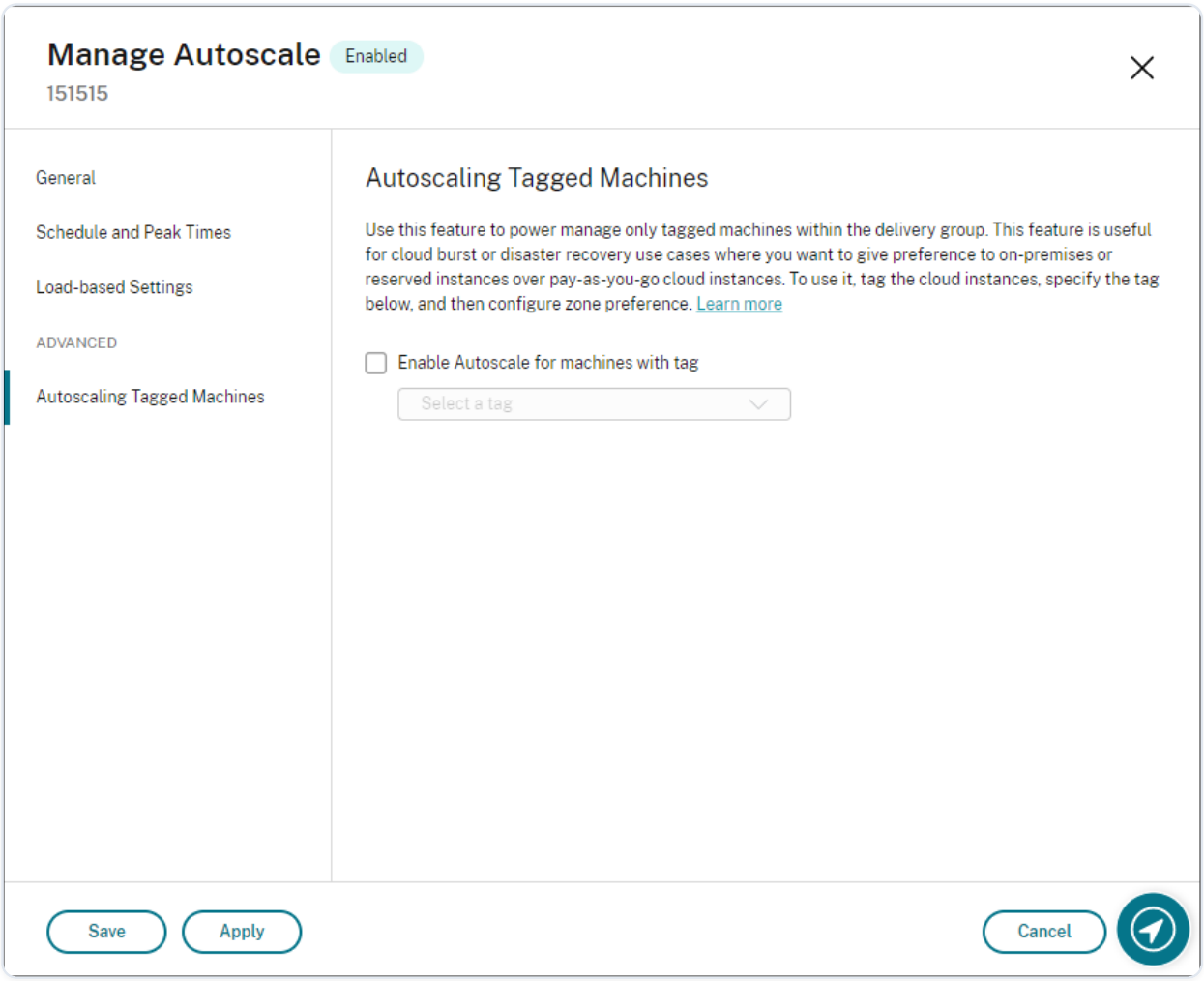
Para dimensionar automaticamente certas máquinas marcadas, você pode usar o console Gerenciar ou o PowerShell.

Usar o console Gerenciar para dimensionar automaticamente certas máquinas marcadas

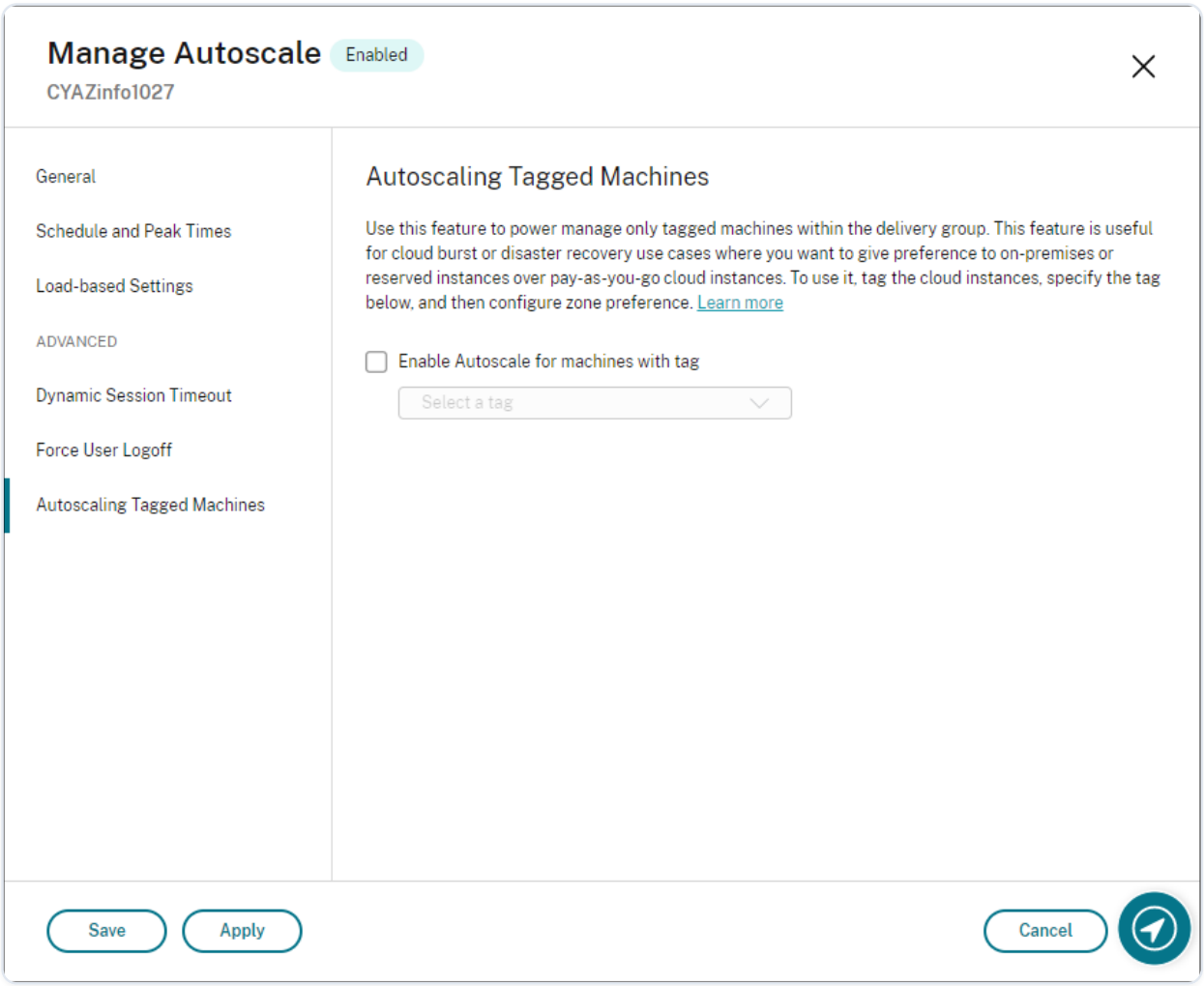
Para dimensionar automaticamente certas máquinas marcadas, conclua as seguintes etapas:

1. Crie uma tag e aplique-a às máquinas aplicáveis no grupo de entrega. Para obter mais informações, consulte Gerenciar tags e restrições de tags.
2. Selecione o grupo de entrega e, em seguida, abra o assistente **Gerenciar Dimensionamento Automático**.
3. Na página **Dimensionamento Automático de Máquinas Marcadas**, selecione **Habilitar Dimensionamento Automático para máquinas com tag**, selecione uma tag na lista e, em seguida, clique em **Aplicar** para salvar suas alterações.

   Interface do usuário para grupos de entrega de SO de sessão única *estáticos* e *aleatórios*:



Interface do usuário para *grupos de entrega de SO de várias sessões*:



Aviso:

- O dimensionamento automático de máquinas com uma tag específica pode fazer com que o histograma seja atualizado automaticamente para refletir o número de máquinas por tag. Na página **Agendamento e Horários de Pico**, você pode atribuir máquinas manualmente a cada slot de tempo, se necessário.
- Você não pode excluir uma tag que está sendo usada em máquinas marcadas. Para excluir a tag, você deve primeiro remover a restrição da tag.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, vá para a página **Gerenciar Autoscale > Máquinas Marcadas com Autoscale** e desmarque **Habilitar Autoscale para máquinas com tag**.

Aviso:

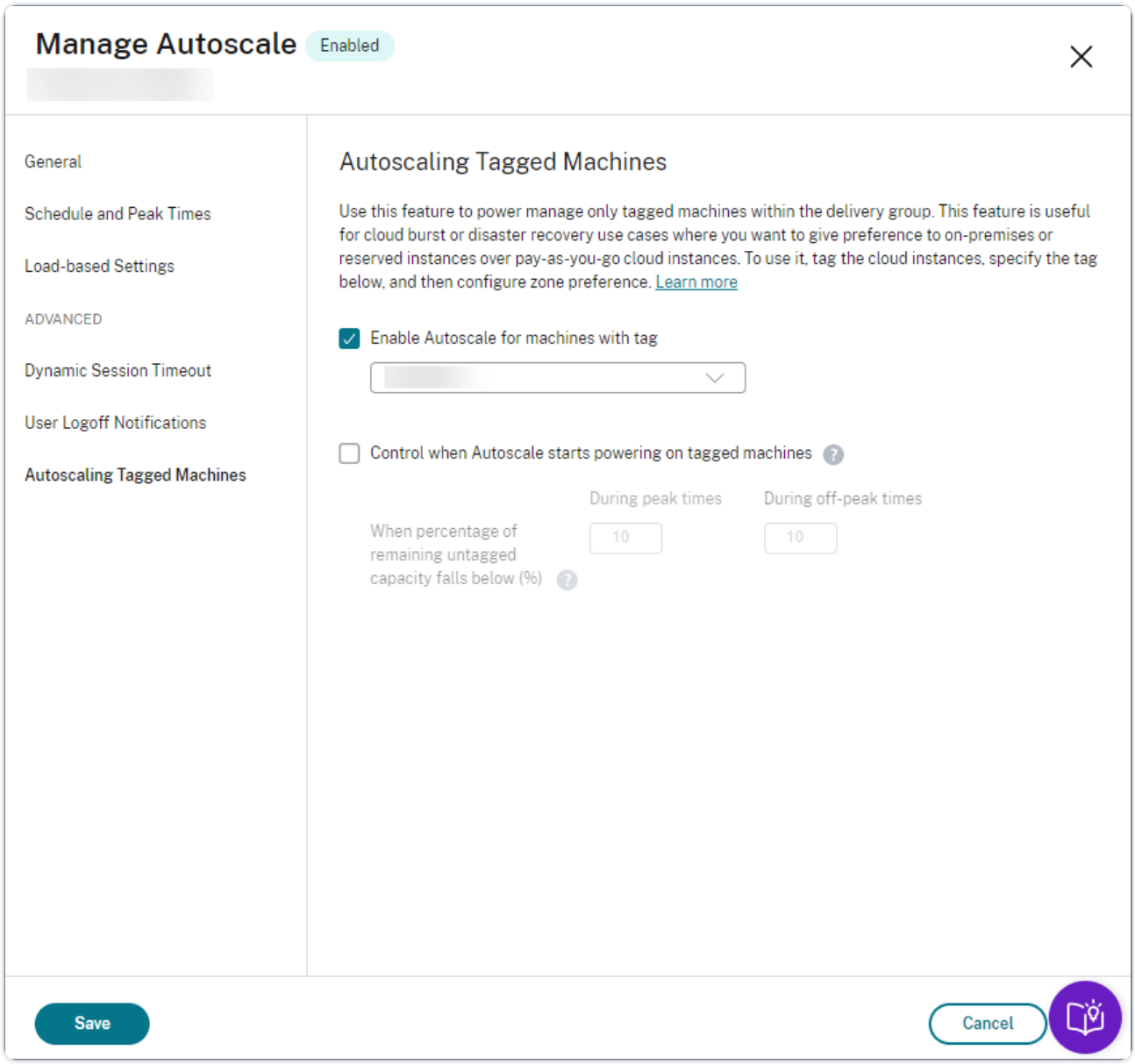
- Se você remover a tag das máquinas aplicáveis sem desmarcar **Habilitar Autoscale para máquinas com tag**, poderá receber um aviso ao abrir o assistente **Gerenciar Autoscale**. A remoção da tag das máquinas pode deixar o Autoscale sem máquinas para gerenciar, pois a tag especificada no Autoscale se tornou inválida. Para resolver o aviso, vá para a página **Máquinas Marcadas com Autoscale**, remova a tag inválida e clique em **Aplicar** para salvar suas alterações.

Controlar quando o Autoscale liga os recursos

Você também pode controlar quando o Autoscale começa a ligar máquinas marcadas com base no uso de máquinas não marcadas. Isso ajuda você a otimizar ainda mais o consumo de suas cargas de trabalho marcadas ou de nuvem pública.

Para fazer isso, conclua as seguintes etapas:

1. Na página **Máquinas Marcadas com Autoscale**, selecione **Controlar quando o Autoscale começa a ligar máquinas marcadas**.
2. Insira a porcentagem de uso de máquina não marcada que você deseja atingir para horários de pico e fora de pico e, em seguida, clique em **Aplicar**. Valores suportados: 0–100.



Dica:

A porcentagem controla quando o Autoscale começa a ligar máquinas marcadas. Quando a porcentagem cai abaixo do limite (padrão, 10%), o Autoscale começa a ligar máquinas marcadas. Quando a porcentagem excede o limite, o Autoscale entra no modo de desligamento. Ao inserir a porcentagem, considere dois cenários:

- Para grupos de entrega de SO de sessão única: O valor é definido como uma porcentagem do número total de máquinas não marcadas em estado ocioso. Exemplo: Você tem 10 máquinas de SO de sessão única não marcadas. Quando apenas uma é deixada sem sessão, o Autoscale começa a ligar uma máquina marcada.

- Para grupos de entrega de SO de múltiplas sessões: O valor é definido como uma porcentagem da capacidade total (em termos de índice de carga) de máquinas não marcadas disponíveis. Exemplo: Você tem 10 máquinas de SO de múltiplas sessões não marcadas. Quando elas estão 90% carregadas, o Autoscale começa a ligar uma máquina marcada.

Usar PowerShell para autoscale de certas máquinas marcadas

Para usar o SDK do PowerShell diretamente, conclua as seguintes etapas:

1. **Criar uma tag.** Use o comando PowerShell New-Brokertag para criar uma tag.
   - Por exemplo: `$managed = New-BrokerTag Managed`. Neste caso, a tag é nomeada "Managed." Para mais informações sobre o comando PowerShell New-Brokertag, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`.
2. **Aplicar a tag às máquinas**. Use o comando PowerShell Get-Brokermachine para aplicar a tag às máquinas em um catálogo que você deseja que o Autoscale gerencie o consumo de energia.
   - Por exemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. Neste caso, o catálogo é nomeado "cloud."
   - Para mais informações sobre o comando PowerShell Get-Brokermachine, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`.

   Observação:

   Você pode adicionar novas máquinas ao catálogo após aplicar a tag. A tag *NÃO* é aplicada automaticamente a essas novas máquinas.
3. **Adicionar máquinas marcadas ao grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia.** Use o comando PowerShell Get-BrokerDesktopGroup para adicionar uma restrição de tag ao grupo de entrega que contém as máquinas (em outras palavras, "restringir inicializações a máquinas com a tag X").

- Por exemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. Neste caso, o UID do Grupo de Entrega é 1.
- Para mais informações sobre o comando PowerShell Get-BrokerDesktopGroup, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, use o comando PowerShell Get-BrokerDesktopGroup.

Exemplo: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`. Neste caso, o UID do grupo de entrega é 1.

> **Observação:**
>
> Máquinas sem tag reiniciam automaticamente depois que os usuários as desligam. Esse comportamento garante que elas se tornem disponíveis para manipular cargas de trabalho mais cedo. Isso pode ser ativado ou desativado por grupo de desktop usando a propriedade `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do catálogo de máquinas**. Existem dois catálogos de máquinas (C1 e C2).
  - O Catálogo C1 contém 5 máquinas (M1 a M5) que são locais nas implantações on-premises.
  - O Catálogo C2 contém 5 máquinas (M6 a M10) que são remotas nas implantações em nuvem.
- **Restrição de tag**. Uma tag chamada "Cloud" é criada e aplicada às máquinas M6 a M10 no catálogo C2.
- **Configuração de zona**. Duas zonas (Z1 e Z2) são criadas.
  - A Zona Z1, que contém o catálogo C1, corresponde às implantações locais.
  - A Zona Z2, que contém o catálogo C2, corresponde às implantações em nuvem.

- **Configuração do grupo de entrega**
  - O grupo de entrega contém 10 máquinas (M1 a M10), 5 máquinas dos catálogos C1 (M1 a M5) e 5 do catálogo C2 (M6 a M10).
  - As máquinas M1 a M5 são ligadas manualmente e permanecem ligadas durante todo o agendamento.
- **Configuração do Autoscale**
  - O buffer de capacidade é definido como 10%.
  - O Autoscale gerencia apenas máquinas com a tag "Cloud". Neste caso, o Autoscale gerencia as máquinas em nuvem M6 a M10.
- **Configuração de aplicativo ou desktop publicado**. As preferências de zona são configuradas para os desktops publicados (por exemplo), onde a Zona Z1 é preferida em relação à Zona Z2 para uma solicitação de inicialização do usuário.
  - A Zona Z1 é configurada como a zona preferencial (zona inicial) para os desktops publicados.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. As sessões de usuário aumentam ainda mais até que todas as máquinas on-premises disponíveis sejam consumidas.
4. Mais sessões de usuário são iniciadas.
5. A sessão de usuário diminui devido ao encerramento da sessão.
6. A sessão de usuário diminui ainda mais até que a carga da sessão seja tratada apenas por máquinas on-premises.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - As máquinas on-premises M1 a M5 estão todas ligadas.
  - Uma máquina na nuvem (por exemplo, M6) está ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina é ligada.

    - O valor do índice de carga de todas as máquinas ligadas (M1 a M6) está em uma carga base (índice de carga igual a 0).

- Usuários fazem logon
    - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas por carga entre essas máquinas on-premises.
    - 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 base.
- Usuários aumentam a carga, consumindo todos os recursos on-premises
    - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas entre essas máquinas locais.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 permanece em uma carga de linha de base.
- Mais um usuário faz logon
    - A sessão excede a preferência de zona e é direcionada para ser hospedada na máquina em nuvem M6.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 aumenta e não está mais em uma carga de linha de base. Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M7) para atender à demanda devido ao buffer de capacidade configurado. Observe que pode levar algum tempo para ligar a máquina M7. Portanto, pode haver um atraso até que a máquina M7 esteja pronta.
- Mais usuários fazem logon
    - As sessões são direcionadas para serem hospedadas na máquina M6.
    - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
    - O valor do índice de carga da máquina ligada M6 aumenta ainda mais, mas a capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
    - O valor do índice de carga da máquina ligada M7 permanece em uma carga de linha de base.

- Ainda mais usuários fazem logon
  - Depois que a máquina M7 estiver pronta, as sessões são direcionadas para serem hospedadas nas máquinas M6 e M7 e são balanceadas entre essas máquinas.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina M7 não está mais em uma carga de linha de base.
  - O valor do índice de carga das máquinas ligadas (M6 e M7) aumenta.
  - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
- A carga da sessão do usuário diminui devido ao encerramento da sessão
  - Depois que os usuários saem de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M7 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas em nuvem (M6 a M7) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina (por exemplo, M7), a menos que novas alterações ocorram; por exemplo, a carga do usuário aumenta novamente ou outras máquinas em nuvem se tornam as menos carregadas.
- A carga da sessão do usuário diminui ainda mais até que uma ou mais máquinas em nuvem não sejam mais necessárias
  - Depois que todas as sessões na máquina M7 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M7.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) pode cair para um nível abaixo de 10.000.
  - O valor do índice de carga da máquina ligada (M6) diminui.
- A sessão do usuário diminui ainda mais até que nenhuma máquina em nuvem seja necessária.
  - Mesmo que não haja sessões de usuário na máquina M6, o Autoscale não a desliga porque ela está reservada como capacidade sobressalente.
  - O Autoscale mantém a máquina em nuvem restante M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário que está chegando.

- As sessões não são direcionadas para serem hospedadas na máquina M6 enquanto as máquinas locais tiverem capacidade disponível.

Notificações de logoff do usuário

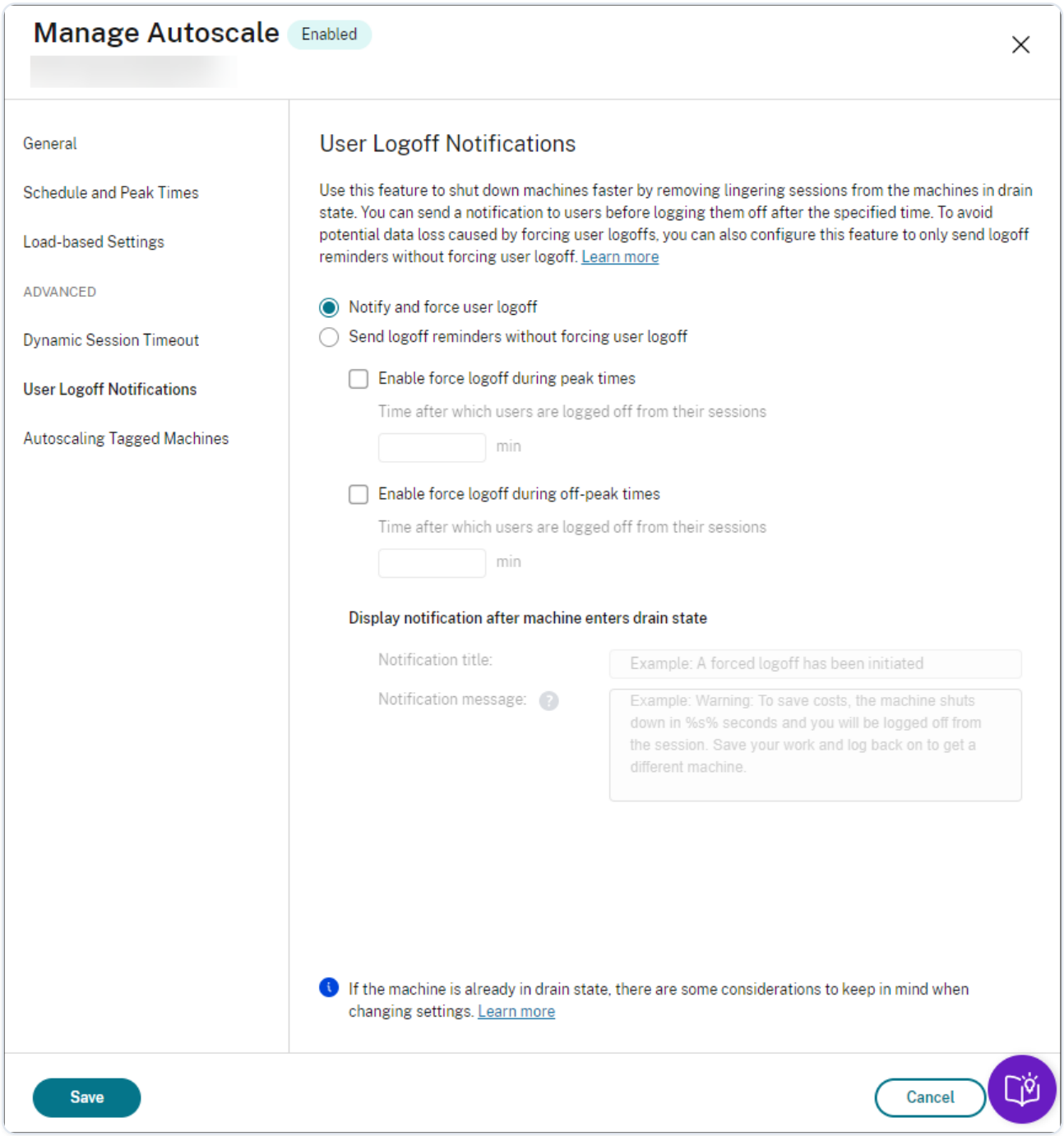
> **Importante:**
>
> Este recurso está disponível apenas na interface do usuário do Autoscale™ para grupos de entrega baseados em aplicativos de várias sessões.
>
> Para melhor alcançar a economia de custos, o Autoscale permite que você force o logoff de sessões persistentes. Ele faz isso permitindo que você envie uma notificação personalizada aos usuários e especifique um período de carência após o qual as sessões são forçadas a fazer logoff. Isso é feito apenas para máquinas em estado de drenagem e não para todas as máquinas ligadas. Para evitar a potencial perda de dados causada pelo logoff forçado de usuários, você pode configurar este recurso para apenas enviar lembretes de logoff sem forçar o logoff do usuário.

Você tem as duas opções a seguir:

- **Notificar e forçar o logoff do usuário**
- **Enviar lembretes de logoff sem forçar o logoff do usuário**

Notificar e forçar o logoff do usuário

Se selecionado, o Autoscale desconecta os usuários de suas sessões após os horários especificados abaixo.



Habilitar logoff forçado durante horários de pico. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de pico quando o tempo especificado expira.

Habilitar logoff forçado durante horários de menor movimento. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de menor movimento quando o tempo especificado expira.

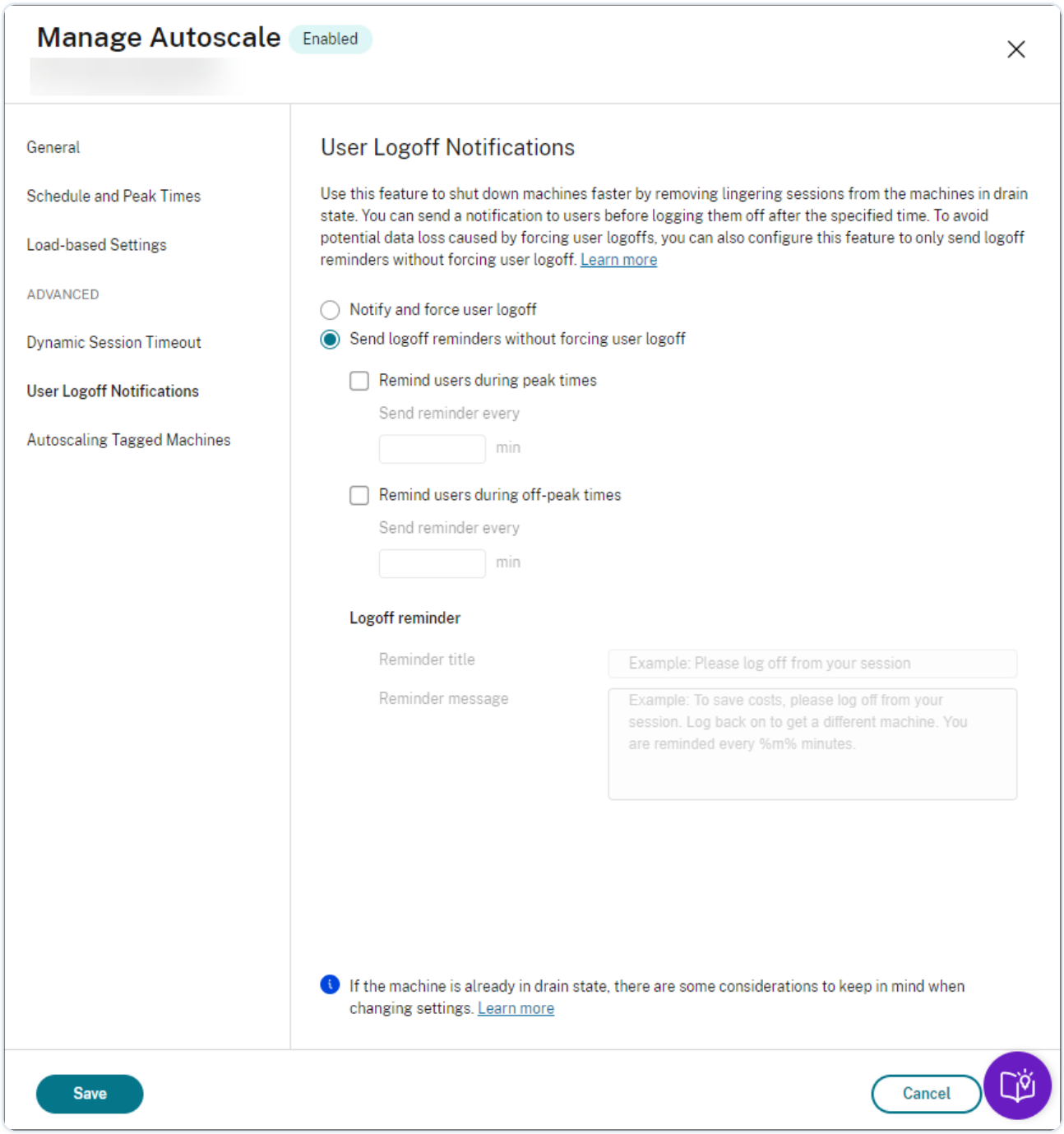
Exibir notificação depois que a máquina entrar no estado de drenagem. Permite que você envie notificações aos usuários depois que a máquina deles entrar no estado de drenagem.

- **Título da notificação**. Permite que você especifique um título para a notificação a ser enviada aos usuários. Exemplo: `A forced logoff has been initiated.`.

- **Mensagem de notificação**. Permite especificar o conteúdo da notificação a ser enviada aos usuários. Você pode usar %s% ou %m% como variáveis para indicar o tempo especificado na mensagem. Para expressar o tempo em segundos, use %s%. Para expressar o tempo em minutos, use %m%. Exemplo: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

Enviar lembretes de logoff sem forçar o logoff do usuário

Se selecionado, os usuários receberão um lembrete para fazer logoff de sua máquina depois que ela entrar no estado de drenagem. Este lembrete pode ser configurado para ser enviado no intervalo especificado abaixo.



Lembrar usuários durante horários de pico. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de pico a cada X minutos (X denota o tempo especificado).

Lembrar usuários durante horários de menor movimento. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de menor movimento a cada X minutos (X denota o tempo especificado).

Lembrete de logoff. Permite configurar o lembrete enviado aos usuários depois que a máquina deles entra no estado de drenagem.

- **Título do lembrete**. Permite especificar um título para o lembrete a ser enviado aos usuários. Exemplo: `Please log off from your session`.
- **Mensagem do lembrete**. Permite especificar uma mensagem a ser enviada aos usuários. Exemplo: `Please log off from your session and log back on to save costs`.

Considerações

Se a máquina já estiver em estado de drenagem, considere o seguinte ao alterar as configurações:

- Se você alterar a configuração de **Enviar lembretes de logoff sem forçar o logoff do usuário** para **Notificar e forçar o logoff do usuário**, a nova configuração entra em vigor imediatamente.
- Se você alterar a configuração de **Notificar e forçar o logoff do usuário** para **Enviar lembretes de logoff sem forçar o logoff do usuário**, a nova configuração não entrará em vigor até a próxima vez que a máquina entrar no estado de drenagem. O usuário ainda é forçado a fazer logoff.

Comandos do SDK do PowerShell do Broker

Você pode configurar o Autoscale para grupos de entrega usando o SDK do PowerShell do Broker. Para configurar o Autoscale usando comandos do PowerShell, você deve usar a versão 7.21.0.12 ou posterior do SDK do PowerShell. Para obter mais informações sobre os SDKs do PowerShell, consulte SDKs e APIs.

Set-BrokerDesktopGroup

Desabilita ou habilita um BrokerDesktopGroup existente ou altera suas configurações. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

Exemplos

Consulte os exemplos a seguir para obter detalhes sobre como usar os cmdlets do PowerShell.

Habilitar Autoscale™

- Suponha que você queira habilitar o Autoscale para o grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

Configurar o buffer de capacidade separadamente para horários de pico e fora de pico

- Suponha que você queira definir o buffer de capacidade para 20% para horários de pico e 10% para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

Configurar a configuração de **tempo limite quando desconectado**

- Suponha que você queira definir o valor de **tempo limite quando desconectado** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

Configurar a configuração de **tempo limite quando desconectado**

- Suponha que você queira definir o valor de **tempo limite quando desconectado** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Configurar a configuração de **atraso de desligamento**

- Suponha que você queira definir o atraso de desligamento para 15 minutos para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

Configurar um período de tempo durante o qual o atraso de desligamento não entra em vigor

- Suponha que você queira que o atraso de desligamento entre em vigor até que 30 minutos tenham decorrido para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`.

Configurar a definição de **custo da instância da máquina**

- Suponha que você queira definir o custo da instância da máquina por hora para 0,2 dólares para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

Cria um BrokerPowerTimeScheme para um grupo de entrega. Para obter mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`.

Exemplo

Suponha que você queira criar um esquema de tempo de energia para um grupo de entrega cujo valor UID é 3. O novo esquema abrange o fim de semana, segunda e terça-feira. O período das 8:00 AM às 6:30 PM é definido como horários de pico para os dias incluídos no esquema. Para horários de pico, o tamanho do pool (o número de máquinas mantidas ligadas) é 20. Para horários fora de pico, é 5. Você pode usar o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

Parâmetros para tempos limite de sessão dinâmicos

Os seguintes cmdlets do SDK do Broker PowerShell foram estendidos para tempos limite de sessão dinâmicos, suportando 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. Esta propriedade tem um valor padrão de 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento para o grupo de entrega apenas durante o horário de pico.
- **DisconnectOffPeakIdleSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante o horário fora de pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário fora de pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário fora de pico.
- **LogoffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de pico.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de não pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de não pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de não pico.

Exemplo

Suponha que você queira definir o tempo limite de sessão ociosa para 3.600 segundos durante os horários de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

Fazer isso desconecta as sessões que estiveram ociosas por mais de 1 hora fora do horário de pico para o grupo de desktop cujo nome é "MyDesktop".

Citrix Insight Services

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios. Seus recursos de instrumentação e telemetria permitem que usuários técnicos (clientes, parceiros e engenheiros) autodiagnostiquem e corrijam problemas e otimizem

seus ambientes. Para obter detalhes e as informações mais recentes sobre o CIS e como ele funciona, consulte `<https://cis.citrix.com>` (credenciais de conta Citrix necessárias).

Todas as informações carregadas para a Citrix são usadas para fins de solução de problemas e diagnóstico, e para melhorar a qualidade, confiabilidade e desempenho dos produtos, sujeitas a:

- Política de Serviços do Citrix Insight em `<https://cis.citrix.com/legal>`
- Política de Privacidade da Citrix em `<https://www.cloud.com/privacy-policy>`

Esta versão do Citrix Virtual Apps and Desktops™ oferece suporte às seguintes tecnologias.

- Análise de instalação e atualização do Citrix Virtual Apps and Desktops
- Programa de Melhoria da Experiência do Cliente Citrix (CEIP)
- Citrix Call Home
- Citrix Scout

Além (e separadamente) do CIS e do Citrix Analytics: o Google Analytics é coletado (e posteriormente carregado) automaticamente quando você instala (ou atualiza) o Studio. Após instalar o Studio, você pode alterar essa configuração com a chave de registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. Um valor de 1 habilita a coleta e o upload, 0 desabilita a coleta e o upload.

Análise de instalação e atualização

Ao usar o instalador completo do produto para implantar ou atualizar componentes do Citrix Virtual Apps and Desktops, informações anônimas sobre o processo de instalação são coletadas e armazenadas na máquina onde você está instalando/atualizando o componente. Esses dados são usados para ajudar a Citrix a melhorar as experiências de instalação de seus clientes.

As informações são armazenadas localmente em `%ProgramData%\Citrix\CTQs`.

O upload automático desses dados é habilitado por padrão nas interfaces gráfica e de linha de comando do instalador completo do produto.

- Você pode alterar o valor padrão em uma configuração de registro. Se você alterar a configuração de registro antes de instalar/atualizar, esse valor será usado quando você usar o instalador completo do produto.
- Você pode substituir a configuração padrão se instalar/atualizar com a interface de linha de comando, especificando uma opção com o comando.

Controlar uploads automáticos:

- Configuração de registro que controla o upload automático de análises de instalação/atualização (padrão = 1):
  - Local: `HKLM:\Software\Citrix\MetaInstall`
  - Nome: SendExperienceMetrics
  - Valor: 0 = desabilitado, 1 = habilitado
- Usando o PowerShell, o seguinte cmdlet desabilita o upload automático de análises de instalação/atualização:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- Para desabilitar uploads automáticos com o comando XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, inclua a opção `/disableexperiencemetrics`.

  Para habilitar uploads automáticos com o comando XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, inclua a opção `/sendexperiencemetrics`.

Programa de Melhoria da Experiência do Cliente Citrix

Quando você participa do Programa de Melhoria da Experiência do Cliente Citrix (CEIP), estatísticas anônimas e informações de uso são enviadas à Citrix para ajudar a Citrix a melhorar a qualidade e o desempenho dos produtos Citrix. Para obter mais informações, consulte https://more.citrix.com/XD-CEIP.

Inscrição durante a criação ou atualização do Site

Você é automaticamente inscrito no CEIP ao criar um Site (após instalar o primeiro Delivery Controller™). O primeiro upload de dados ocorre aproximadamente sete dias após a criação do Site.

Você pode interromper sua participação a qualquer momento após criar o Site. Selecione o nó **Configurações** no painel esquerdo do Web Studio e desative a configuração **Programa de Melhoria da Experiência do Cliente Citrix**.

Ao atualizar uma implantação do Citrix Virtual Apps and Desktops:

- Se você atualizar de uma versão que não suportava o CEIP, será perguntado se deseja participar.

- Se você atualizar de uma versão que suportava o CEIP e a participação estava ativada, o CEIP é ativado no Site atualizado.
- Se você atualizar de uma versão que suportava o CEIP e a participação estava desativada, o CEIP é desativado no Site atualizado.
- Se você atualizar de uma versão que suportava o CEIP e a participação é desconhecida, será perguntado se deseja participar.

As informações coletadas são anônimas, portanto, não podem ser visualizadas depois de serem carregadas para o Citrix Insight Services.

Inscrição ao instalar um VDA

Por padrão, você é automaticamente inscrito no CEIP ao instalar um VDA do Windows. Você pode alterar esse padrão em uma configuração de registro. Se você alterar a configuração de registro antes de instalar o VDA, esse valor será usado.

Configuração de registro que controla a inscrição automática no CEIP (padrão = 1):

Local: HKLM: `\\Software\Citrix\Telemetry\CEIP` Nome: Enabled Valor: 0 = desativado, 1 = ativado

Por padrão, a propriedade `Enabled` está oculta no registro. Quando não especificada, o recurso de upload automático é ativado.

Usando o PowerShell, o seguinte cmdlet desativa a inscrição no CEIP:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

Os pontos de dados de tempo de execução coletados são periodicamente gravados como arquivos em uma pasta de saída (padrão %programdata%/Citrix/VdaCeip).

O primeiro upload de dados ocorre aproximadamente sete dias após a instalação do VDA.

Inscrição ao instalar outros produtos e componentes

Você também pode participar do CEIP ao instalar produtos, componentes e tecnologias Citrix relacionados, como Citrix Provisioning™, AppDNA, Citrix License Server, Citrix Workspace™ app para Windows, Universal Print Server e Session Recording. Consulte a documentação deles para obter detalhes sobre a instalação e os valores padrão de participação.

Citrix Call Home

Ao instalar determinados componentes e recursos no Citrix Virtual Apps and Desktops, é oferecida a oportunidade de participar do Citrix Call Home. O Call Home coleta dados de diagnóstico e, em seguida, carrega periodicamente pacotes de telemetria contendo esses dados diretamente para o Citrix Insight Services (via HTTPS na porta padrão 443) para análise e solução de problemas.

No Citrix Virtual Apps and Desktops, o Call Home é executado como um serviço em segundo plano sob o nome Citrix Telemetry Service. Para obter mais informações, consulte https://more.citrix.com/XD-CALLHOME.

A funcionalidade de agendamento do Call Home também está disponível no Citrix Scout. Para obter detalhes, consulte Citrix Scout.

O que é coletado

O rastreamento do Citrix Diagnostic Facility (CDF) registra informações que podem ser úteis para a solução de problemas. O Call Home coleta um subconjunto de rastreamentos CDF que podem ser úteis ao solucionar falhas comuns, por exemplo, registros de VDA e inicializações de aplicativos/desktops. Essa tecnologia é conhecida como rastreamento sempre ativo (AOT). Os logs AOT são salvos em disco em C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT.

O Call Home não coleta nenhuma outra informação de Event Tracing for Windows (ETW), nem pode ser configurado para fazê-lo.

O Call Home também coleta outras informações, como:

- Registros criados pelo Citrix Virtual Apps and Desktops em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informações do Windows Management Instrumentation (WMI) no namespace Citrix.
- Lista de processos em execução.
- Dumps de falha de processos Citrix que são armazenados em %PROGRAM `DATA%\Citrix\CDF`.
- Informações de instalação e atualização. Isso pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront™, logs de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

As informações de rastreamento são compactadas à medida que são coletadas. O Citrix Telemetry Service retém um máximo de 10 MB de informações de rastreamento recentes compactadas, com um limite de tempo máximo de oito dias.

- A compactação de dados permite que o Call Home ocupe pouco espaço no VDA.
- Os rastreamentos são mantidos na memória para evitar IOPs em máquinas provisionadas.
- O buffer de rastreamento usa um mecanismo circular para reter rastreamentos na memória.

O Call Home coleta os principais pontos de dados listados em Pontos de dados chave do Call Home.

Resumo de configuração e gerenciamento

Você pode se inscrever no Call Home ao usar o assistente de instalação do produto completo ou posteriormente, usando cmdlets do PowerShell. Ao se inscrever, por padrão, os diagnósticos são coletados e carregados para a Citrix todo domingo, aproximadamente às 3:00 AM, horário local. O upload é randomizado com um intervalo de duas horas a partir do horário especificado. Isso significa que um upload usando o agendamento padrão ocorre entre 3:00 AM e 5:00 AM.

Se você não quiser carregar informações de diagnóstico de forma agendada (ou se quiser alterar um agendamento), você pode usar cmdlets do PowerShell para coletar e carregar diagnósticos manualmente ou armazená-los localmente.

Ao se inscrever em uploads agendados do Call Home e ao carregar manualmente informações de diagnóstico para a Citrix, você fornece credenciais de conta Citrix ou Citrix Cloud™. A Citrix troca as credenciais por um token de upload que é usado para identificar o cliente e carregar os dados. As credenciais não são salvas.

Quando um upload ocorre, uma notificação é enviada por e-mail para o endereço associado à conta Citrix.

Se você habilitar o Call Home ao instalar um componente, você pode desativá-lo mais tarde.

Pré-requisitos

- A máquina deve estar executando o PowerShell 3.0 ou posterior.
- O Serviço de Telemetria Citrix deve estar em execução na máquina.
- A variável de sistema `PSModulePath` deve ser definida para o caminho de instalação da Telemetria, por exemplo, `C:\Program Files\Citrix\Telemetry Service\`.

Habilitar o Call Home durante a instalação do componente

Durante a instalação ou atualização do VDA: Ao instalar ou atualizar um Virtual Delivery Agent usando a interface gráfica no instalador completo do produto, você será perguntado se deseja participar do Call Home. Existem duas opções:

- Participar do Call Home.
- Não participar do Call Home.

Se você estiver atualizando um VDA e já estava inscrito no Call Home, essa página do assistente não aparecerá.

Durante a instalação ou atualização do Controller: Ao instalar ou atualizar um Delivery Controller usando a interface gráfica, você será perguntado se deseja participar do Call Home. Existem três opções:

Ao instalar um Controller, você não pode configurar informações na página Call Home do assistente de instalação se esse servidor tiver uma GPO do Active Directory com a configuração de política "Fazer logon como um serviço" aplicada. Para obter detalhes, consulte CTX218094.

Se você estiver atualizando um Controller e já estava inscrito no Call Home, não será perguntado sobre a participação.

Cmdlets do PowerShell

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Para usar um servidor proxy para uploads, consulte Configurar um servidor proxy.

- **Habilitar uploads agendados:** As coletas de diagnóstico são automaticamente carregadas para a Citrix. Se você não inserir cmdlets adicionais para um agendamento personalizado, o agendamento padrão será usado.

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  Para confirmar que os uploads agendados estão habilitados, digite `Get-CitrixCallHomeGet-CitrixCallHome`. Se habilitado, o retorno é `IsEnabled=True` e `IsMasterImage=False`.

- **Habilitar uploads agendados para máquinas criadas a partir de uma imagem mestre:** Habilitar uploads agendados em uma imagem mestre elimina a necessidade de configurar cada máquina criada no catálogo de máquinas.

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

Para confirmar que os uploads agendados estão habilitados, digite **Get-CitrixCallHome**. Se habilitado, o retorno é `IsEnabled=True` e `IsMasterImage=True`.

- **Criar um agendamento personalizado:** Crie um agendamento diário ou semanal para coletas e uploads de diagnóstico.

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

Exemplos:

O cmdlet a seguir cria um agendamento para agrupar e carregar dados às 22:20 todas as noites. O parâmetro Hours usa um relógio de 24 horas. Quando o valor do parâmetro `UploadFrequency` é Daily, o parâmetro `DayOfWeek` é ignorado, se especificado.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Para confirmar o agendamento, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, ele retorna `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`.

O cmdlet a seguir cria um agendamento para agrupar e carregar dados às 10:20 de toda quarta-feira à noite.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

Para confirmar o agendamento, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, ele retorna `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`.

Desabilitar Call Home

Você pode desabilitar o Call Home usando um cmdlet do PowerShell ou através do Citrix Scout.

Os logs AOT são coletados e salvos em disco, mesmo quando os uploads agendados do Call Home estão desabilitados. (Quando os uploads agendados estão desabilitados, os logs AOT não

são carregados automaticamente para a Citrix.) Você pode desabilitar a coleta e o armazenamento local dos logs AOT.

Desabilitar Call Home com PowerShell

Após executar o cmdlet a seguir, os dados de diagnóstico não serão carregados para a Citrix automaticamente. (Você ainda pode carregar dados de diagnóstico usando o Citrix Scout ou cmdlets do PowerShell de telemetria.)

```
Disable-CitrixCallHome
```

Para confirmar que o Call Home está desabilitado, digite `Get-CitrixCallHome`. Se desabilitado, o retorno é `IsEnabled=False` e `IsMasterImage=False`.

Desabilitar um agendamento de coleta usando o Citrix Scout

Para desabilitar um agendamento de coleta de diagnóstico usando o Citrix Scout, siga as orientações em Agendar coletas. Na etapa 3, clique em **Desativar** para cancelar o agendamento para as máquinas selecionadas.

Desabilitar a coleta de logs AOT

Após executar o cmdlet a seguir (com o campo `Enabled` definido como `false`), os logs AOT não serão coletados.

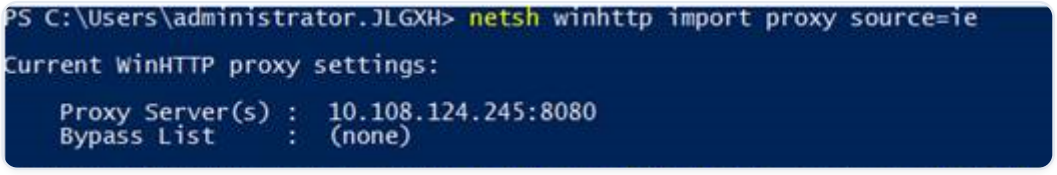
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

O parâmetro `Listen` contém argumentos no formato JSON.

Configurar um servidor proxy para uploads do Call Home

Conclua as seguintes tarefas na máquina onde o Call Home está habilitado. Os diagramas de exemplo no procedimento a seguir contêm o endereço do servidor e a porta 10.158.139.37:3128. Suas informações serão diferentes.

1. Adicione as informações do servidor proxy em seu navegador. No Internet Explorer, selecione **Opções da Internet \> Conexões \> Configurações da LAN**. Selecione **Usar um servidor proxy para sua LAN**" e insira o endereço do servidor proxy e o número da porta.
2. No PowerShell, execute `netsh winhttp import proxy source=ie`.



3. Usando um editor de texto, edite o arquivo de configuração TelemetryService.exe, que está localizado em `C:\Program Files\Citrix\Telemetry Service`. Adicione as informações mostradas na caixa vermelha.



4. Reinicie o Serviço de Telemetria.

Execute os cmdlets do Call Home no PowerShell.

Coletar e carregar informações de diagnóstico manualmente

Você pode usar o site do CIS para carregar um pacote de informações de diagnóstico para o CIS. Você também pode usar cmdlets do PowerShell para coletar e carregar informações de diagnóstico para o CIS.

Para carregar um pacote usando o site do CIS:

1. Faça logon no Citrix Insight Services usando suas credenciais de conta Citrix.
2. Selecione **Meu Espaço de Trabalho**.
3. Selecione **Healthcheck** e, em seguida, navegar até o local dos seus dados.

O CIS oferece suporte a vários cmdlets do PowerShell que gerenciam uploads de dados. Esta documentação aborda os cmdlets para dois casos comuns:

- Use o cmdlet `Start-CitrixCallHomeUpload` para coletar e carregar manualmente um pacote de informações de diagnóstico para o CIS. (O pacote não é salvo localmente.)
- Use o cmdlet `Start-CitrixCallHomeUpload` para coletar dados manualmente e armazenar um pacote de informações de diagnóstico localmente. Isso permite que você visualize os dados. Mais tarde, use o cmdlet `Send-CitrixCallHomeBundle` para carregar manualmente

uma cópia desse pacote para o CIS. (Os dados que você salvou originalmente permanecem localmente.)

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Ao inserir um cmdlet para carregar dados para o CIS, você será solicitado a confirmar o upload. Se o cmdlet expirar antes que o upload seja concluído, verifique o status do upload no log de eventos do sistema. A solicitação de upload pode ser rejeitada se o serviço já estiver realizando um upload.

Coletar dados e carregar pacote para o CIS:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string] [-Description string] [-IncidentTime string] [-SRNumber string] [-Name string] [-UploadHeader string] [-AppendHeaders string] [-Collect string] [<CommonParameters>]
```

Coletar dados e salvá-los localmente:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-Description string] [-IncidentTime string] [-SRNumber string] [-Name string] [-UploaderHeader string] [-AppendHeaders string] [-Collect strings] [<CommonParameters>]
```

Os seguintes parâmetros são válidos:

- **Credential:** Direciona o upload para o CIS.
- **InputPath:** Local do arquivo zip a ser incluído no pacote. Este pode ser um arquivo adicional que o Suporte Citrix solicita. Certifique-se de incluir a extensão .zip.
- **OutputPath:** Local onde as informações de diagnóstico são salvas. Este parâmetro é obrigatório ao salvar dados do Call Home localmente.
- **Description and Incident Time:** Informações de formato livre sobre o upload.
- **SRNumber:** Número do incidente do Suporte Técnico Citrix.
- **Name:** Nome que identifica o pacote.
- **UploadHeader:** String formatada em JSON especificando os cabeçalhos de upload carregados para o CIS.

- **AppendHeaders:** String formatada em JSON especificando os cabeçalhos anexados carregados para o CIS.
- **Coletar:** string formatada em JSON especificando quais dados coletar ou omitir, no formato {'collector':{'enabled':Boolean}}, onde Boolean é true ou false. Os valores de coletor válidos são:
  - 'WMI'
  - 'processo'
  - 'registro'
  - 'relatório de falhas'
  - 'rastreamento'
  - 'arquivo'
  - 'MSI'
  - 'dados locais'
  - 'dados do site'
  - 'SFB'

  Por padrão, todos os coletores, exceto 'sfb', estão habilitados.

  O coletor 'sfb' foi projetado para ser usado sob demanda para diagnosticar problemas do Skype for Business. Além do parâmetro 'enabled', o coletor 'sfb' oferece suporte aos parâmetros 'account' e 'accounts' para especificar usuários de destino. Use um dos formatos:
  - "-Collect "`{'sfb':{'account':'domain\\user1'}}`"
  - "-Collect "{'sfb':{'accounts':}}"
- **Parâmetros Comuns:** Consulte a ajuda do PowerShell.

Carregar dados que foram salvos localmente anteriormente:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string
[<CommonParameters>]
```

O parâmetro `Path` especifica o local do pacote salvo anteriormente.

Exemplos:

O cmdlet a seguir solicita o upload de dados do Call Home (excluindo dados do coletor WMI) para o CIS. Esses dados se referem a falhas de registro de VDAs do Citrix Provisioning, que foram observadas às 14h30 para o caso de Suporte Citrix 123456. Além dos dados do Call Home, o arquivo "`c:\Diagnostics\ExtraData.zip`" é incorporado ao pacote carregado.

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

O cmdlet a seguir salva dados do Call Home relacionados ao caso de Suporte Citrix 223344, observado às 8h15. Os dados são salvos no arquivo mydata.zip em um compartilhamento de rede. Além dos dados do Call Home, o arquivo "`c:\Diagnostics\ExtraData.zip`" será incorporado ao pacote salvo.

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

O cmdlet a seguir carrega o pacote de dados que você salvou anteriormente.

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

Citrix Scout

Introdução

O Citrix Scout coleta diagnósticos e executa verificações de integridade. Você pode usar os resultados para manter sua implantação do Citrix Virtual Apps and Desktops™. A Citrix oferece análise abrangente e automatizada de coletas de diagnóstico por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com a orientação do Suporte Citrix.

Você pode carregar arquivos de coleta para a Citrix para análise e orientação do Suporte Citrix. Ou, você pode salvar uma coleta localmente para sua própria revisão e, em seguida, carregar o arquivo de coleta para a Citrix para análise.

O Scout oferece os seguintes procedimentos:

- **Coletar:** Executa uma coleta de diagnóstico única em máquinas que você seleciona em um site. Você pode então carregar o arquivo para a Citrix ou salvá-lo localmente.
- **Rastrear e Reproduzir:** Inicia um rastreamento manual nas máquinas que você seleciona. Em seguida, você recria problemas nessas máquinas. Após recriar o problema, o rastreamento é interrompido. O Scout então coleta outros diagnósticos e carrega o arquivo para a Citrix, ou salva o arquivo localmente.
- **Agendar:** Agenda coletas de diagnóstico para ocorrerem diariamente ou semanalmente em um horário especificado nas máquinas que você seleciona. O arquivo é automaticamente carregado para a Citrix.
- **Verificação de Integridade:** Executa verificações que avaliam a integridade e a disponibilidade do site e seus componentes. Você pode executar verificações de integridade para Delivery Controllers, Virtual Delivery Agents (VDAs), servidores StoreFront™ e Citrix License Servers. Se problemas forem encontrados durante as verificações, o Scout fornece um relatório detalhado. Cada vez que o Scout inicia, ele verifica se há scripts de verificação de integridade atualizados. Se novas versões estiverem disponíveis, o Scout as baixa automaticamente, para uso na próxima vez que as verificações de integridade forem executadas.

> **Observação:**
>
> Os procedimentos **Rastrear e Reproduzir**, **Agendar** e **Verificação de Integridade** não estão atualmente disponíveis para Linux VDA.

> A interface gráfica descrita neste artigo é a principal forma de usar o Scout. Alternativamente, você pode usar o PowerShell para configurar coletas e uploads de diagnóstico únicos ou agendados. Consulte Call Home.

Onde executar o Scout:

- Em uma implantação local, execute o Scout a partir de um Delivery Controller™ para capturar diagnósticos ou executar verificações em um ou mais Virtual Delivery Agents (VDAs), Delivery

Controllers, servidores StoreFront e License Servers. Você também pode executar o Scout a partir de um VDA para coletar diagnósticos locais.

- Em um ambiente Citrix Cloud que usa Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), execute o Scout a partir de um VDA para coletar diagnósticos locais.

O log para o aplicativo Scout é armazenado em `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Este arquivo pode ser usado para solução de problemas.

O que é coletado

Os diagnósticos coletados pelo Scout incluem arquivos de log de rastreamento do Citrix Diagnostic Facility (CDF). Um subconjunto de rastreamentos CDF chamado Always-on Tracing (AOT) também está incluído. As informações AOT podem ser úteis ao solucionar problemas comuns, como registros de VDA e inicializações de aplicativos/desktops. Nenhuma outra informação de Event Tracing for Windows (ETW) é coletada.

A coleta inclui:

- Entradas de registro criadas pelo Citrix Virtual Apps and Desktops em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informações do Windows Management Instrumentation (WMI) no **namespace Citrix**.
- Processos em execução.
- Dumps de falha de processos Citrix que são armazenados em `%PROGRAMDATA%\Citrix\CDF`.
- Informações de política Citrix, em formato CSV.
- Informações de instalação e atualização. A coleta pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront, logs de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

Sobre as informações de rastreamento:

- As informações de rastreamento são compactadas à medida que são coletadas, mantendo uma pequena pegada na máquina.
- Em cada máquina, o Serviço de Telemetria Citrix mantém informações de rastreamento recentes compactadas por um máximo de oito dias.

- A partir do Citrix Virtual Apps and Desktops 7 1808, os rastreamentos AOT são salvos no disco local por padrão. (Em versões anteriores, os rastreamentos eram mantidos na memória.) Caminho padrão = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partir do Citrix Virtual Apps and Desktops 7 1811, os rastreamentos AOT salvos em compartilhamentos de rede são coletados com outros diagnósticos.
- Você pode modificar o tamanho máximo (padrão = 10 MB) e a duração da fatia, usando o cmdlet `Enable-CitrixTrace` ou a string de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Os rastreamentos são anexados ao arquivo até que o arquivo atinja 10% de `MaxSize`.

Para uma lista dos pontos de dados que o Scout coleta, consulte Pontos de dados chave do Call Home.

Configuração do Scout

O Scout pode ser configurado para funcionar em VDAs Linux. Para obter mais informações sobre VDA Linux e telemetria, consulte Integrar com o Serviço de Telemetria Citrix

O VDA Linux pode alterar automaticamente a porta do socket `ctxtelemetry` ou a porta para o serviço de telemetria. Se isso acontecer, você deve configurar a porta manualmente.

1. navegar até C:\Program Files\Citrix\Telemetry Service
2. Abra o arquivo ScoutUI.exe.config.
3. Altere o valor de LinuxVDATelemetryServicePort ou LinuxVDATelemetryWakeupPort para o que foi configurado no VDA Linux:

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. Salve as alterações e feche o arquivo.
2. Abra o Scout novamente para garantir que ele carregue a configuração mais recente.

Sobre as verificações de integridade

Os dados de verificação de integridade são armazenados em pastas em `C:\ProgramData\Citrix\TelemetryService\`.

Verificações de integridade do site

As verificações de integridade do site estão incluídas no Serviço de Teste de Ambiente, que fornece uma avaliação abrangente dos serviços da FlexCast Management Architecture (FMA). Além de verificar a disponibilidade do serviço, essas verificações procuram outros indicadores de integridade, como conexões de banco de dados.

As verificações de integridade do site são executadas nos Delivery Controllers. Dependendo do tamanho do seu site, essas verificações podem levar até uma hora para serem concluídas.

VERIFICAÇÕES DE CONFIGURAÇÃO DO DELIVERY CONTROLLER

Como parte das verificações de integridade do site. As verificações de configuração do Delivery Controller verificam se os seguintes problemas existem, com base nas recomendações da Citrix para sites do Virtual Apps and Desktops:

- Um ou mais Delivery Controllers estão em um estado de falha.
- Existe apenas um Delivery Controller no site.
- Os Delivery Controllers são de versões diferentes.

Além de atender às permissões e requisitos para verificações de integridade, as verificações de configuração do Delivery Controller exigem:

- Pelo menos um Controller ligado.
- O Serviço Broker em execução em um Controller.
- Uma conexão funcional do Controller com o banco de dados do site.

Verificações de integridade do VDA

As verificações de integridade do VDA identificam possíveis causas para problemas comuns de registro do VDA, inicialização de sessão e redirecionamento de fuso horário.

Para registro no VDA, o Scout verifica:

- Instalação do software VDA
- Associação de domínio da máquina VDA
- Disponibilidade da porta de comunicação do VDA
- Status do serviço VDA
- Configuração do firewall do Windows
- Comunicação com o Controller
- Sincronização de tempo com o Controller

- Status de registro do VDA

Para inicializações de sessão em VDAs, o Scout verifica:

- Disponibilidade da porta de comunicação para inicialização de sessão
- Status dos serviços de inicialização de sessão
- Configuração do firewall do Windows para inicialização de sessão
- Licenças de Acesso para Cliente dos Serviços de Área de Trabalho Remota do VDA
- Caminho de inicialização do aplicativo VDA
- Configurações de registro para inicialização de sessão

Para redirecionamento de fuso horário em VDAs, o Scout verifica:

- Instalação de hotfix do Windows
- Instalação de hotfix do Citrix
- Configurações de política de grupo da Microsoft
- Configurações de política de grupo do Citrix

Para o Profile Management em VDAs, o Scout verifica:

- Detecção de hipervisor
- Detecção de provisionamento
- Citrix Aplicativos Virtuais e Desktops
- Configuração de vDisk pessoal
- Repositório de usuário
- Detecção de status do serviço Profile Management
- Teste de hooking do Winlogon.exe

Para executar verificações no Profile Management, você deve instalar e habilitar o Profile Management no VDA. Para obter mais informações sobre as verificações de configuração do Profile Management, consulte o artigo da Central de Conhecimento CTX132805.

Verificações de integridade do StoreFront

As verificações do StoreFront verificam:

- O serviço Citrix Default Domain está em execução
- O serviço Citrix Credential Wallet está em execução

- Conexão do servidor StoreFront com a porta 88 do Active Directory
- Conexão do servidor StoreFront com a porta 389 do Active Directory
- A URL base tem um FQDN válido
- O endereço IP correto da URL base pode ser recuperado
- O pool de aplicativos do IIS está usando .NET 4.0
- Se o certificado está vinculado à porta SSL para a URL do host
- Se a cadeia de certificados está completa
- Se os certificados expiraram
- Se um certificado está prestes a expirar (dentro de 30 dias)

Verificações do Servidor de Licenças

As verificações do Servidor de Licenças verificam:

- Conexão do Servidor de Licenças a partir do Delivery Controller
- Status de acesso remoto do firewall do Servidor de Licenças
- Status do serviço de Licenciamento Citrix
- Estado do modo de cache de licenças do Servidor de Licenças
- Conexão das portas do Servidor de Licenças
- Se o daemon do fornecedor Citrix (CITRIX) está em execução
- Se os relógios do sistema estão sincronizados
- Se o serviço de Licenciamento Citrix está sendo executado sob a conta de Serviço Local
- Presença do arquivo `CITRIX.opt`
- Data de elegibilidade dos Serviços de Sucesso do Cliente
- Atualização do Servidor de Licenças Citrix
- Se o certificado do Servidor de Licenças está no armazenamento raiz confiável do Delivery Controller

Além de atender às permissões e requisitos para verificações de integridade, o Servidor de Licenças deve estar associado a um domínio. Caso contrário, o Servidor de Licenças não é descoberto.

Executar verificações de integridade

O procedimento de Verificação de Integridade compreende a seleção de máquinas, o início da verificação e, em seguida, a revisão do relatório de resultados.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Verificação de Integridade**.
2. Selecione as máquinas. Clique em **Localizar máquina** para descobrir máquinas. A página **Selecionar máquinas** lista todos os VDAs, Delivery Controllers e Servidores de Licenças descobertos no site. Você pode filtrar a exibição por nome da máquina. Selecione a caixa de seleção ao lado de cada máquina da qual deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

   Para adicionar outros tipos de componentes (como servidores StoreFront e máquinas VDA), consulte Adicionar máquinas manualmente e Importar máquinas VDA. Não é possível adicionar manualmente Servidores Citrix Provisioning™ ou Servidores de Licenças.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar, uma mensagem será exibida na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

   - Resolver o problema e, em seguida, selecionar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (deixe sua caixa de seleção desmarcada). As verificações de integridade não são executadas para essa máquina.

   Quando os testes de verificação forem concluídos, clique em **Continuar**.
3. Execute as verificações de integridade nas máquinas selecionadas. O resumo lista as máquinas onde os testes são executados (as máquinas que você selecionou e que passaram nos testes de verificação). Clique em **Iniciar Verificação**.

   Durante e após a verificação:

   - A coluna **Status** indica o estado de verificação atual de uma máquina.
   - Para parar todas as verificações em andamento, clique em **Parar Verificação** no canto inferior direito da página. (Você não pode cancelar a verificação de integridade de uma única máquina, apenas de todas as máquinas selecionadas. As informações das máquinas que concluíram as verificações são mantidas.

- Quando as verificações forem concluídas para todas as máquinas selecionadas, o botão **Parar Verificação** no canto inferior direito muda para **Concluído**.
- Se uma verificação falhar, você pode clicar em **Tentar Novamente** na coluna **Ação**.
- Se uma verificação for concluída sem problemas encontrados, a coluna **Ação** estará vazia.
- Se uma verificação encontrar problemas, clique em **Ver Detalhes** para mostrar os resultados.
- Após a conclusão da verificação para todas as máquinas selecionadas, não clique em **Voltar**. (Se você o fizer, os resultados da verificação serão perdidos.)

4. Quando as verificações forem concluídas, clique em **Concluído** para retornar à página inicial do Scout.

Resultados da verificação de integridade

Para verificações Citrix que geram relatórios, os relatórios contêm:

- Hora e data em que o relatório de resultados foi gerado
- Máquinas que foram verificadas
- Condições que a verificação procurou nas máquinas de destino

Permissões e requisitos

Permissões:

- Para coletar diagnósticos:
  - Você deve ser um administrador local e usuário de domínio para cada máquina da qual você está coletando diagnósticos.
  - Você deve ter permissão para gravar no diretório LocalAppData em cada máquina.
- Para executar verificações de integridade:
  - Você deve ser um membro do grupo de usuários do domínio.
  - Você deve ser um administrador completo ou ter uma função personalizada com permissões somente leitura e de **Executar Testes de Ambiente** para o site.
  - Defina a política de execução de script para pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** outros privilégios de execução de script também podem funcionar.
- Use **Executar como administrador** ao iniciar o Scout.

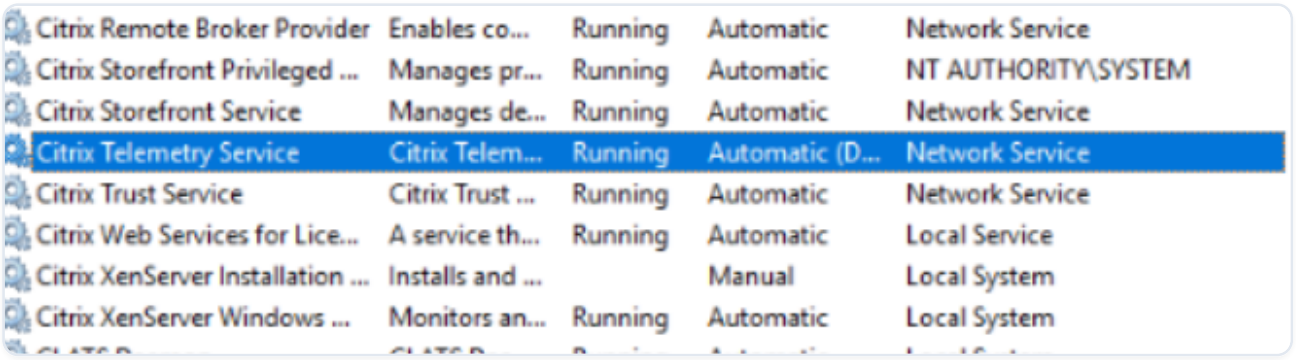
Para cada máquina da qual você coleta diagnósticos ou executa verificações de integridade:

- O Scout 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 Serviço de Telemetria Citrix deve estar em execução na máquina.
- O acesso à Infraestrutura de Gerenciamento do Windows (WMI) deve estar habilitado na máquina.
- Para definir um agendamento para a coleta de diagnóstico, a máquina deve estar executando uma versão compatível do Scout.

Não use o cifrão ($) em nomes de usuário especificados em nomes de caminho. Isso impede a coleta de informações de diagnóstico.

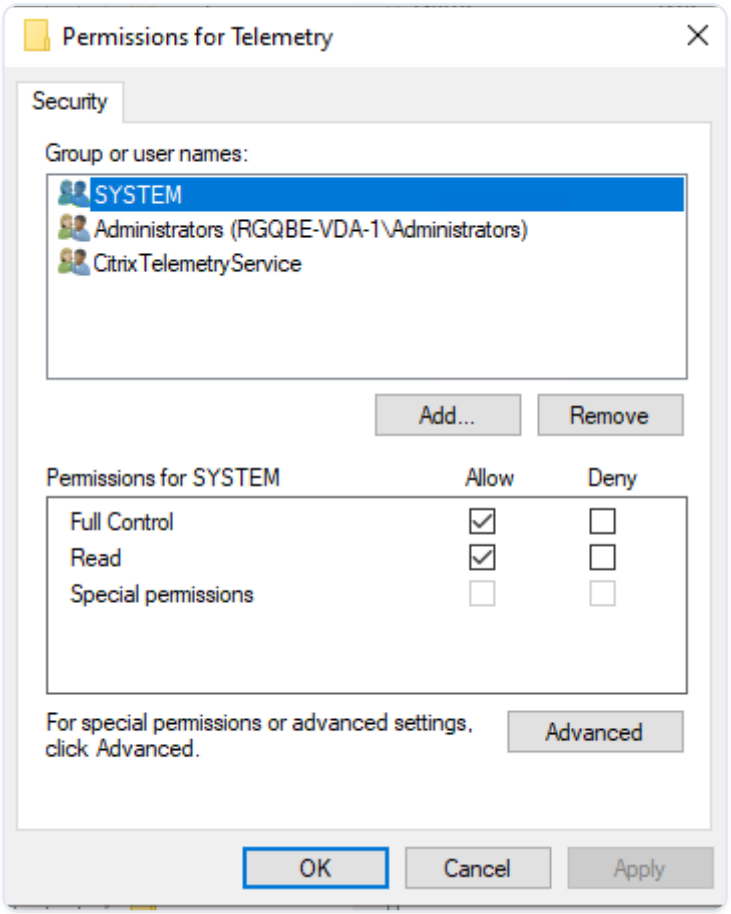
O Scout executa testes de verificação nas máquinas que você seleciona para garantir que esses requisitos sejam atendidos.

O Serviço de Telemetria para Windows é executado no Serviço de Rede.

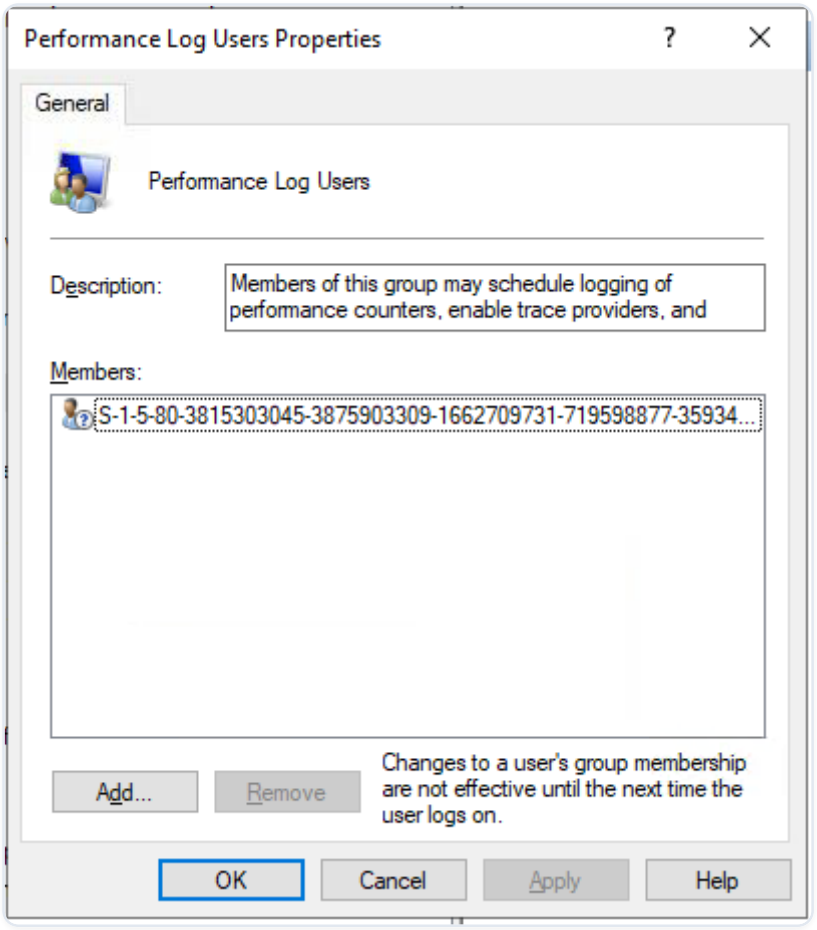


A Pasta de Rastreamento AOT é salva em `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Somente usuários no grupo Administrador, Sistema e SID do Serviço de Telemetria têm permissão para acessar o registro `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.



O SID do Serviço de Telemetria permanece no grupo Usuários do Log de Desempenho após a desinstalação do Serviço de Telemetria, mas você pode removê-lo manualmente.



Testes de verificação

Antes do início de uma coleta de diagnóstico ou verificação de integridade, testes de verificação são executados automaticamente para cada máquina selecionada. Esses testes garantem que os requisitos sejam atendidos. Se um teste falhar para uma máquina, o Scout exibirá uma mensagem com ações corretivas sugeridas.

- **O Scout não consegue acessar esta máquina** - Certifique-se de que:
  - A máquina está ligada.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)
  - O compartilhamento de arquivos e impressoras está ativado. Consulte a documentação da Microsoft para obter instruções.
- **Habilitar PSRemoting e WinRM** - Você pode habilitar o PowerShell remoting e o WinRM ao mesmo tempo. Usando **Executar como administrador**, execute o cmdlet `Enable-PSRemoting`. Para obter detalhes, consulte a ajuda da Microsoft para o cmdlet.
- **Scout requer PowerShell 3.0 (mínimo)** - Instale o PowerShell 3.0 (ou posterior) na máquina e, em seguida, habilite o PowerShell remoting.

- **Não é possível acessar o diretório LocalAppData nesta máquina** - Certifique-se de que a conta tenha permissão para gravar no diretório LocalAppData na máquina.
- **Não é possível localizar o Citrix Telemetry Service** - Certifique-se de que o Citrix Telemetry Service esteja instalado e iniciado na máquina.
- **Não é possível obter o agendamento** - Atualize a máquina para (mínimo) XenApp e XenDesktop 7.14.
- **WMI não está em execução na máquina** - Certifique-se de que o acesso ao Windows Management Instrumentation (WMI) esteja habilitado.
- **Conexões WMI bloqueadas** - Habilite o WMI no serviço Windows Firewall.
- **Versão mais recente do Citrix Telemetry Service necessária** - (A versão é verificada apenas para Coletar e Rastrear e Reproduzir.) Atualize a versão do Telemetry Service na máquina (consulte Instalar e atualizar). Se você não atualizar o serviço, essa máquina não será incluída nas ações **Coletar** ou **Rastrear e Reproduzir**.
- **Scout não consegue se conectar ao soquete systemd nesta máquina** - Certifique-se de que:
  - A porta 7503 está aberta. Verifique se o `systemd ctxtelemetry.socket` está escutando na porta 7503 na máquina. A porta pode ser diferente se a porta `ctxtelemetry.socket` tiver sido alterada. Consulte Configuração do Scout para ajustar as portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)
- **O Linux VDA Telemetry Service não está iniciado nesta máquina** - Certifique-se de que:
  - A porta 7502 está aberta. Verifique se o Serviço de Telemetria do Linux VDA está instalado e iniciado na máquina. A porta pode ser diferente se a porta do serviço de telemetria tiver sido alterada. Consulte Configuração do Scout para ajustar as portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)

Compatibilidade de versão

Esta versão do Scout (3.x) destina-se a ser executada em Controladores e VDAs do Citrix Virtual Apps and Desktops (ou mínimo XenApp e XenDesktop 7.14).

Uma versão anterior do Scout é fornecida com as versões do XenApp e XenDesktop anteriores à 7.14. Para obter informações sobre essa versão anterior, consulte CTX130147.

Se você atualizar um Controlador ou VDA anterior à versão 7.14 para a versão 7.14 (ou uma versão posterior suportada), a versão anterior do Scout será substituída pela versão atual.

| Recurso | Scout 2.23 | Scout 3.0 | --- | --- | ---| -- | Suporta Citrix Virtual Apps and Desktops (além de XenApp e XenDesktop 7.14 a 7.18) | Sim | Sim Suporta XenDesktop 5.x, 7.1–7.13 | Sim | Não Suporta XenApp 6.x, 7.5 a 7.13 | Sim | Não Entregue com o produto | 7.1–7.13 | A partir de 7.14 Pode ser baixado do artigo CTX | Sim | Não Capturar rastreamentos CDF | Sim | Sim Capturar rastreamentos Always-on (AOT) | Não | Sim Permitir a coleta de dados de diagnóstico | Até 10 máquinas de uma vez (por padrão) | Ilimitado (sujeito à disponibilidade de recursos) Permitir que dados de diagnóstico sejam enviados para a Citrix | Sim | Sim Permitir que dados de diagnóstico sejam salvos localmente | Sim | Sim Suportar credenciais do Citrix Cloud™ | Não | Sim Suportar credenciais da Citrix | Sim | Sim Suportar servidor proxy para uploads | Sim | Sim Ajustar agendamentos | N/A | Sim Suporte a scripts | Linha de comando (somente Controller local) | PowerShell usando cmdlets Call Home (qualquer máquina com o Serviço de Telemetria instalado) Verificações de integridade | Não | Sim Mascaramento de Dados | Não | A partir da versão 3.17

Instalar e atualizar

Por padrão, o Scout é instalado ou atualizado automaticamente como parte do Serviço de Telemetria Citrix quando você instala ou atualiza um VDA ou um Controller.

Se você omitir o Serviço de Telemetria Citrix ao instalar um VDA, ou remover o serviço posteriormente, execute `TelemetryServiceInstaller_xx.msi` da pasta `x64\Virtual Desktop Components` ou `x86\Virtual Desktop Components` na mídia de instalação do Citrix Virtual Apps and Desktops.

Ao selecionar a ação **Coletar** ou **Rastrear e Reproduzir**, você será notificado se uma máquina estiver executando uma versão mais antiga do Serviço de Telemetria Citrix. A Citrix recomenda usar a versão mais recente suportada. Se você não atualizar o Serviço de Telemetria nessa máquina, ele não será incluído nas ações **Coletar** ou **Rastrear e Reproduzir**. Para atualizar o Serviço de Telemetria, use o mesmo procedimento de instalação.

Autorização de upload

Se você planeja fazer upload de coleções de diagnóstico para a Citrix, você deve ter uma conta Citrix ou Citrix Cloud. (Estas são as credenciais que você usa para acessar downloads da Citrix ou acessar o Citrix Cloud Control Center.) Após a validação das suas credenciais de conta, um token é emitido.

Se você autenticar com uma conta Citrix ou uma conta Citrix Cloud, clique em um link para acessar o Citrix Cloud usando HTTPS com seu navegador padrão. Depois de inserir suas credenciais do Citrix Cloud, o token é exibido. Copie o token e cole-o no Scout. Você pode então continuar no assistente do Scout.

O token é armazenado localmente na máquina onde você está executando o Scout. Para permitir o uso desse token na próxima vez que você executar **Coletar** ou **Rastrear e Reproduzir**, selecione a caixa de seleção **Armazenar token e pular esta etapa no futuro**.

Você deve reautorizar cada vez que selecionar **Agendar** na página inicial do Scout. Você não pode usar um token armazenado ao criar ou alterar um agendamento.

Usar um proxy para uploads

Se você deseja usar um servidor proxy para fazer upload de coleções para a Citrix, pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Alternativamente, você pode especificar o endereço IP e o número da porta do servidor proxy.

Localizar máquina

Para os procedimentos **Coletar**, **Rastrear e Reproduzir** e **Agendar**, o Scout lista os Controllers e VDAs que ele descobre automaticamente.

Quando você executa Scout Health Check a partir do Delivery Controller, clique em **Localizar máquina** para descobrir máquinas, incluindo controladores de entrega, VDAs, servidores de licença e servidores StoreFront.

Quando você executa o Scout Health Check a partir de uma máquina ingressada no domínio que não é um Delivery Controller, o Scout não consegue descobrir máquinas automaticamente. Você precisa adicionar máquinas manualmente ou importar máquinas VDA.

Adicionar máquinas manualmente

Depois que o Scout lista os Controladores e VDAs que ele descobre, você pode adicionar manualmente outras máquinas na implantação, como servidores StoreFront, Servidores de Licença e servidores Citrix Provisioning.

Ao executar verificações de integridade:

- Os Servidores de Licença Citrix no domínio são descobertos automaticamente. Você não pode adicionar Servidores de Licença manualmente.

- As verificações de integridade não oferecem suporte atualmente a servidores Citrix Provisioning.

Em qualquer página do Scout que liste as máquinas descobertas, clique em **+ Adicionar máquina**. Digite o FQDN da máquina que você deseja adicionar e, em seguida, clique em **Continuar**. Repita para adicionar outras máquinas, conforme necessário. (Embora inserir um alias DNS em vez de um FQDN possa parecer válido, as verificações de integridade podem falhar.)

As máquinas adicionadas manualmente sempre aparecem no topo da lista de máquinas, acima das máquinas descobertas.

Uma maneira fácil de identificar uma máquina adicionada manualmente é o botão vermelho de exclusão no lado direito da linha. Somente as máquinas adicionadas manualmente têm esse botão. As máquinas descobertas não têm.

Para remover uma máquina adicionada manualmente, clique no botão vermelho no lado direito da linha. Confirme a exclusão. Repita para excluir outras máquinas adicionadas manualmente.

O Scout lembra as máquinas adicionadas manualmente até que você as remova. Quando você fecha e reabre o Scout, as máquinas adicionadas manualmente ainda são listadas no topo da lista.

Os rastreamentos CDF não são coletados ao usar **Rastrear e Reproduzir** em servidores StoreFront. No entanto, todas as outras informações de rastreamento são coletadas.

Importar máquinas VDA

Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

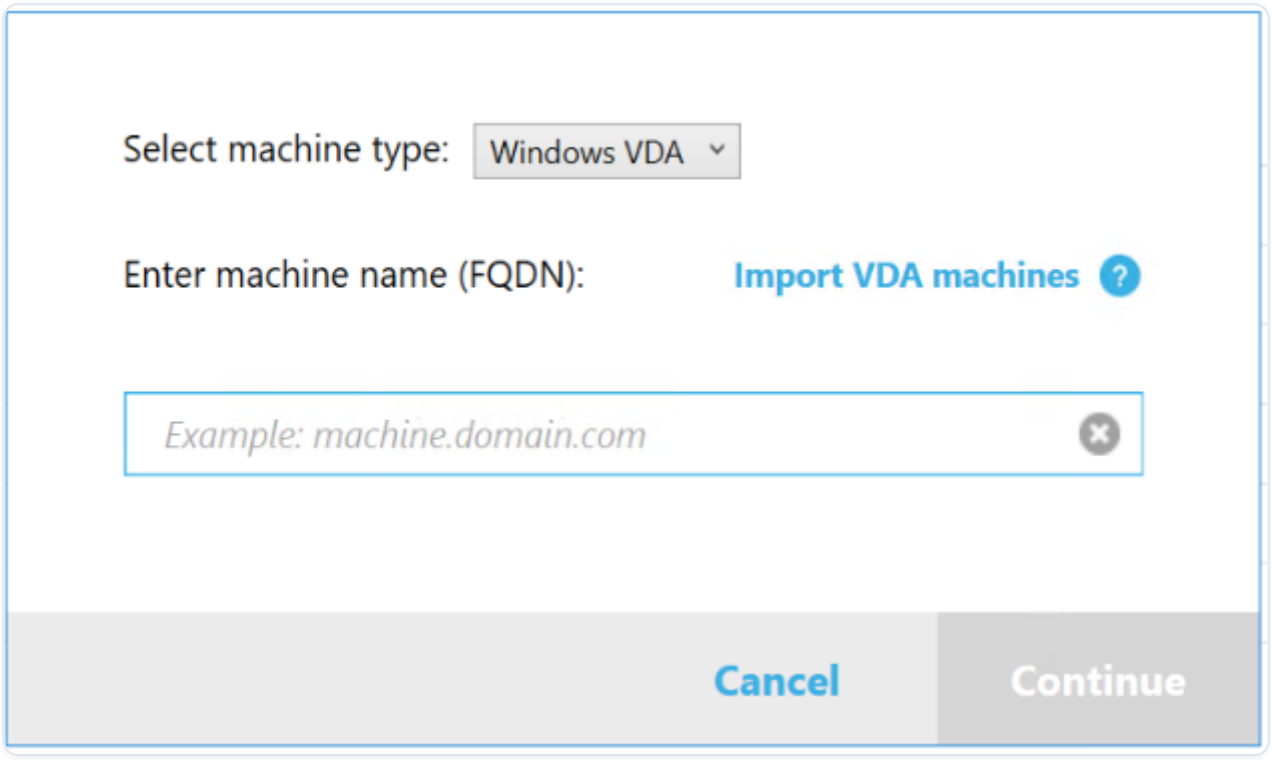
1. No Delivery Controller ou Connector, gere o arquivo de lista de máquinas com o comando PowerShell. No Connector, você deve inserir as credenciais Citrix e selecionar o cliente na caixa de diálogo pop-up.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. Copie o arquivo machineList.txt para a máquina ingressada no domínio na qual você deseja iniciar o Scout Health Check.
3. Na página Scout Health Check, clique em **Adicionar Máquina**.
4. Selecione o tipo de máquina **Windows VDA**.
5. Clique em **Importar máquinas VDA**.
6. Selecione o arquivo machineList.txt.

7. Clique em **Abrir**.

As máquinas VDA importadas são listadas na página Scout Health Check.



Coletar diagnósticos

O procedimento de **Coleta** compreende a seleção de máquinas, o início da coleta de diagnósticos e, em seguida, o upload do arquivo contendo a coleta para a Citrix ou salvá-lo localmente.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Coletar**.
2. Selecione as máquinas.

   - Em um Controller, a página **Selecionar máquinas** lista todos os VDAs e Controllers no site. Você pode filtrar a exibição por nome da máquina. Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.
   - Em outros componentes (como servidores VDA), a página **Selecionar máquinas** lista apenas a máquina local. A adição manual de máquinas não é suportada.

   Selecione a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

O Scout inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar, uma mensagem será exibida na coluna **Status** e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolver o problema e, em seguida, selecionar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignorar essa máquina (deixe a caixa de seleção desmarcada). Os diagnósticos não serão coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

3. Coletar diagnósticos. O resumo lista todas as máquinas das quais os diagnósticos são coletados (as máquinas que você selecionou e que passaram nos testes de verificação). Clique em **Iniciar Coleta**.

   Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta para uma máquina.
   - Para interromper uma coleta em andamento em uma única máquina, clique em **Cancelar** na coluna **Ação** para essa máquina.
   - Para interromper todas as coletas em andamento, clique em **Parar Coleta** no canto inferior direito da página. Os diagnósticos das máquinas que concluíram a coleta são mantidos. Para retomar a coleta, clique em **Repetir** na coluna **Ação** para cada máquina.
   - Quando a coleta for concluída para todas as máquinas selecionadas, o botão **Parar Coleta** no canto inferior direito mudará para **Continuar**.
   - Para coletar diagnósticos novamente, clique em **Coletar Novamente** na coluna **Ação** dessa máquina. A coleta mais recente sobrescreve a anterior.
   - Se uma coleta falhar, você pode clicar em **Repetir** na coluna **Ação**. Somente coletas bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Voltar**. (Se você clicar, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

4. Salvar ou carregar a coleção. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo na máquina local.

   Se você optar por carregar o arquivo agora, continue com a Etapa 5.

Se você optar por salvar o arquivo localmente:

- Uma caixa de diálogo **Salvar** do Windows é exibida. navegar até o local desejado.
- Quando o salvamento local for concluído, o caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Você pode carregar o arquivo mais tarde para a Citrix. Consulte CTX136396.

Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir mais nenhuma etapa neste procedimento.

5. autenticar para uploads e, opcionalmente, especifique um proxy. Para obter detalhes, consulte Autorização de upload.

   - Se você não se autenticou pelo Scout, continue com esta etapa.
   - Se você se autenticou pelo Scout, o token de autorização armazenado é usado por padrão. Se for isso que você deseja fazer, selecione esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleção. Continue com a Etapa 6.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as propriedades de internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será aberto em uma página do Citrix Cloud onde um token é exibido. Copie o token e cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

6. Insira informações sobre o upload.

- O campo de nome contém o nome padrão para o arquivo dos diagnósticos coletados. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo de nome vazio, o nome padrão será usado.)
- Opcionalmente, especifique um número de caso de suporte Citrix de 8 dígitos.
- No campo opcional **Descrição**, descreva o problema e indique quando ele ocorreu, se aplicável.

Quando terminar, clique em **Iniciar Upload**.

Durante o upload, a parte inferior esquerda da página mostra aproximadamente a porcentagem do upload que foi concluída. Para cancelar um upload em andamento, clique em **Parar Upload**.

Quando o upload for concluído, o URL de sua localização será exibido e vinculado. Você pode seguir o link para o local da Citrix para visualizar a análise do upload, ou pode copiar o link.

Clique em **Concluído** para retornar à página inicial do Scout.

Rastrear e reproduzir

O procedimento **Rastrear e Reproduzir** compreende a seleção de máquinas, o início de um rastreamento, a reprodução de problemas, a conclusão da coleta de diagnósticos e, em seguida, o upload do arquivo para a Citrix ou o salvamento localmente.

Este procedimento é semelhante ao procedimento padrão de **Coleta**. No entanto, ele permite que você inicie um rastreamento em máquinas e, em seguida, recrie problemas nessas máquinas. Todas as coletas de diagnóstico incluem informações de rastreamento AOT. Este procedimento adiciona rastreamentos CDF para auxiliar na solução de problemas.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página inicial, clique em **Rastrear e Reproduzir**.
2. Selecione as máquinas. A página **Selecionar máquinas** lista todos os VDAs e Controladores no site. Você pode filtrar a exibição pelo nome da máquina. Selecione a caixa de seleção ao lado de cada máquina da qual deseja coletar rastreamentos e diagnósticos. Em seguida, clique em **Continuar**.

   Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.

Scout automaticamente inicia testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados em Testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será postada na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolva o problema e, em seguida, selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignore essa máquina (deixe sua caixa de seleção desmarcada). Diagnósticos e rastreamentos não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

3. Inicie o rastreamento. O resumo lista todas as máquinas das quais os rastreamentos são coletados. Clique em **Iniciar Rastreamento**.

   Em uma ou mais das máquinas selecionadas, reproduza os problemas que você encontrou. A coleta de rastreamento continua enquanto você faz isso. Quando terminar de reproduzir o problema, clique em **Continuar** no Scout. Isso interrompe o rastreamento.

   Depois de interromper o rastreamento, indique se você reproduziu o problema durante o rastreamento.

4. Colete diagnósticos das máquinas. Clique em **Iniciar Coleta**. Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta para uma máquina.
   - Para interromper uma coleta em andamento em uma única máquina, clique em **Cancelar** na coluna **Ação** para essa máquina.
   - Para interromper todas as coletas em andamento, clique em **Parar Coleta** no canto inferior direito da página. Os diagnósticos das máquinas que concluíram a coleta são mantidos. Para retomar a coleta, clique em **Repetir** na coluna **Ação** para cada máquina.
   - Quando a coleta for concluída para todas as máquinas selecionadas, o botão **Parar Coleta** no canto inferior direito muda para **Continuar**.
   - Para coletar diagnósticos novamente de uma máquina, clique em **Coletar Novamente** na coluna **Ação** dessa máquina. A coleta mais recente sobrescreve a anterior.
   - Se uma coleta falhar, você pode clicar em **Repetir** na coluna **Ação**. Somente as coletas bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Voltar**. (Se você o fizer, a coleta será perdida.)

   Quando a coleta for concluída, clique em **Continuar**.

5. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para a Citrix ou salvá-lo localmente.

   Se você optar por carregar o arquivo agora, continue com a Etapa 6.

   Se você optar por salvar o arquivo localmente:

   - Uma caixa de diálogo Salvar do Windows é exibida. Selecione o local desejado.
   - Quando o salvamento local for concluído, o caminho do arquivo será exibido e vinculado. Você pode visualizar o arquivo. Lembre-se: Você pode carregar o arquivo mais tarde da Citrix; consulte CTX136396 para Citrix Insight Services.

   Clique em **Concluído** para retornar à página inicial do Scout. Você não precisa concluir mais nenhuma etapa neste procedimento.

6. autenticar para uploads e, opcionalmente, especifique um proxy. Revise Autorização de upload para obter detalhes deste processo.

   - Se você não se autenticou através do Scout, continue com esta etapa.
   - Se você se autenticou através do Scout, o token de autorização armazenado é usado por padrão. Se é isso que você deseja fazer, escolha esta opção e clique em **Continuar**. Você não será solicitado a fornecer credenciais para esta coleta. Continue com a Etapa 7.
   - Se você se autenticou anteriormente, mas deseja reautorizar e obter um novo token, clique em **Alterar/Reautorizar** e continue com esta etapa.

   Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**. A página de credenciais aparece somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você deseja usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
   - Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será iniciado em uma página do Citrix Cloud onde um token é exibido. Copie o token e, em seguida, cole-o na página do Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continuar**.

7. Forneça informações sobre o upload.

   Insira os detalhes do upload:

   - O campo de nome contém o nome padrão para o arquivo dos diagnósticos coletados. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo de nome vazio, o nome padrão será usado.)
   - Opcionalmente, especifique um número de caso de Suporte Citrix de 8 dígitos.
   - No campo opcional Descrição, descreva o problema e indique quando o problema ocorreu, se aplicável.

   Quando terminar, clique em **Iniciar Upload**.

   Durante o upload, a parte inferior esquerda da página aproxima a porcentagem do upload concluído. Para cancelar um upload em andamento, clique em **Parar Upload**.

   Quando o upload for concluído, o URL de sua localização será exibido e vinculado. Você pode seguir o link para o local da Citrix para visualizar a análise do upload, ou pode copiar o link.

   Clique em **Concluído** para retornar à página inicial do Scout.

Habilitar coleta de log adicional

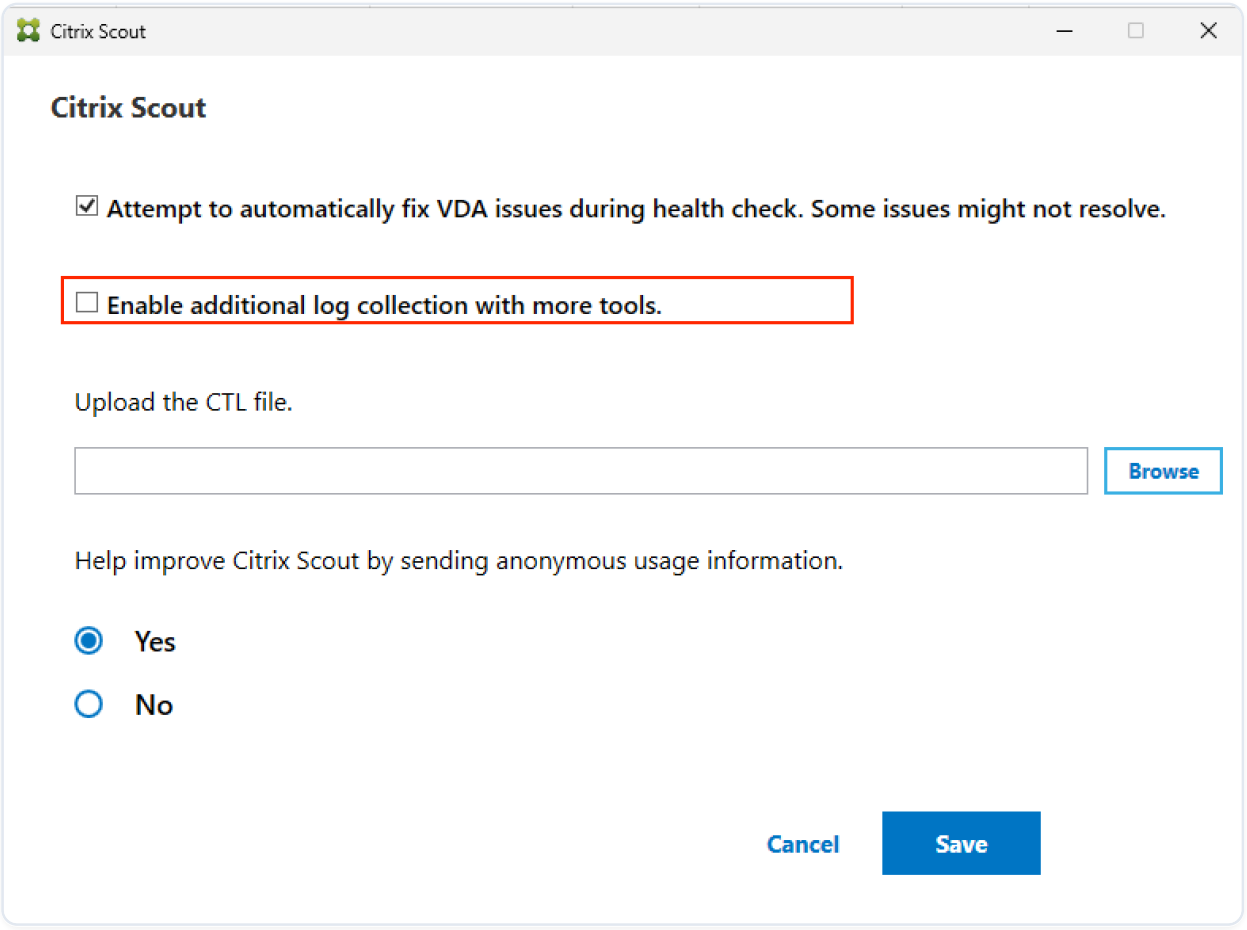
A função **Habilitar coleta de log adicional** permite que você use a função de rastreamento e reprodução com mais ferramentas, como perfmon, Netsh, DebugView e Wireshark.

A partir da versão 2407, ao habilitar a coleta de log adicional, o Scout detecta automaticamente as ferramentas relacionadas ao CDC instaladas em sua máquina e coleta automaticamente os logs de rastreamento relacionados às ferramentas CDC no pacote zip. Você pode personalizar esses arquivos zip e anexá-los ao Scout. Com essa automação, você pode usar o Citrix Scout de forma mais eficaz e isso ajuda a diagnosticar os problemas rapidamente.

> **Observação:**
>
> Isso se aplica apenas a máquinas locais.
>
> Para configurar a coleta de log adicional:

1. Inicie o Citrix Scout.
2. Clique no ícone de engrenagem **Configurações**.

3. Clique em **Habilitar coleta de log adicional com mais ferramentas**.
4. Clique em **Salvar**.



Para habilitar a coleta de log adicional, certifique-se de que as seguintes ferramentas necessárias estejam instaladas e que seus diretórios sejam criados manualmente no local especificado.

Locais de instalação da ferramenta:

- Logs do Procdump: Baixe o Procdump e coloque-o em %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe
- Logs do StoreFront: Baixe o DbgView e coloque-o em %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exe
- Logs do Procmon: Baixe o Process Monitor e coloque-o em %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe
- Logs do Wireshark: Instale o Wireshark manualmente em seu sistema.

Para coletar logs adicionais:

1. Na página inicial do Scout, clique em **Rastrear e Reproduzir**.

2. Na página **Selecionar ou adicionar máquinas** para coletar dados, marque a caixa da máquina local. O status deve aparecer como *Verificado*.
3. Clique em **Continuar** e siga as instruções Rastrear e Reproduzir.
4. Após a conclusão, verifique os logs no arquivo zip. Os logs são compactados na pasta *CDCLogs*.

> **Observação:**
>
> Se a Ferramenta Procmon for selecionada para rastreamento, os logs do Process Monitor podem crescer rapidamente. Certifique-se de selecionar apenas as ferramentas necessárias. Você também pode monitorar o tamanho dos logs em *%temp%\Scout-CDC-Log*.

Agendar coletas

> **Observação:**
>
> Atualmente, você pode agendar coletas, mas não verificações de integridade.

O procedimento de Agendamento compreende a seleção de máquinas e, em seguida, a configuração ou cancelamento do agendamento. As coletas agendadas são automaticamente carregadas para a Citrix. (Você pode salvar coletas agendadas localmente usando a interface PowerShell. Consulte Citrix Call Home.)

1. Inicie o Scout. No menu Iniciar da máquina, selecione **Citrix > Citrix Scout**. Na página inicial, clique em **Agendar**.
2. Selecione as máquinas. Todos os VDAs e Controladores no site são listados. Você pode filtrar a exibição pelo nome da máquina.

   Ao instalar VDAs e Controladores usando a interface gráfica, se você configurou um agendamento de Call Home (consulte Citrix Call Home), o Scout exibe essas configurações por padrão. Você pode usar esta versão do Scout para iniciar coletas agendadas pela primeira vez ou alterar um agendamento configurado anteriormente.

Embora você tenha ativado/desativado o Call Home por máquina durante a instalação do componente, um agendamento configurado no Scout afeta todas as máquinas que você selecionar.

Selecione a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e, em seguida, clique em **Continuar**.

Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.

O Scout inicia automaticamente testes de verificação em cada uma das máquinas selecionadas, garantindo que elas atendam aos critérios em Testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será exibida na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode:

- Resolva o problema e, em seguida, selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignore essa máquina (deixe sua caixa de seleção desmarcada). Diagnósticos (ou rastreamentos) não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continuar**.

A página de resumo lista as máquinas às quais os agendamentos são aplicados. Clique em **Continuar**.

3. Defina o agendamento. Indique quando você deseja que os diagnósticos sejam coletados. Lembre-se: O agendamento afeta todas as máquinas selecionadas.

   - Para configurar um agendamento semanal para as máquinas selecionadas, clique em **Semanal**. Escolha o dia da semana. Insira a hora do dia (formato 24 horas) para o início da coleta.
   - Para configurar um agendamento diário para as máquinas selecionadas, clique em **Diário**. Insira a hora do dia (formato 24 horas) para o início da coleta.
   - Para cancelar um agendamento existente para as máquinas selecionadas (e não substituí-lo por outro), clique em **Desativar**. Isso cancela qualquer agendamento que tenha sido configurado anteriormente para essas máquinas.

   Clique em **Continuar**.

4. autenticar para uploads e, opcionalmente, especifique um proxy. Revise Autorização de upload para obter detalhes deste processo. Lembre-se: Você não pode usar um token armazenado para autenticar ao trabalhar com um agendamento do Scout.

Escolha se deseja usar credenciais Citrix ou credenciais Citrix Cloud para autenticar o upload. Clique em **Continuar**.

Na página de credenciais:

- Se você deseja usar um servidor proxy para o upload do arquivo, clique em **Configurar proxy**. Você pode instruir o Scout a usar as configurações de proxy configuradas para as Propriedades da Internet do seu navegador. Ou, você pode inserir o endereço IP e o número da porta do servidor proxy. Feche a caixa de diálogo do proxy.
- Para uma conta Citrix Cloud, clique em **Gerar token**. Seu navegador padrão será aberto em uma página do Citrix Cloud onde um token é exibido. Copie o token e, em seguida, cole-o na página do Scout.
- Para uma conta Citrix, insira suas credenciais.

Quando terminar, clique em **Continuar**.

Revise o agendamento configurado. Clique em **Concluído** para retornar à página inicial do Scout.

Durante uma coleta, o log de aplicativos do Windows de cada máquina selecionada contém entradas sobre a coleta e o upload.

Mascaramento de dados

As informações de diagnóstico coletadas usando o Citrix Scout podem conter informações sensíveis à segurança. O recurso de mascaramento de dados do Citrix Scout permite mascarar dados sensíveis em arquivos de diagnóstico antes de enviá-los para a Citrix.

O mascaramento de dados do Scout é configurado para mascarar o endereço IP, nomes de máquinas, nomes de domínio, nomes de usuário, nomes de hypervisor, nomes de Delivery Group, nomes de catálogo, nomes de aplicativos e SIDs.

> **Observação:**

> Os rastreamentos CDF são criptografados e não podem ser mascarados.

> Os logs do Linux VDA são compactados para o formato `.tar.gz2` e não podem ser mascarados.

Coletar novos diagnósticos e realizar mascaramento de dados

Para usar o recurso de mascaramento de dados do Citrix Scout, inicie o Scout a partir da linha de comando.

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório onde o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie o Scout: `ScoutUI.exe datamasking`.
4. Clique em **Coletar** ou **Rastrear e Reproduzir** para coletar diagnósticos.
5. Após a conclusão da coleta, selecione **Habilitar mascaramento de dados**. Esta opção é habilitada por padrão.
6. Configure a máscara de dados. Você pode usar as regras padrão ou personalizar as regras.
7. Selecione se deseja carregar ou salvar a coleção de diagnósticos.
    - Se você selecionar **Carregar a coleção de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleção de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

Executar mascaramento de dados em diagnósticos existentes

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório onde o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie o Scout diretamente no modo de mascaramento de dados: `ScoutUI.exe datamasking filePath`.
4. Selecione “Habilitar mascaramento de dados” para continuar. Esta opção está habilitada por padrão.
5. Configure a máscara de dados. Você pode executar o mascaramento de dados com as regras padrão ou personalizar as regras.
6. Selecione se deseja carregar ou salvar a coleção de diagnósticos.
    - Se você selecionar **Carregar a coleção de diagnósticos para a Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Salvar a coleção de diagnósticos em sua máquina local**, tanto os diagnósticos originais quanto os mascarados serão salvos no local especificado.

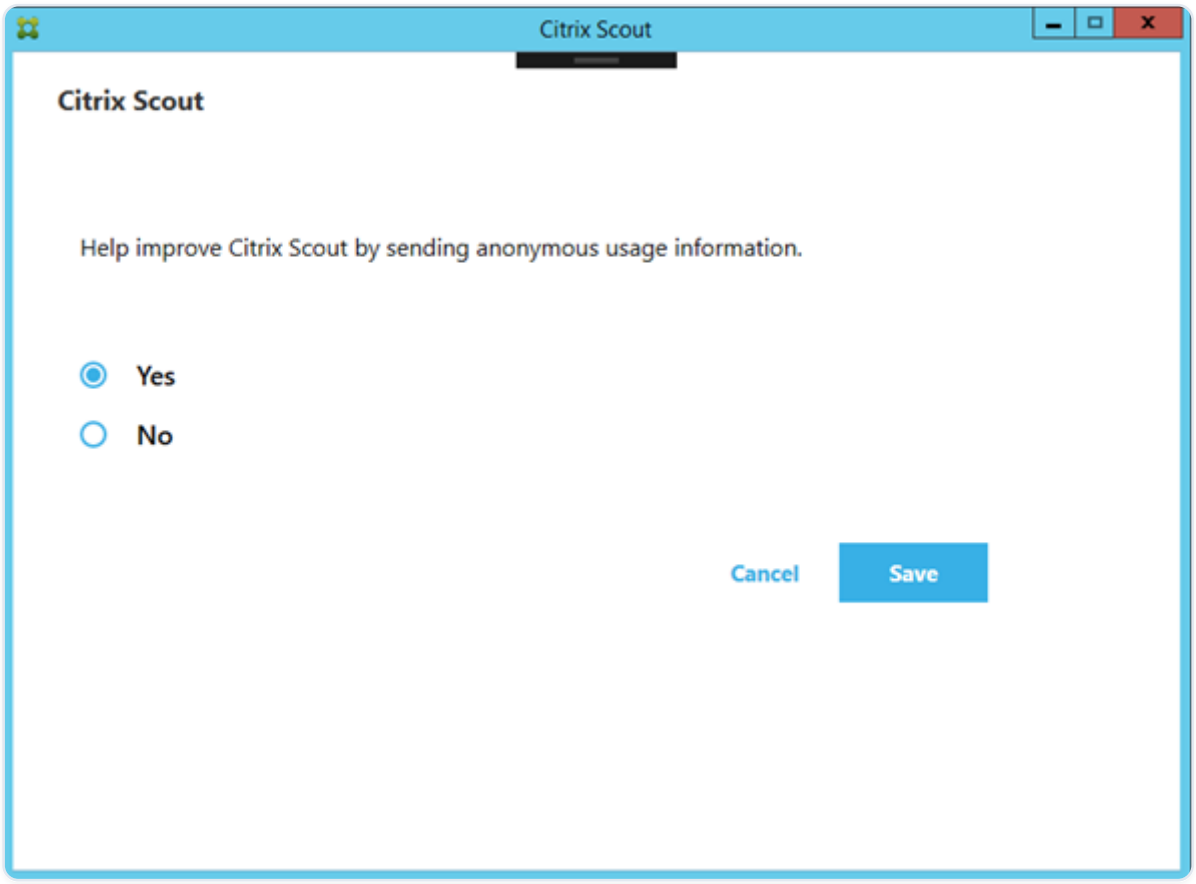
Locais do arquivo de dados mascarados e do arquivo de mapeamento

Depois de carregar ou salvar a coleção de diagnósticos, clique no link para abrir os diagnósticos originais e mascarados, e abra o arquivo de informações de mapeamento.

Coleta de dados de uso

Ao usar o Scout, a Citrix usa o Google Analytics para coletar dados de uso anônimos que serão utilizados para futuros recursos e melhorias do produto. A coleta de dados é habilitada por padrão.

Para alterar a coleta e o upload de dados de uso, clique no ícone de engrenagem **Configurações** na interface do usuário do Scout. Você pode então escolher se deseja enviar as informações selecionando **Sim** ou **Não** e, em seguida, clicando em **Salvar**.



Principais pontos de dados do Call Home

O Call Home coleta os seguintes pontos de dados principais.

(M) = Capturado apenas durante a coleta manual (cmdlet do PowerShell `Start-CitrixCallHomeUpload`)

NOME DO ARQUIVO	CATEGORIA	GRUPO DE DADOS

		Máquinas
		XDSite
		Informações do Site
		Informações do DB do Broker (M)
		Versão do DB instalada (M)
		Status do Serviço Broker (M)
		Instâncias de Serviço Registradas (M)
		Teste de Licença do Broker (M)
		Sessão HDX™ Ativa (M)
		Administrador do Broker
		Permissão de Administrador do Broker
		Configuração RDS (inclui LicensingSettings, SessionSettings, SpecifiedLicenseServers e RegisteredLicenseServers)
		Serviço de Monitoramento (M) (inclui MonitorConfiguration, MonitorDataStore, MonitorDBConnection, MonitorDBSchemaVersion, MonitorService, MonitorServiceAddedCapability, MonitorServiceInstance, MonitorServiceStatus e MonitorInstalledDBVersion)

		Registro de Configuração
		Log de Conexão
		Conexões de Hypervisor (M)
		Conexão de Hypervisor do Broker
		Alertas de Hypervisor
		Catálogos
		Agentes de SO de múltiplas sessões (M)
		Agentes de SO de sessão única (M)
		Aplicativos Publicados
		Grupos de Entrega
		Agentes de Entrega Configurados

		Componentes Instalados do Citrix
		Informações do Serviço de Broker Citrix
		Arquivo de configuração do Serviço de Broker
		Arquivo de configuração do Machine Creation Services™
		Arquivo de configuração do Serviço de Host
		Arquivo de configuração do Serviço de Identidade AD

		Arquivo de configuração do Serviço de Configuração
		Arquivo de configuração do Serviço de Log de Configuração
		Arquivo de configuração do Serviço de Administração Delegada
		Arquivo de configuração do Serviço de Teste de Ambiente
		Arquivo de configuração do Serviço de Monitoramento
		Arquivo de configuração do Serviço Storefront™
		Arquivo de configuração do Agente da Estação de Trabalho
		Informações do VDA Citrix
		Hotfix Citrix XD
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		Computador
		BIOS
		Informações de Memória

		Processador
		Dispositivo PNP
		Dispositivo
		Unidade de Disco
		Unidade Lógica
		Uso do Arquivo de Paginação
		Adaptador de Rede
		Configuração do Adaptador de Rede
		ipConfig
		Controlador de Vídeo
		Controlador IDE
		Controlador SCSI

		HKLM: \Software\Wow6432Node\Citrix
		HKLM: \System\CurrentControlSet\Control\Citrix
		HKLM: \SOFTWARE\Policies\Citrix
		HKLM: \Software\Microsoft\Cryptography
		HKLM: \Software\Wow6432Node\Microsoft\Cryptography

		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\Session Manager
		HKLM:\System\CurrentControlSet\Control\Terminal Server
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation

		HKLM: \SYSTEM\CurrentControlSet\ Control\FileSystem
		HKLM: \SYSTEM\CurrentControlSet\ Control\Windows
		HKLM: \SYSTEM\CurrentControlSet\ Control\TimeZoneInformation

		Driver
		EnvVariables
		SO
		Processo
		Serviço
		Service Pack
		GPResult
		Hotfix da Microsoft
		Netstat
		Driver PNP

		Log de Eventos do Sistema
		AOT (Rastreamento Sempre Ativo)
		Dumps de Falha

		tempo de atividade

		memória
		sistema do computador
		processador
		controlador de vídeo
		unidade de disco
		informações do navegador
		tempos de reinicialização
		uso de memória
		uso de disco
		resoluções de sessão ICA
		profundidade de cor ICA
		ID da máquina CEIP do metainstalador

		Número de Lojas
		Número de Servidores no Grupo de Servidores
		Número de Delivery Controller™ por Loja
		HTTPS Habilitado
		Experiência Clássica Habilitada Para Citrix Receiver™
		Configuração do Receiver HTML5 Para Citrix Receiver

		Controle de Workspace Habilitado Para Citrix Receiver
		Acesso Remoto Habilitado Para Loja
		Número de Gateways
		Serviço JSON explícito para autenticação NetScaler® integrada

Administração delegada

Observação:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente em Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O modelo de administração delegada oferece a flexibilidade para corresponder à forma como sua organização deseja delegar atividades de administração, usando controle baseado em função e objeto. A administração delegada acomoda implantações de todos os tamanhos e permite configurar mais granularidade de permissões à medida que sua implantação cresce em complexidade. A administração delegada usa três conceitos: administradores, funções e escopos.

- **Administradores:** Um administrador representa uma pessoa ou um grupo de pessoas identificadas por sua conta do Active Directory. Cada administrador está associado a um ou mais pares de função e escopo.
- **Funções:** Uma função representa uma função de trabalho e tem permissões definidas associadas a ela. Por exemplo, a função de Administrador de Grupo de Entrega tem permissões como 'Criar Grupo de Entrega' e 'Remover Desktop do Grupo de Entrega'. Um administrador pode ter várias funções para um site, então uma pessoa pode ser um

Administrador de Grupo de Entrega e um Administrador de Catálogo de Máquinas. As funções podem ser integradas ou personalizadas.

As funções integradas são:

FUNÇÃO	PERMISSÕES
Administrador Completo	Pode executar todas as tarefas e operações. Um Administrador Completo é sempre combinado com o escopo Todos.
Administrador Somente Leitura	Pode ver todos os objetos em escopos especificados, além de informações globais, mas não pode alterar nada. Por exemplo, um Administrador Somente Leitura com Escopo=Londres pode ver todos os objetos globais (como Registro de Configuração) e quaisquer objetos com escopo de Londres (por exemplo, Grupos de Entrega de Londres). No entanto, esse administrador não pode ver objetos no escopo de Nova York (assumindo que os escopos de Londres e Nova York não se sobreponham).
Administrador de Help Desk	Pode visualizar Grupos de Entrega e gerenciar as sessões e máquinas associadas a esses grupos. Pode ver o Catálogo de Máquinas e as informações do host para os Grupos de Entrega que estão sendo monitorados. Também pode executar operações de gerenciamento de sessão e gerenciamento de energia de máquina para as máquinas nesses Grupos de Entrega.
Administrador de Catálogo de Máquinas	Pode criar e gerenciar Catálogos de Máquinas e provisionar as máquinas neles. Pode construir Catálogos de Máquinas a partir da infraestrutura de virtualização, Provisioning Services e máquinas físicas. Esta função pode gerenciar imagens base e instalar software, mas não pode atribuir aplicativos ou desktops a usuários.

FUNÇÃO	PERMISSÕES
Administrador de Grupo de Entrega	Pode entregar aplicativos, desktops e máquinas; também pode gerenciar as sessões associadas. Também pode gerenciar configurações de aplicativos e desktops, como políticas e configurações de gerenciamento de energia.
Administrador de Host	Pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, aplicativos ou desktops aos usuários.

Em certas edições do produto, você pode criar funções personalizadas para atender aos requisitos de sua organização e delegar permissões com mais detalhes. Você pode usar funções personalizadas para alocar permissões na granularidade de uma ação ou tarefa em um console.

- **Escopos:** Um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma que seja relevante para sua organização (por exemplo, o conjunto de Delivery Groups usado pela equipe de Vendas). Os objetos podem estar em mais de um escopo; você pode pensar nos objetos sendo rotulados com um ou mais escopos. Existe um escopo integrado: 'Todos', que contém todos os objetos. A função de Administrador Completo está sempre emparelhada com o escopo **Todos**.

Exemplo

A Empresa XYZ decidiu gerenciar aplicativos e desktops com base em seu departamento (Contas, Vendas e Armazém) e em seu sistema operacional de desktop (Windows 7 ou Windows 8). O administrador criou cinco escopos e então rotulou cada Delivery Group com dois escopos: um para o departamento onde são usados e outro para o sistema operacional que utilizam.

Os seguintes administradores foram criados:

ADMINISTRADOR	FUNÇÕES	ESCOPOS
domain/fred	Administrador Completo	Todos (a função de Administrador Completo sempre tem o escopo Todos)

ADMINISTRADOR	FUNÇÕES	ESCOPOS
domain/rob	Administrador Somente Leitura	Todos
domain/heidi	Administrador Somente Leitura, Administrador de Suporte Técnico	Todas as Vendas
domain/warehouseadmin	Administrador de Help Desk	Armazém
domain/peter	Administrador de Grupo de Entrega, Administrador de Catálogo de Máquinas	Win7

- Fred é um Administrador Completo e pode visualizar, editar e excluir todos os objetos no sistema.
- Rob pode visualizar todos os objetos no site, mas não pode editá-los ou excluí-los.
- Heidi pode visualizar todos os objetos e realizar tarefas de suporte técnico em Grupos de Entrega no escopo de Vendas. Isso permite que ela gerencie as sessões e máquinas associadas a esses grupos; ela não pode fazer alterações no Grupo de Entrega, como adicionar ou remover máquinas.
- Qualquer pessoa que seja membro do grupo de segurança do Active Directory warehouseadmin pode visualizar e realizar tarefas de suporte técnico em máquinas no escopo de Armazém.
- Peter é um especialista em Windows 7 e pode gerenciar todos os Catálogos de Máquinas do Windows 7 e entregar aplicativos, desktops e máquinas do Windows 7, independentemente do escopo de departamento em que estejam. A administradora considerou tornar Peter um Administrador Completo para o escopo Win7. No entanto, ela decidiu contra isso, porque um Administrador Completo também tem direitos totais sobre todos os objetos que não estão no escopo, como 'Site' e 'Administrador'.

Como usar a administração delegada

Geralmente, o número de administradores e a granularidade de suas permissões dependem do tamanho e da complexidade da implantação.

- Em implantações pequenas ou de prova de conceito, um ou poucos administradores fazem tudo. Não há delegação. Nesse caso, crie cada administrador com a função de Administrador Completo integrada, que tem o escopo Todos.
- Em implantações maiores com mais máquinas, aplicativos e desktops, é necessária mais delegação. Vários administradores podem ter responsabilidades funcionais mais específicas (funções). Por exemplo, dois são Administradores Completos e outros são Administradores de Suporte Técnico. Além disso, um administrador pode gerenciar apenas certos grupos de objetos (escopos), como catálogos de máquinas. Nesse caso, crie novos escopos, além de administradores com uma das funções integradas e os escopos apropriados.
- Implantações ainda maiores podem exigir mais (ou mais específicos) escopos, além de diferentes administradores com funções não convencionais. Nesse caso, edite ou crie mais escopos, crie funções personalizadas e crie cada administrador com uma função integrada ou personalizada, além de escopos existentes e novos.

Para flexibilidade e facilidade de configuração, você pode criar escopos ao criar um administrador. Você também pode especificar escopos ao criar ou editar Catálogos de Máquinas ou conexões.

Criar e gerenciar administradores

Quando você cria um site como administrador local, sua conta de usuário se torna automaticamente um Administrador Completo com permissões totais sobre todos os objetos. Depois que um site é criado, os administradores locais não têm privilégios especiais.

A função de Administrador Completo sempre tem o escopo Todos; você não pode alterar isso.

Por padrão, um administrador é habilitado. Desabilitar um administrador pode ser necessário se você estiver criando o administrador agora, mas essa pessoa não iniciará as tarefas de administração até mais tarde. Para administradores habilitados existentes, você pode querer desabilitar vários deles enquanto reorganiza seus objetos/escopos e, em seguida, reabilitá-los quando estiver pronto para entrar em operação com a configuração atualizada. Você não pode desabilitar um Administrador Completo se isso resultar na ausência de um Administrador Completo habilitado. A caixa de seleção habilitar/desabilitar está disponível ao criar, copiar ou editar um administrador.

Ao excluir um par função/escopo ao copiar, editar ou excluir um administrador, ele exclui apenas o relacionamento entre a função e o escopo para esse administrador. Ele não exclui a função nem o escopo. Também não afeta nenhum outro administrador que esteja configurado com esse par função/escopo.

Para criar e gerenciar administradores, siga estas etapas:

1. Faça login no Web Studio, clique em **Administrators** no painel esquerdo e, em seguida, clique na guia **Administrators**.
2. Siga as instruções para a tarefa que deseja concluir:

    - **Criar um administrador:** Clique em **Create Administrator** na barra de ações. Digite ou procure o nome da conta de usuário, selecione ou crie um escopo e, em seguida, selecione uma função. O novo administrador é habilitado por padrão; você pode alterar isso.
    - **Copiar um administrador:** Selecione o administrador e, em seguida, clique em **Copy Administrator** na barra de ações. Digite ou procure o nome da conta de usuário. Você pode selecionar e, em seguida, editar ou excluir qualquer um dos pares função/escopo e adicionar novos. O novo administrador é habilitado por padrão; você pode alterar isso.
    - **Editar um administrador:** Selecione o administrador e, em seguida, clique em **Edit Administrator** na barra de ações. Você pode editar ou excluir qualquer um dos pares função/escopo e adicionar novos.
    - **Excluir um administrador:** Selecione o administrador e, em seguida, clique em **Delete Administrator** na barra de ações. Você não pode excluir um Administrador Completo se isso resultar na ausência de um Administrador Completo habilitado.

O painel superior exibe os administradores que você criou. Selecione um administrador para visualizar seus detalhes no painel inferior. A coluna **Warnings** indica se os pares de função e escopo associados ao administrador contêm funções ou escopos inutilizáveis. A seguinte mensagem de aviso aparece se um par de função e escopo associado contiver funções ou escopos inutilizáveis:

- Função ou escopo associado não utilizável

> **Importante:**
>
> Uma mensagem de aviso aparece apenas quando um par de função e escopo associado contém funções ou escopos inutilizáveis, ou ambos.
>
> Para remover o par função e escopo do administrador, conclua uma das seguintes etapas:

- Excluir o par de função e escopo.

    a. Na barra de ações, clique em **Editar Administrador**.

b. Na janela **Nome e Detalhes do Administrador**, selecione o par de função e escopo e clique em **Excluir**.

c. Clique em **Salvar** para sair.

- Excluir o administrador.

a. Na barra de ações, clique em **Excluir Administrador**.

b. Na janela de confirmação, clique em **Excluir**.

Criar e gerenciar funções

Quando os administradores criam ou editam uma função, eles podem habilitar apenas as permissões que eles próprios possuem. Isso impede que os administradores criem uma função com mais permissões do que as que eles têm atualmente e, em seguida, a atribuam a si mesmos (ou editem uma função à qual já estão atribuídos).

Os nomes de função podem conter até 64 caracteres Unicode; eles não podem conter: barra invertida, barra, ponto e vírgula, dois pontos, sinal de cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda ou para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo. As descrições podem conter até 256 caracteres Unicode.

Você não pode editar ou excluir uma função interna. Você não pode excluir uma função personalizada se algum administrador a estiver usando.

> **Observação:**
>
> Apenas certas edições do produto suportam funções personalizadas. Somente as edições que suportam funções personalizadas têm entradas relacionadas na barra de ações.

Para criar e gerenciar funções, siga estas etapas:

1. Faça login no Web Studio, clique em **Administradores** no painel esquerdo e, em seguida, clique na guia **Funções**.
2. Siga as instruções para a tarefa que você deseja concluir:

   - **Visualizar detalhes da função:** Selecione a função. O painel inferior lista os tipos de objeto e as permissões associadas para a função. Clique na guia **Administradores** no

painel inferior para visualizar uma lista de administradores que atualmente têm essa função.

- **Criar uma função personalizada:** Clique em **Criar Função** no painel de ações. Insira um nome e uma descrição. Selecione os tipos de objeto e as permissões.
- **Copiar uma função:** Selecione a função e clique em **Copiar Função** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
- **Editar uma função personalizada:** Selecione a função e clique em **Editar Função** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário.
- **Excluir uma função personalizada:** Selecione a função e clique em **Excluir Função** na barra de ações. Quando solicitado, confirme a exclusão.

Criar e gerenciar escopos

Ao criar um site, o único escopo disponível é o escopo 'Todos', que não pode ser excluído.

Você pode criar escopos usando o procedimento a seguir. Você também pode criar escopos ao criar um administrador; cada administrador deve ser associado a pelo menos um par de função e escopo. Ao criar ou editar desktops, catálogos de máquinas, aplicativos ou hosts, você pode adicioná-los a um escopo existente. Se você não os adicionar a um escopo, eles permanecerão parte do escopo 'Todos'.

A criação do site não pode ser escopada, nem os objetos de administração delegada (escopos e funções). No entanto, os objetos que você não pode escopar são incluídos no escopo 'Todos'. (Administradores Completos sempre têm o escopo Todos.) Máquinas, ações de energia, desktops e sessões não são diretamente escopados. Os administradores podem ter permissões alocadas sobre esses objetos por meio dos catálogos de máquinas ou grupos de entrega associados.

Regras para criar e gerenciar escopos:

- Os nomes de escopo podem conter até 64 caracteres Unicode. Os nomes de escopo não podem incluir: barra invertida, barra, ponto e vírgula, dois pontos, cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda, seta para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo.
- As descrições de escopo podem conter até 256 caracteres Unicode.
- Ao copiar ou editar um escopo, lembre-se de que a remoção de objetos do escopo pode tornar esses objetos inacessíveis ao administrador. Se o escopo editado for emparelhado com uma

ou mais funções, certifique-se de que as atualizações do escopo não tornem nenhum par função/escopo inutilizável.

Para criar e gerenciar escopos, siga estas etapas:

1. Faça login no Web Studio, clique em **Administradores** no painel esquerdo e, em seguida, clique na guia **Escopos**.
2. Siga as instruções para a tarefa que você deseja concluir:

   - **Criar um escopo:** Clique em **Criar novo Escopo** na barra de ações. Insira um nome e uma descrição. Para incluir todos os objetos de um tipo específico (por exemplo, Grupos de Entrega), selecione o tipo de objeto. Para incluir objetos específicos, expanda o tipo e selecione objetos individuais (por exemplo, Grupos de Entrega usados pela equipe de Vendas).
   - **Copiar um escopo:** Selecione o escopo e clique em **Copiar Escopo** na barra de ações. Insira um nome e uma descrição. Altere os tipos de objeto e os objetos, conforme necessário.
   - **Editar um escopo:** Selecione o escopo e clique em **Editar Escopo** na barra de ações. Altere o nome, a descrição, os tipos de objeto e os objetos, conforme necessário.
   - **Excluir um escopo:** Selecione o escopo e clique em **Excluir Escopo** na barra de ações. Quando solicitado, confirme a exclusão.

Configurar o gerenciamento de locatários

Configure o gerenciamento de locatários para criar partições de gerenciamento dentro de um único site do Citrix Virtual Apps and Desktops. Cada locatário possui recursos e configurações segregados, como catálogos de máquinas e grupos de entrega. Administradores com acesso a um locatário específico podem gerenciar apenas os recursos e configurações associados a esse locatário. Exemplos de casos de uso incluem empresas com diferentes silos de negócios (divisões independentes ou equipes de gerenciamento de TI separadas) em um único site.

Em um nível superior, o fluxo de trabalho para configurar o gerenciamento de locatários inclui:

1. Criar locatários
2. Adicionar administradores para locatários

Criar locatários

Crie um locatário criando um escopo de locatário. As etapas detalhadas são as seguintes:

1. Faça login no Web Studio, clique em **Administradores** no painel esquerdo e, em seguida, clique na guia **Escopos**.
2. Clique em *Criar Escopo** para iniciar a criação do locatário.
3. Insira os seguintes detalhes para o escopo do locatário:

    a. Digite um nome descritivo para o escopo. Este nome também serve como identificador do locatário.

    b. (Opcional) Insira uma breve descrição.

    c. Selecione **Escopo do locatário**.

    d. Se necessário, selecione os objetos associados ao locatário. Você também pode adicionar objetos a escopos de locatário ao criar ou gerenciar objetos.

    e. Clique em **OK** para concluir a criação.

Após a conclusão, você pode ver:

- O novo registro de escopo de locatário aparece na lista Escopo, identificado como **Locatário** na coluna **Tipo**.
- O nome do escopo é exibido na lista suspensa **Todos os Locatários**, localizada no canto superior direito do Web Studio.

Ao trabalhar com um escopo de locatário, tenha estas considerações em mente:

- A propriedade do locatário segue uma ordem de atribuição hierárquica: Hospedagem > Catálogos de Máquinas > Grupos de Entrega > Aplicativos. Objetos de nível inferior herdam a propriedade do locatário de objetos de nível superior. Por exemplo, ao selecionar um grupo de entrega para um escopo de locatário, certifique-se de também selecionar a hospedagem e o catálogo de máquinas associados. Caso contrário, o grupo de entrega não poderá herdar a propriedade do locatário.
- Após criar um escopo de locatário, você pode editar as atribuições de locatário modificando objetos. Quando uma atribuição de locatário é alterada, ela ainda está sujeita à restrição de que deve ser atribuída aos mesmos locatários ou a um subconjunto desses locatários. No entanto, objetos de nível inferior não são reavaliados quando as atribuições de locatário mudam. Certifique-se de que os objetos estejam devidamente restritos ao alterar as atribuições de locatário. Por exemplo, se um catálogo de máquinas estiver disponível para `TenantA` e `TenantB`, você pode criar um grupo de entrega para `TenantA` e outro para `TenantB`. (`TenantA` e `TenantB` estão ambos associados a esse catálogo de máquinas.)

Você pode então alterar o catálogo de máquinas para ser associado apenas a `TenantA`. Como resultado, o grupo de entrega associado a `TenantB` torna-se inválido.

Adicionar administradores para locatários

Adicione administradores para um locatário atribuindo contas de usuário com funções de administrador e locatários.

Para adicionar um administrador para um locatário, siga estas etapas:

1. Faça login no Web Studio, clique em **Administradores** no painel esquerdo e, em seguida, clique na guia **Administradores**.
2. Clique em **Adicionar Administrador** e siga estas etapas para concluir:
    a. Digite ou procure o nome da conta de usuário e clique em **Avançar**.
    b. Selecione **Acesso personalizado** e, em seguida, selecione uma ou mais funções (por exemplo, Administrador de Catálogo de Máquinas) conforme necessário.
    c. Clique em **Editar escopos** ao lado de cada função, altere o escopo de **Todos** para o escopo de locatário desejado e, em seguida, clique em **Salvar**.
3. Clique em **Avançar**.
4. Na página **Revisar e confirmar**, clique em **Enviar convite**.

Criar relatórios

Você pode criar dois tipos de relatórios de administração delegada:

- Um relatório HTML que lista os pares função/escopo associados a um administrador, além das permissões individuais para cada tipo de objeto (por exemplo, grupos de entrega e catálogos de máquinas). Você gera este relatório a partir do Web Studio.

  Para criar este relatório, siga estas etapas:

  a. Faça login no Web Studio, clique em **Administradores** no painel esquerdo
  b. Selecione um administrador e, em seguida, clique em **Criar Relatório** na barra de ações.

  Você também pode solicitar este relatório ao criar, copiar ou editar um administrador.
- Um relatório HTML ou CSV que mapeia todas as funções internas e personalizadas para permissões. Você gera este relatório executando um script PowerShell chamado OutputPermissionMapping.ps1.

Para executar este script, você deve ser um Administrador Completo, um Administrador Somente Leitura ou um administrador personalizado com permissão para ler funções. O script está localizado em: Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

Sintaxe:

`OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

PARÂMETRO	DESCRIÇÃO
`-Help`	Exibe a ajuda do script.
`-Csv`	Especifica a saída CSV. Padrão = HTML
`-Path string`	Onde gravar a saída. Padrão = stdout
`-AdminAddress string`	Endereço IP ou nome do host do Delivery Controller™ para conectar. Padrão = localhost
`-Show`	(Válido apenas quando o parâmetro `-Path` também é especificado) Ao gravar a saída em um arquivo, `-Show` faz com que a saída seja aberta em um programa apropriado, como um navegador da web.
Parâmetros Comuns	`Verbose`, `Debug`, `ErrorAction`, `ErrorVariable`, `WarningAction`, `WarningVariable`, `OutBuffer` e `OutVariable`. Para obter detalhes, consulte a documentação da Microsoft.

O exemplo a seguir grava uma tabela HTML em um arquivo chamado Roles.html e abre a tabela em um navegador da web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
```

```
-Path Roles.html –Show
```

O exemplo a seguir grava uma tabela CSV em um arquivo chamado Roles.csv. A tabela não é exibida.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Em um prompt de comando do Windows, o comando de exemplo anterior é:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

Controladores de Entrega

Observação:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O Delivery Controller é o componente do lado do servidor responsável por gerenciar o acesso do usuário, além de intermediar e otimizar conexões. Os Controladores também fornecem os Machine Creation Services™ que criam imagens de desktop e servidor.

Um site deve ter pelo menos um Controlador. Após instalar o Controlador inicial, você pode adicionar mais Controladores ao criar um site, ou posteriormente. Existem dois benefícios principais em ter mais de um Controlador em um site.

- **Redundância:** Como melhor prática, em um site de produção, sempre tenha pelo menos dois Controladores em servidores físicos diferentes. Se um Controlador falhar, os outros podem gerenciar as conexões e administrar o site.
- **Escalabilidade:** À medida que a atividade do site aumenta, o mesmo acontece com a utilização da CPU no Controlador e a atividade do banco de dados. Controladores adicionais permitem que você manipular mais usuários e mais solicitações de aplicativos e desktops, e podem melhorar a capacidade de resposta geral.

Cada Controlador se comunica diretamente com o banco de dados do site. Em um site com mais de uma zona, os Controladores em cada zona se comunicam com o banco de dados do site na zona primária.

> **Importante:**
>
> Não altere o nome do computador ou a associação ao domínio de um Controlador depois que o site for configurado.

Como os VDAs se registram nos Controladores

Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) com um Delivery Controller no site. Para obter informações sobre o registro de VDA, consulte Registro de VDA com Controladores.

Adicionar, remover ou mover Controladores

Para adicionar, remover ou mover um Controlador, você deve ter as permissões de função de servidor e função de banco de dados listadas no artigo Bancos de Dados.

A instalação de um Controlador em um nó em uma instalação de cluster SQL ou espelhamento SQL não é suportada.

Ao adicionar um Delivery Controller™ a um site, certifique-se de adicionar as credenciais de logon para essa máquina a quaisquer SQL Servers de réplica que você usa para alta disponibilidade.

Se sua implantação usa espelhamento de banco de dados:

- Antes de adicionar, remover ou mover um Controller, certifique-se de que os bancos de dados principal e espelhado estejam em execução. Além disso, se você estiver usando scripts com o SQL Server Management Studio, habilite o modo SQLCMD antes de executar os scripts.

- Para verificar o espelhamento após adicionar, remover ou mover um Controller, execute o cmdlet PowerShell `Get-configdbconnection`. Esse cmdlet garante que o Failover Partner tenha sido definido na string de conexão para o espelho.

Depois de adicionar, remover ou mover um Controller:

- Se a atualização automática estiver habilitada, os VDAs receberão uma lista atualizada de Controllers em até 90 minutos.
- Se a atualização automática não estiver habilitada, certifique-se de que a configuração da política do Controller ou a chave de registro ListOfDDCs sejam atualizadas para todos os VDAs. Depois de mover um Controller para outro site, atualize a configuração da política ou a chave de registro em ambos os sites.

Adicionar um Controller

Você pode adicionar Controllers ao criar um site e posteriormente. Não é possível adicionar Controllers instalados com uma versão anterior deste software a um site que foi criado com esta versão.

1. Execute o instalador em um servidor que contenha um sistema operacional compatível. Instale o componente Delivery Controller e quaisquer outros componentes principais que desejar. Conclua o assistente de instalação.
2. Se você ainda não criou um site, execute o Citrix Site Manager neste Controller para criar um site. O endereço IP deste Controller é adicionado automaticamente ao novo site.

   Se você planeja gerar scripts que inicializam os bancos de dados, adicione os Controllers antes de gerar os scripts.
3. Se você já criou um site, siga estas etapas:

   a. Execute o Citrix Site Manager neste Controller, clique em **Join an existing site** e digite o endereço de um Controller no site ao qual você deseja ingressar.

   b. Execute a ferramenta de configuração do Studio para adicionar o Controller ao Web Studio.

Remover um Controller

Remover um Controller de um site não desinstala o software Citrix ou qualquer outro componente. Essa ação remove o Controller do banco de dados para que ele não possa mais ser usado para intermediar conexões e executar outras tarefas. Se você remover um Controller, poderá adicioná-

lo novamente ao mesmo site ou a outro site. Um site requer pelo menos um Controller, portanto, você não pode remover o último listado no Web Studio.

Quando você remove um Controller de um site, o logon do Controller para o servidor de banco de dados não é removido. Isso evita a remoção potencial de um logon que é usado pelos serviços de outros produtos na mesma máquina. O logon deve ser removido manualmente se não for mais necessário. A permissão de função de servidor `securityadmin` é necessária para remover o logon.

Depois de remover um Controller:

- VDAs usando atualização automática se registram novamente com outros Controllers disponíveis. Esse novo registro ocorre somente se o mecanismo de atualização automática estiver habilitado e os VDAs puderem alcançar outros controllers (na mesma zona secundária que o Controller removido, ou na zona primária para implantações locais).
- Atualize as informações do Controller no Citrix StoreFront. Para obter mais informações, consulte Gerenciar Controllers.
- No Citrix StoreFront, atualize as URLs da Secure Ticket Authority (STA) para acesso remoto através do Citrix Gateway. Para obter mais informações, consulte Gerenciar Secure Ticket Authorities.
- No Citrix Gateway, atualize quaisquer URLs STA do servidor virtual. Para obter mais informações, consulte Citrix Gateway.

> **Importante:**
>
> Não remova o Controller do Active Directory antes de removê-lo do site.

1. Certifique-se de que o Controller esteja ligado para que o Web Studio possa carregar e exibir o Controller que você deseja remover.
2. Depois que o Web Studio tiver carregado completamente o Controller, verifique se todos os serviços no Controller estão em execução e se o Controller permanece ligado.
3. Faça login no Web Studio, selecione **Configurações** no painel esquerdo.
4. Localize o bloco **Delivery Controller** e clique em **Editar**.
5. Na página **Gerenciar Delivery Controller**, selecione o Controller que você deseja remover.

6. Selecione **Remover Controller**. Se você não tiver as funções e permissões de banco de dados corretas, será oferecida a opção de gerar um script que permite ao seu administrador de banco de dados remover o Controller para você.

   O Web Studio executa uma verificação prévia antes de remover um Controller. Um controller é seguro para remover se estiver desligado e não estiver no seguinte status de serviço:

   - Desconhecido
   - Falha pendente
   - Versão mais antiga
   - Versão mais recente
   - Alteração de versão em andamento
   - Recursos obrigatórios ausentes

   Se o Controller não estiver desligado e estiver em qualquer um dos status de serviço mencionados, o Web Studio solicitará que você desligue o Controller.

7. Você deve remover a conta de máquina do Controller do servidor de banco de dados. Antes de remover, verifique se outro serviço não está usando a conta.

Depois de usar o Web Studio para remover um Controller, o tráfego para esse Controller pode persistir por um curto período para garantir a conclusão adequada das tarefas atuais. Se você quiser forçar a remoção de um Controller em pouco tempo, a Citrix recomenda que você desligue o servidor onde ele foi instalado ou remova esse servidor do Active Directory. Em seguida, reinicie os outros Controllers no site para garantir que não haja mais comunicação com o Controller removido.

Mover um Controller para outra zona

Se o seu site contiver mais de uma zona, você poderá mover um Controller para uma zona diferente. Consulte as Zonas para obter informações sobre como essa movimentação pode afetar o registro de VDA e outras operações.

1. Selecione **Zona** no painel esquerdo.
2. Selecione uma zona no painel do meio e, em seguida, selecione um Controller.
3. Selecione **Mover Itens** na barra de ações.
4. Na página **Mover Itens** que aparece, selecione a zona para onde você deseja mover o Controller.
5. Clique em **Salvar**.

Mover um VDA para outro site

Se um VDA foi provisionado usando o Citrix Provisioning™ ou é uma imagem existente, você pode mover um VDA para outro site (do site 1 para o site 2) ao atualizar, ou ao mover uma imagem de VDA que foi criada em um site de teste para um site de produção. VDAs provisionados usando Machine Creation Services (MCS) não podem ser movidos de um site para outro. O MCS não oferece suporte à alteração da ListOfDDCs que um VDA verifica para se registrar em um Controller. VDAs provisionados usando MCS sempre verificam a ListOfDDCs associada ao site em que foram criados.

Existem duas maneiras de mover um VDA para outro site: usando o instalador ou as políticas do Citrix.

Instalador

Execute o instalador e adicione um Controller, especificando o FQDN (entrada DNS) de um Controller no site 2.

Especifique os Controllers no instalador apenas quando a configuração da política de Controllers não for usada.

Editor de Política de Grupo

O exemplo a seguir move vários VDAs entre sites.

1. Crie uma política no site 1 que contenha as seguintes configurações e, em seguida, filtre a política para o nível do Grupo de Entrega para iniciar uma migração em fases de VDA entre os sites.
    - Controllers: Contendo FQDNs (entradas DNS) de um ou mais Controllers no site 2.
    - Habilitar atualização automática de Controllers: definido como desabilitado.
2. Cada VDA no Grupo de Entrega é alertado dentro de 90 minutos sobre a nova política. O VDA ignora a lista de Controllers que recebe (porque a atualização automática está desabilitada); ele seleciona um dos Controllers especificados na política, que lista os Controllers no site 2.
3. Quando o VDA se registra com sucesso em um Controller no site 2, ele recebe a ListOfDDCs do site 2 e as informações da política, que têm a atualização automática habilitada por padrão. O Controller com o qual o VDA foi registrado no site 1 não está na lista enviada pelo Controller no site 2. Assim, o VDA se registra novamente, escolhendo entre os Controllers na lista do site 2. A partir de então, o VDA é automaticamente atualizado com informações do site 2.

Para obter informações sobre como usar o Editor de Política de Grupo, consulte a documentação de políticas do Citrix.

Suporte a IPv4/IPv6

Esta versão oferece suporte a implantações puras de IPv4, puras de IPv6 e de pilha dupla que usam redes IPv4 e IPv6 sobrepostas.

Os seguintes componentes suportam apenas IPv4. Todos os outros suportam IPv4 e IPv6.

- XenServer®
- Virtual Delivery Agents (VDAs) não controlados pela configuração de política **Only use IPv6 Controller registration**

As comunicações IPv6 são controladas com duas configurações de política Citrix® relacionadas à conexão do VDA.

- **Configuração principal que impõe o uso de IPv6:** Only use IPv6 Controller registration.

  Esta configuração de política controla qual forma de endereço o VDA usa para se registrar no Delivery Controller.

  Quando ativado, o VDA se registra e se comunica com o Controller usando um único endereço IPv6 escolhido na seguinte precedência: endereço IP global, Unique Local Address (ULA), endereço link-local (somente se nenhum outro endereço IPv6 estiver disponível).

  Quando desativado, o VDA se registra e se comunica com o Controller usando o endereço IPv4 da máquina. Este é o valor padrão.

  Se uma equipe usa frequentemente uma rede IPv6, publique os desktops e aplicativos para esses usuários com base em uma imagem ou Unidade Organizacional (OU) que tenha a configuração de política **Only use IPv6 Controller registration** ativada.

  Se uma equipe usa frequentemente uma rede IPv4, publique os desktops e aplicativos para esses usuários com base em uma imagem ou OU que tenha a configuração de política **Only use IPv6 Controller registration** desativada.
- **Configuração dependente que define uma máscara de rede IPv6:** Controller registration IPv6 netmask.

  Uma máquina pode ter vários endereços IPv6. Esta configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial, em vez de um IP global, se um estiver registrado. Esta configuração especifica a rede onde o VDA se registra. O VDA se registra apenas no primeiro endereço que corresponde à máscara de rede especificada.

Esta configuração é válida apenas quando a configuração de política **Only use IPv6 Controller registration policy** está ativada. Padrão = String vazia

Considerações de implantação

Se seu ambiente contiver redes IPv4 e IPv6, crie configurações de grupo de entrega separadas para clientes somente IPv4 e para clientes que podem acessar a rede IPv6. Considere usar nomes, atribuição manual de grupo do Active Directory ou filtros SmartAccess para diferenciar os usuários. A reconexão da sessão pode falhar se a conexão começar em uma rede IPv6 e, em seguida, você tentar se conectar novamente de um cliente que tem apenas acesso IPv4.

NOTA - Estas considerações não se aplicam se você tiver resolução de DNS ativada

Licenciamento para Citrix Virtual Apps and Desktops™ usando o Web Studio

Observação:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

No Web Studio, você pode gerenciar e rastrear o licenciamento, se o servidor de licenças estiver no mesmo domínio do Web Studio ou em um domínio confiável. Para obter informações sobre tarefas de licenciamento, consulte a documentação de licenciamento e Licenciamento de vários tipos.

A tabela a seguir lista as edições e modelos de licença suportados:

PRODUTOS	EDIÇÕES	MODELOS DE LICENÇA
Citrix Virtual Apps	Premium, Advanced, Standard	Concorrente
Citrix Virtual Desktops	Premium, Advanced, Standard	Usuário/Dispositivo e Concorrente

Para obter mais informações, consulte Licença Concorrente e Licença de Usuário/Dispositivo.

Versão de Lançamento Atual (CRs) e Lançamento de Serviço de Longo Prazo (LTSRs) suportadas

A Citrix recomenda fortemente que você sempre use a versão mais recente disponível do Citrix License Server para se beneficiar de quaisquer melhorias funcionais ou de segurança que ela possa conter.

> **Observação:**
>
> O License Server VPX foi descontinuado e não receberá mais manutenção ou correções de segurança. Os clientes que usam a versão 11.16.6 ou anteriores do License Server VPX são aconselhados a migrar para a versão mais recente do License Server para Windows o mais rápido possível.

> Para obter mais informações sobre as datas de ciclo de vida dos produtos Citrix, consulte Matriz de Produtos.

Para obter informações sobre produtos e versões de produtos legados, consulte a Matriz de Produtos Legados.

Você deve ser um administrador de licenças completo para concluir as seguintes tarefas. Para visualizar informações de licença no Web Studio, um administrador deve ter pelo menos a permissão de administração delegada de Leitura de Licenciamento. As funções integradas de Administrador Completo e Administrador Somente Leitura possuem essa permissão.

Baixar e instalar uma licença da Citrix usando o Web Studio

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Alocar Licenças** na barra de ações.
3. Insira o Código de Acesso da Licença. Você o recebeu em um e-mail da Citrix após a compra ou renovação das licenças.
4. Selecione um produto e escolha **Alocar Licenças**. As licenças disponíveis para esse produto são alocadas e baixadas. Depois de alocar e baixar todas as licenças para um Código de Acesso de Licença específico, você não poderá reutilizar esse Código de Acesso de Licença. Para fazer outras transações com o mesmo código, faça login em Minha Conta.

Adicionar licenças armazenadas no seu computador local ou na rede

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Adicionar Licenças** na barra de ações.
3. Navegue até um arquivo de licença e adicione-o ao servidor de licenças.

Alterar o servidor de licenças

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Alterar Servidor de Licenças** na barra de ações.
3. Digite o endereço do servidor de licenças no formato *nome:porta*, onde o nome é um endereço DNS, NetBIOS ou IP. Se você não especificar um número de porta, a porta padrão (27000) será usada.

Selecione o tipo de licença a ser usado

- Ao configurar o Site, depois de especificar o servidor de licenças, você será solicitado a selecionar o tipo de licença a ser usado. Se não houver licenças no servidor, a opção de usar o produto por um período de teste de 30 dias sem licença será selecionada automaticamente.
- Se houver licenças no servidor, seus detalhes serão exibidos e você poderá selecionar uma delas. Ou, você pode adicionar um arquivo de licença ao servidor e depois selecioná-lo.

Alterar a edição do produto e o modelo de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione **Editar Edição do Produto** na barra de ações.
3. Atualize as opções apropriadas.

Para acessar o Console de Administração de Licenças, na barra de ações, selecione **Console de Administração de Licenças**. O console aparece imediatamente ou, se o painel estiver configurado com proteção por senha, você será solicitado a fornecer as credenciais do Console de Administração de Licenças. Para obter detalhes sobre como usar o console, consulte a documentação de licenciamento.

> **Observação:**
>
> Ao alternar licenças no Web Studio, a alteração leva até 5 minutos para aparecer no Citrix Director. Por exemplo, se você alternar entre Advanced e Premium.

Adicionar um administrador de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento**.
3. Selecione **Adicionar administrador de licenciamento** na barra de ações.
4. Procure o usuário que você deseja adicionar como administrador e escolha as permissões.

Alterar as permissões de um administrador de licenciamento ou excluir um administrador de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento** e, em seguida, selecione o administrador.
3. Selecione **Editar administrador de licenciamento** ou **Excluir administrador de licenciamento** na barra de ações.

Adicionar um grupo de administradores de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento**.
3. Selecione **Adicionar grupo de administradores de licenciamento** na barra de ações.
4. Procure o grupo que você deseja que atue como administradores de licenciamento e escolha as permissões. Adicionar um Grupo do Active Directory concede permissões de administrador de licenciamento aos usuários dentro desse grupo.

Alterar as permissões de um grupo de administradores de licenciamento ou excluir um grupo de administradores de licenciamento

1. Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo.
2. Selecione a guia **Administradores de Licenciamento** e, em seguida, selecione o grupo de administradores.
3. Selecione **Editar grupo de administradores de licenciamento** ou **Excluir grupo de administradores de licenciamento** na barra de ações.

Visualizar informações de licença

Faça login no Web Studio e selecione **Licenciamento** no painel esquerdo. Um resumo do uso da licença e das configurações do Site é exibido com uma lista de todas as licenças atualmente instaladas no servidor de licenças especificado.

Certifique-se de que as configurações de licenciamento para o site, que incluem o tipo de produto, edição da licença e modelo de licenciamento, correspondam às licenças que seu Servidor de Licenças configurado usa. Caso contrário, você pode ter que baixar ou alocar suas licenças existentes para corresponder às configurações de licença do site.

Execute o comando `Get-Brokersite` para obter as seguintes informações de licenciamento:

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **Observação:**
>
> Use as APIs de licenciamento em nuvem para obter as informações no Citrix DaaS. Para obter informações sobre as APIs de licenciamento em nuvem, consulte APIs para gerenciar o licenciamento do Citrix Cloud.

Visualizar alertas de expiração de licença

O Web Studio consulta as datas de expiração dos arquivos de licença do Citrix License Server. O Web Studio alerta os administradores na guia Visão Geral se os arquivos de licença estão próximos da expiração ou já expiraram.

Links relacionados

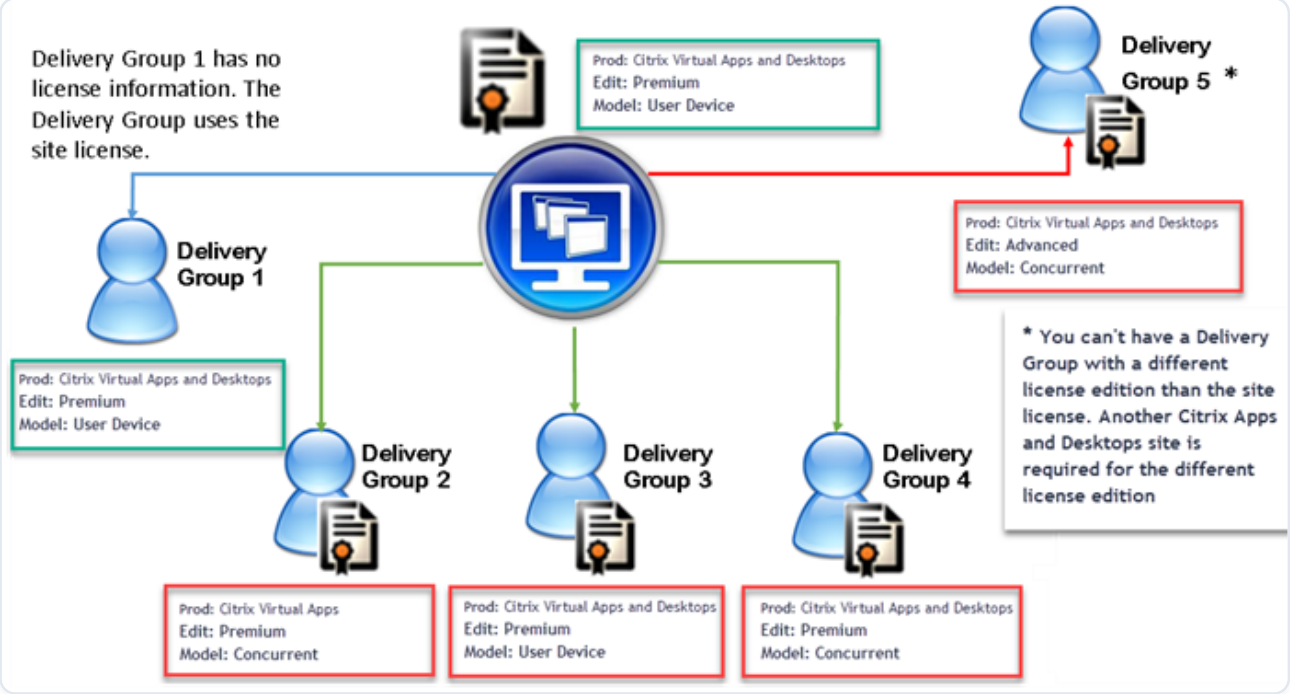
- Consulte Assinatura local da Citrix para licenças de varejo anuais e baseadas em prazo.
- Consulte Transição e Upgrade (TTU) com Direitos Híbridos.

Licenciamento multitipo

O licenciamento multitipo suporta o consumo de diferentes tipos de licença para grupos de entrega em um único site do Citrix Virtual Apps and Desktops. **Tipo** é uma única combinação de ID do Produto (XDT ou MPS) e Modelo (UserDevice ou Concurrent). Os grupos de entrega devem usar a mesma Edição do Produto (PLT/Premium ou ENT/Advanced) configurada no nível do site.

Esteja ciente das considerações especiais no final deste artigo ao configurar o licenciamento multitipo para suas implantações do Citrix Virtual Apps and Desktops.

Se o licenciamento multitipo não estiver configurado, diferentes tipos de licença só poderão ser usados quando configurados para sites separados. Os grupos de entrega usam a licença do site. Para limitações importantes de notificação quando o licenciamento multitipo estiver configurado, consulte Considerações especiais.



Para determinar os grupos de entrega que consomem os diferentes tipos de licenças, use estes cmdlets do Broker PowerShell:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Para instalar licenças, use:

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

As datas do Customer Success Services são específicas para cada arquivo de licença e para cada produto e modelo. Grupos de entrega configurados de forma diferente podem ter datas de Customer Success Services diferentes entre si.

Considerações especiais

O licenciamento multitipo tem funcionalidade diferente do licenciamento regular do Citrix Virtual Apps and Desktops™.

Não há alertas e notificações do Director ou Studio para grupos de entrega configurados para usar um tipo que difere da configuração do site:

- Nenhuma informação ao se aproximar dos limites de licença ou do acionamento ou expiração do modo de intermitência de licença.
- Nenhuma notificação quando um grupo específico tem um problema.

Grupos de entrega configurados para licenças de múltiplos tipos consomem APENAS esse tipo de licença e não retornam à configuração do site quando totalmente consumidos.

Embora os nomes das edições de licença Citrix Virtual Apps Standard e Citrix Virtual Desktops™ Standard indiquem que ambos são Standard, eles não são a mesma edição. O licenciamento de múltiplos tipos não está disponível com licenças Citrix Virtual Apps Standard e Citrix Virtual Desktop Standard.

Matriz de compatibilidade de licenças

Esta tabela detalha nomes de produtos antigos, novos nomes de produtos e os nomes de recursos associados. As quatro colunas de compatibilidade especificam quais combinações de produto e modelo de licença são compatíveis para licenciamento de múltiplos tipos. CCU e CCS significam licenças concorrentes e UD são licenças de usuário/dispositivo.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

SDK do Broker PowerShell

O objeto **DesktopGroup** possui estas duas propriedades que você pode manipular usando os cmdlets New-BrokerDesktopGroup e Set-BrokerDesktopGroup associados.

NOME	VALOR	RESTRIÇÃO
LicenseModel	Um parâmetro (Concorrente ou Usuário/Dispositivo) que especifica o modelo de licenciamento para o grupo. Se nenhum for especificado, o modelo de licença de todo o site será usado.	Se a alternância de recurso estiver desativada, a tentativa de definir uma propriedade falhará.
ProductCode	Uma string de texto de XDT (para Citrix Virtual Desktops) ou MPS (para Citrix Virtual Apps™) especificando o ID do Produto de licenciamento para o grupo. Se nenhum for especificado, o código do produto de todo o site será usado.	Se a alternância de recursos estiver desativada, a tentativa de definir uma propriedade falhará.

Para obter mais informações sobre o LicenseModel e o ProductCode, consulte about_Broker_Licensing.

New-BrokerDesktopGroup

Cria um grupo de desktops para gerenciar a corretagem de grupos de desktops. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`.

Set-BrokerDesktopGroup

Desativa ou ativa um grupo de desktops de corretor existente ou altera suas configurações. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`

Get-BrokerDesktopGroup

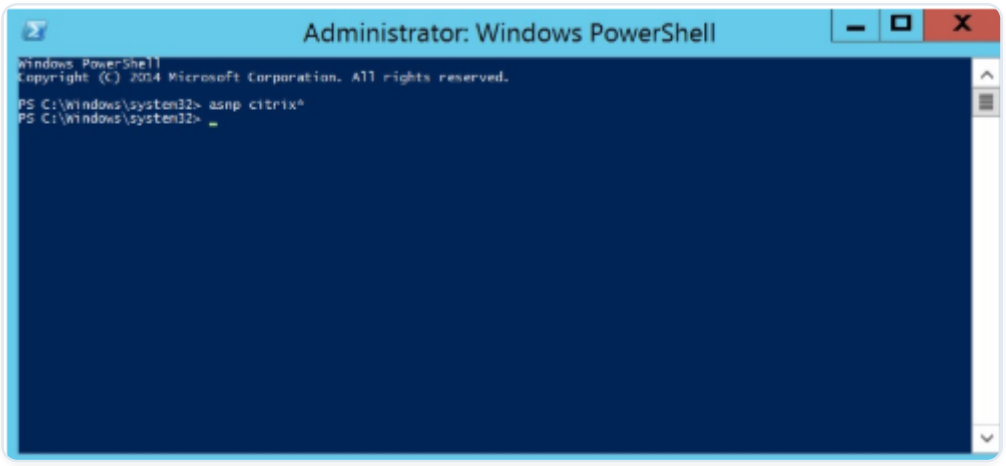
Recupera grupos de desktops que correspondem aos critérios especificados. A saída do cmdlet Get-BrokerDesktopGroup inclui as propriedades **ProductCode** e **LicenseModel** do grupo. Se as propriedades não tiverem sido definidas usando New-BrokerDesktopGroup ou Set-BrokerDesktopGroup, valores nulos serão retornados. Se nulo, o modelo de licença e o código do produto de todo o site serão usados. Para obter mais informações sobre este cmdlet, consulte

`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`.

Configurar diferentes produtos e modelos de licença por grupo de entrega

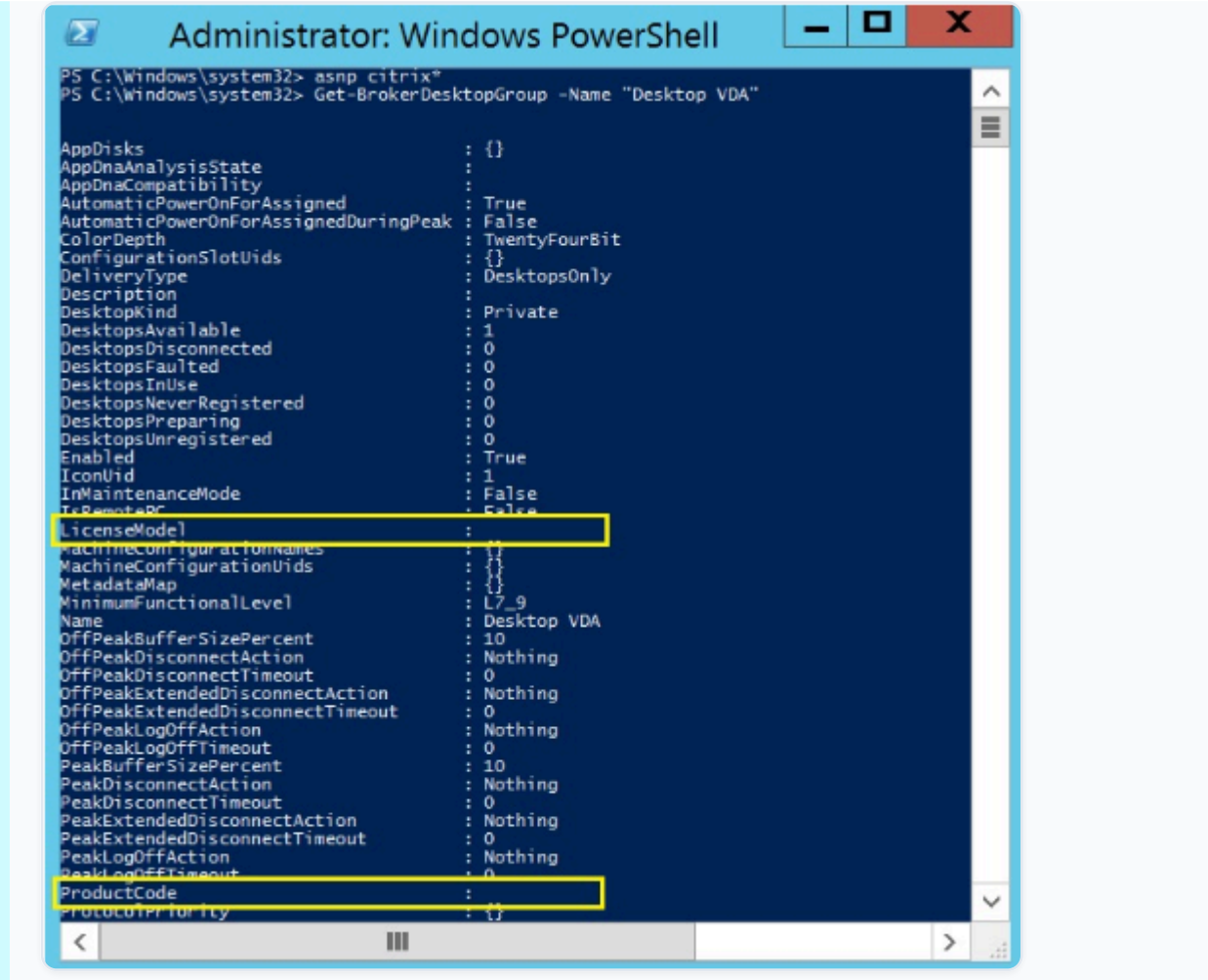
> **Observação:**
>
> Não é possível configurar dois ou mais tipos diferentes de produtos, edições ou modelos de licença em um único grupo de entrega. Caso você tenha diferentes tipos de produtos, edições ou modelos de licença, configure-os em grupos de entrega separados.

1. Abra o PowerShell com direitos administrativos e adicione o snap-in do Citrix.

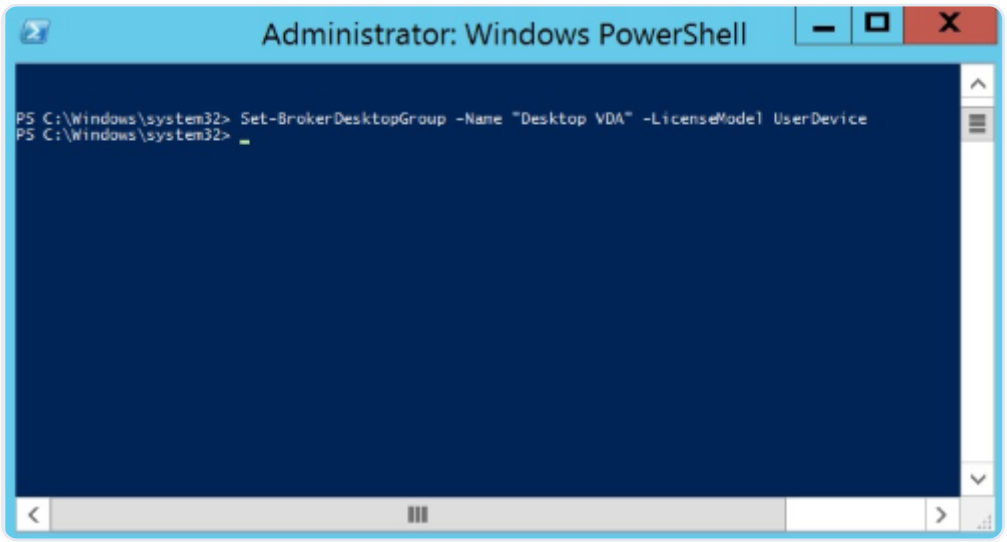


2. Execute o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para visualizar a configuração de licença atual. Encontre os parâmetros **LicenseModel** e **ProductCode**. Se você não configurou esses parâmetros antes, eles podem estar em branco.

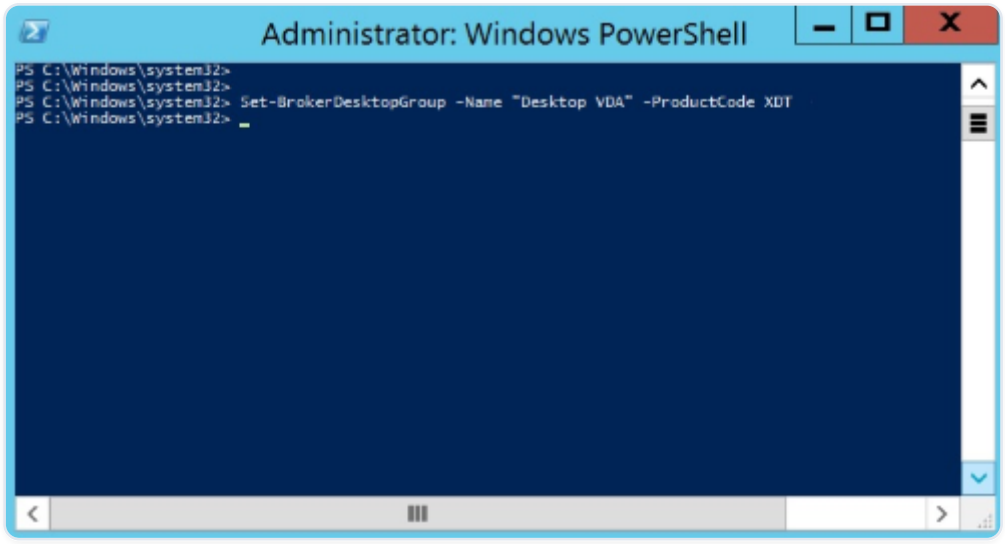
> **Observação:**
>
> Se um grupo de entrega não tiver informações de licença definidas, ele usará como padrão a **licença de site no nível do site**.



3. Altere o modelo de licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**.

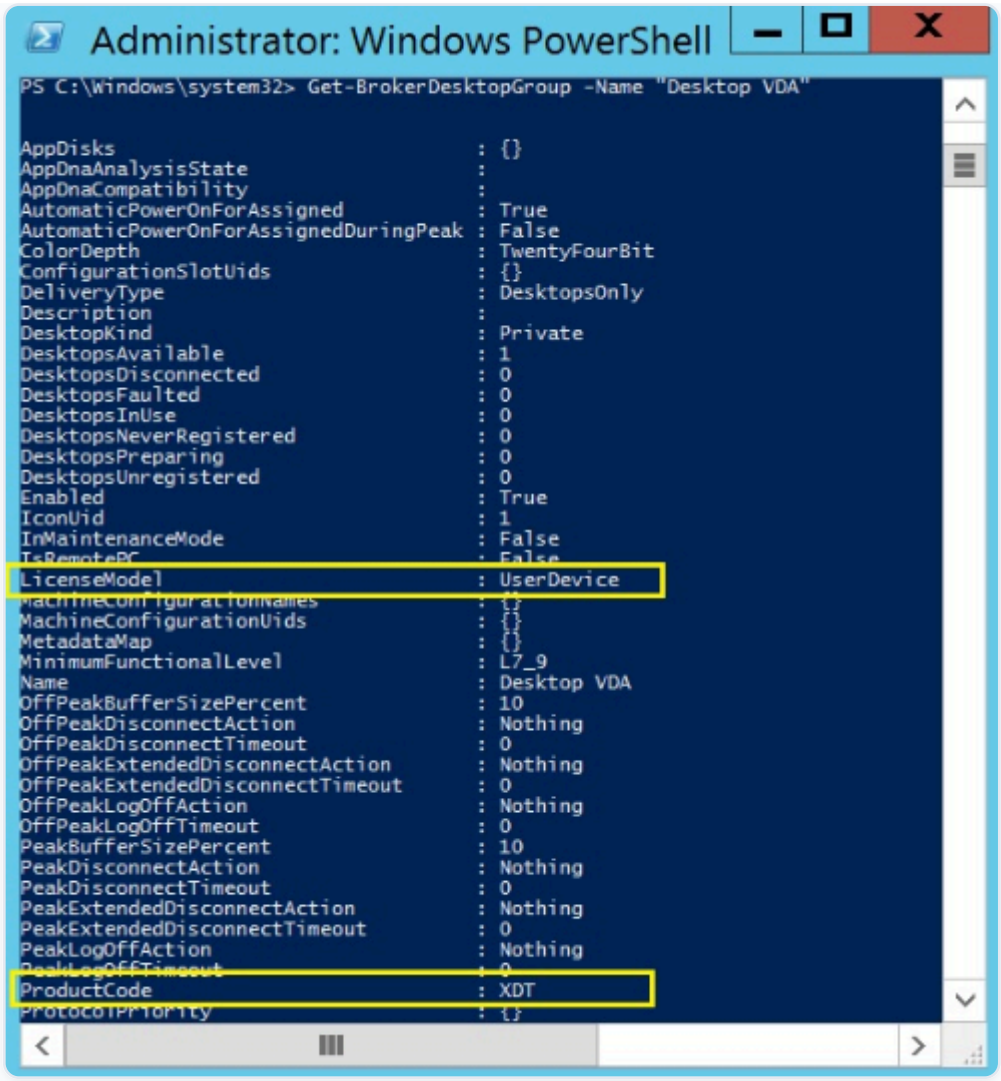


4. Altere o produto da licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**.



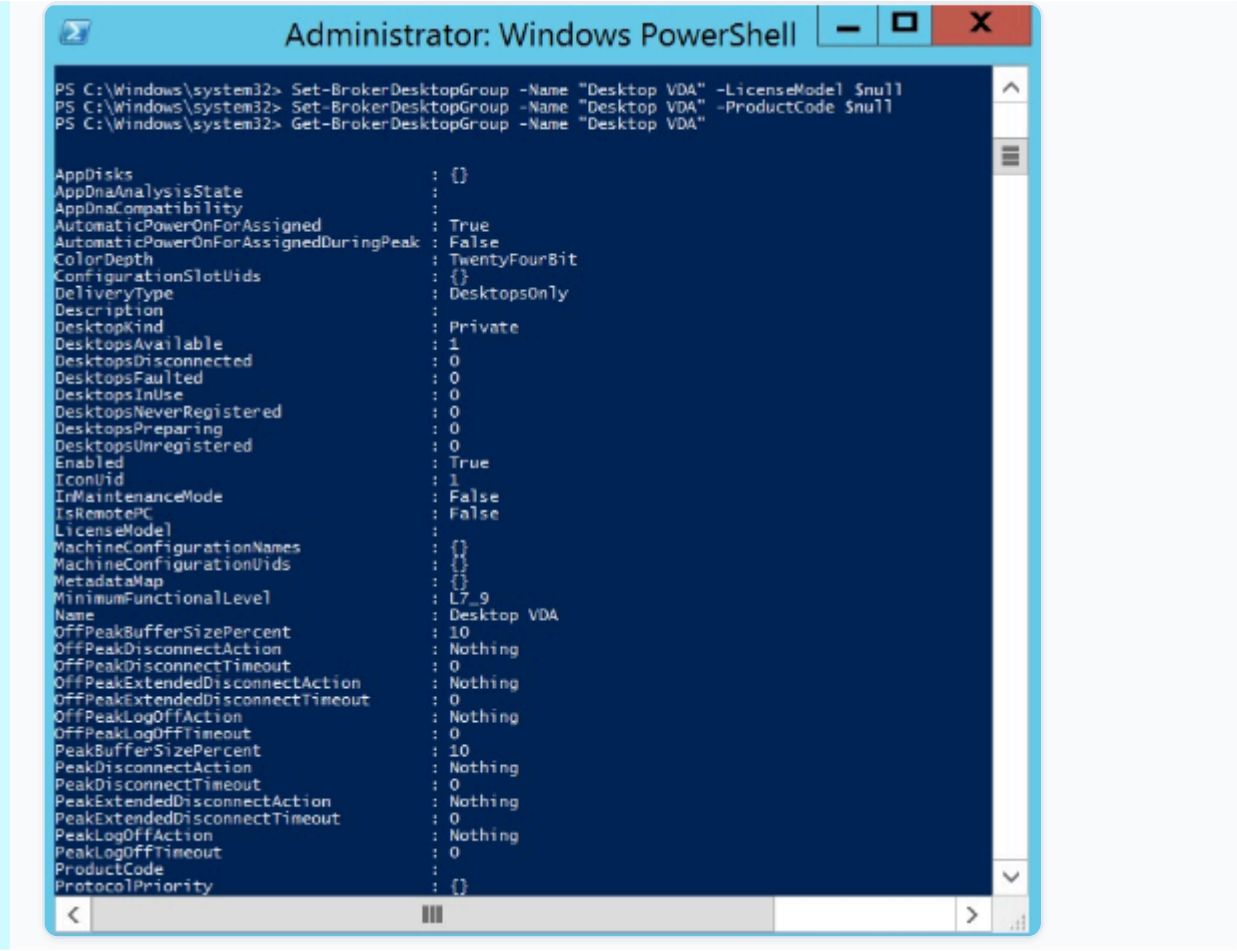
5. Insira o comando **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** para validar as alterações.

> **Observação:**
>
> Não é possível misturar e combinar edições no mesmo site. Por exemplo, licenças Premium e Advanced. Vários sites são necessários se você tiver licenças com edições diferentes.



6. Remova a configuração da licença executando os mesmos comandos **Set-BrokerDesktopGroup** conforme descrito nas etapas anteriores e defina o valor como **$null**.

> **Observação:**
>
> O Studio não exibe a configuração de licença para cada grupo de entrega. Use o PowerShell para visualizar a configuração atual.



Exemplo

Este exemplo de cmdlet do PowerShell ilustra a configuração de licenciamento de vários tipos para dois grupos de entrega existentes e cria e configura um terceiro grupo de entrega.

Para ver o produto da licença e o modelo de licença associados a um grupo de entrega, use o cmdlet do PowerShell **Get-BrokerDesktopGroup**.

1. Configuramos o primeiro grupo de entrega para XenApp® e Concorrente.

   Set-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Apps Premium Concurrent" -ProductCode MPS -LicenseModel Concurrent

2. Configuramos o segundo grupo de entrega para XenDesktop® e Concorrente.

   Set-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Desktops Premium Concurrent" -ProductCode XDT -LicenseModel Concurrent

3. Criamos e configuramos o terceiro grupo de entrega para XenDesktop e UserDevice.

New-BrokerDesktopGroup -Name "Grupo de entrega para Citrix Virtual Desktops Premium UserDevice" -PublishedName "MeuDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Elementos de dados de telemetria do Citrix Virtual Apps and Desktops™

Broker

Uso

CABEÇALHOS

CHAVE	DESCRIÇÃO	EXEMPLO
Versão	Indica a versão do evento de telemetria.	1
id	Indica um identificador exclusivo do evento de uso.	d4ce7919-5d80-44de-a8fa-102923fe0ead
Tipo	Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem.	SendBrokerTelemetryData
st	Indica o carimbo de data/hora quando o evento é gerado no Broker.	2011-08-12T20:17:46.384Z
produção	Identifica o produto de origem e a implantação do evento de uso.	XenDesktop.Broker (Cloud) OnPrem.Broker (OnPrem)
prodVer	Indica a versão do produto Citrix DaaS/ Citrix Virtual Apps and Desktops.	7.25.0.0

CARGA ÚTIL

CAMPO	DESCRIÇÃO	EXEMPLO
TotalPublishedApps	Indica o número total de aplicativos publicados.	10
TotalPublishedDesktops	Indica o número total de Desktops publicados.	10
VDAs.Total	Indica o número total de VDAs.	10
VDAs.OSTypes	Indica o número total de VDAs por tipo de SO, como Windows, Linux e Mac.	10
VDAs.OSVersions	Indica o número total por versões de SO, como Windows 10, 11, 2022, 2019.	10
VDAs.HostingLocations.Azure	Indica o número de VDAs para cada local de hospedagem compatível, como Azure, AWS, GCP, Nutanix, VMWare, XenServer e HyperV.	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Indica o número de máquinas provisionadas pelo Machine Creation Service (MCS).	10

CAMPO	DESCRIÇÃO	EXEMPLO
VDAs.ProvisionedMethod.ManualOr3P	Indica o número de máquinas provisionadas manualmente ou por 3P.	10
VDAs.SessionSupport.StaticSingle	Indica o número de máquinas com sessão única atribuída estaticamente.	10
VDAs.SessionSupport.DynamicSingle	Indica o número de máquinas com sessão única atribuída dinamicamente.	10
VDAs.SessionSupport.Multi	Indica o número total de máquinas multi-sessão.	10
VDAs.RemotePCAccess.Windows	Indica o número de máquinas de Acesso Remoto a PC por tipo de SO (Win, Mac, Linux).	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	Indica o número de VDAs com agentes de gravação de sessão ativos.	5
VDAs.Subscriptions	Indica o número de assinaturas de nuvem pública de VDAs.	2
VDAs.LocationTypes	Indica o número de tipos de localização de VDAs.	2
AutoScale.DGWithAutoscaleEnabled	Indica o número de grupos de entrega com **Autoscale** Ativado.	2
AutoScale.TotalMachinesCtrlByAutoscale	Indica o número de máquinas controladas pelo autoscale.	5

CAMPO	DESCRIÇÃO	EXEMPLO
AutoScale.VerticalAutoscaleEnabledByDGandSite	Indica o número de máquinas com **Autoscale Vertical** habilitado por DG e Site.	2
AutoScale.TaggedBasedAutoscaledDG	Indica o número de grupos de entrega com autoscale baseado em tags.	2
DeliveryGroup.TotalRebootSchedulesEnabled	Indica o número de grupos de entrega com **Agendamentos de Reinicialização** habilitados.	2
DeliveryGroup.Total	Indica o número total de grupos de entrega.	10
Policy.TotalPolicySets	Indica o número de conjuntos de políticas.	3
Policy.TotalPolicies	Indica o número de políticas de grupo.	2
Policy.TotalPolicySettings	Indica o número de configurações de grupo.	2
PublishedPackageApps.AppVSingleAdmin	Indica o número total de aplicativos empacotados publicados no modo AppV Single Admin.	2
PublishedPackageApps.AppVDualAdmin	Indica o número total de aplicativos empacotados publicados no modo AppV Dual Admin.	2
PublishedPackageApps.Msix	Indica o número total de aplicativos empacotados publicados no modo MSIX.	2
PublishedPackageApps.AppAttach	Indica o número total de aplicativos empacotados	2

CAMPO	DESCRIÇÃO	EXEMPLO
	publicados no modo AppAttach.	
PublishedPackageApps.FlexApp	Indica o número total de aplicativos empacotados publicados no modo FlexApp.	2

Sessão

CABEÇALHOS

CAMPO	DESCRIÇÃO	EXEMPLO
Versão	Indica a versão do evento de uso da licença.	1
id	Indica um identificador exclusivo do evento de uso.	d4ce7919-5d80-44de-a8fa-102923fe0ead
tipo	Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem.	Cloud.Licensing
st	Indica o carimbo de data/hora quando o evento é gerado no Broker.	2011-08-12T20:17:46.384Z
produto	Identifica o produto de origem e a implantação do evento de uso.	XenDesktop.Broker (Cloud) OnPrem.Broker (OnPrem)
prodVer	Indica a versão do produto Citrix DaaS	7.25.0.0

CAMPO	DESCRIÇÃO	EXEMPLO
	ou Citrix Virtual Apps and Desktops.	
usuário	Identifica o ID do Usuário para identificar de forma exclusiva um usuário que inicia o lançamento da sessão. **O valor é embaralhado.**	fullName: C648FE671A44B3F7 **(sempre embaralhado)** samName:C758LH671A44B3F7 **(sempre embaralhado)** upn: C7948FE671A44B3F7 **(sempre embaralhado)** userLicenseId:C265FE671A44B3F7 **(sempre embaralhado)** userSid: C097FE671A44B3F7 **(sempre embaralhado)**
tenant para id	Indica o ID do Cliente da conta Citrix Cloud™. Para a implantação local, este campo não é aplicável e não possui valor.	joj1mh0598tj
dvc para dvcId	Indica o ID do dispositivo para identificar de forma exclusiva um dispositivo de onde o	AE18C4D5

CAMPO	DESCRIÇÃO	EXEMPLO
	lançamento da sessão é iniciado.	
dvc para dvcName	Indica o nome amigável para o dispositivo. **O valor é embaralhado.**	C758LH671A44B3F7 **(sempre embaralhado)**

CARGA ÚTIL

CAMPO	DESCRIÇÃO	EXEMPLO
appProtectionKeyLoggingRequired	Indica se a sessão é iniciada com a Proteção contra Registro de Teclas ativada.	Falso
appProtectionScreenCaptureRequired	Indica se a sessão é iniciada com a Proteção contra Captura de Tela ativada.	Falso
cspTenantCustomerId	Indica o ID do Cliente de uma conta Citrix Cloud de um locatário CSP. Para a implantação local, este campo não é aplicável e não possui valor.	6c2vtxgxyftt
isAnonymousUser	Indica se uma sessão não autenticada é iniciada.	Falso
licenseActivityTimeStamp	Indica o carimbo de data/hora quando o payload é gerado.	2011-08-12T20:17:46.384Z

CAMPO	DESCRIÇÃO	EXEMPLO
licenseActivityType	Indica o tipo de evento de licenciamento. Este campo indica se o tipo de evento de licenciamento é para ação de atribuição ou liberação.	Conectar
licenseModel	Indica o modelo de licença da implantação.	UserDevice
productEdition	Indica a edição do produto da implantação.	Premium
productId	Indica o ID do produto do produto na implantação.	CAVDS
protocolo	Indica o protocolo usado para iniciar a sessão.	HDX™
sessionKey	Indica um identificador exclusivo para a sessão.	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	Indica o tipo de suporte de sessão.	SingleSession
sessionType	Indica o tipo de sessão.	Application
versão	Indica a versão do payload.	1.3
workerSid	Indica um identificador exclusivo para o	1E5LH671A44B3F7 **(sempre embaralhado)**

CAMPO	DESCRIÇÃO	EXEMPLO
	VDA usado na sessão.**O valor é embaralhado.**	
isWindows365	Indica se a sessão é iniciada para o Windows 365.	Verdadeiro
entitlementType	Indica o tipo de direito de licença do Cliente.	Produção
siteId	Indica um identificador exclusivo para o site.	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	Indica um identificador exclusivo para o Grupo de Área de Trabalho ou de Entrega.	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Indica o tipo de aplicativo Citrix Workspace™.	Windows
clientVersion	Indica a versão do aplicativo Citrix Workspace.	23.5.1.83
workerCloudType	Indica o tipo de nuvem pública usado para o provisionamento de VDA.	Azure
enabledFeatures	Indica os recursos habilitados para a sessão. Por exemplo, em uma sessão onde	66

CAMPO	DESCRIÇÃO	EXEMPLO
	`AppProtectionScreenCaptureRequired` e `SessionRecording` estão habilitados, o valor deste campo é 66.	
launchRequestSource	Registra o produto usado para solicitar o lançamento. Pode ser On-prem StoreFront™ ou Cloud StoreFront.	0 (StoreFront ou 3P) 1 (Workspace)
isEvents	Indica as falhas críticas em {{page.lic}}.	Não foi possível criar o banco de dados ST.
heartBeatTime	Indica o tempo de pulsação do servidor de licenças para CIS ou Citrix Analytic Service.	1689058813
vdaTelemetry	Indica o payload que é capturado para App Layering, User Personalization Layer, User Profile management, Workspace Environment Management™ e recursos HDX.	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1

CAMPO	DESCRIÇÃO	EXEMPLO
		CPM_version: 22.3.4000 wem_enableMethod : 1 wem_agentVersion: 2402.1

Studio

Uso

CABEÇALHOS

CAMPO	DESCRIÇÃO	EXEMPLO
Versão	Indica a versão do evento de uso da licença.	1
id	Indica um identificador exclusivo do evento de uso.	8c2e20a5-ca3f-4401-ad69-d037933c40a0
Tipo	Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso na nuvem	Studio.Usage
st	Indica o carimbo de data/hora quando o evento é gerado no Studio.	2024-03-22T01:32:23.4056195Z
produção	Identifica o produto de origem e a implantação do evento de uso.	XenDesktop.Studio
prodVer	Indica a versão do produto Citrix DaaS/Citrix Virtual Apps and Desktops	7.42.0.0

CARGA ÚTIL

CAMPO	DESCRIÇÃO	EXEMPLO
AdminLoginList	Indica a lista de SamAccountName de administradores exclusivos. **O valor é embaralhado.**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(sempre embaralhado)**
TotalApiRequests	Indica as solicitações de API do serviço de Orquestração.	{TotalApiRequests: 1000}
BackupCount	Indica a contagem de backups que foi operada pelo administrador do Studio.	{BackupCount: 200}
RestoreCount	Indica a contagem de restaurações que foi operada pelo administrador do Studio.	{RestoreCount: 20}

Director

Relatório de uso

CABEÇALHOS

CAMPO	DESCRIÇÃO	EXEMPLO
Ver.	Indica a versão do evento de uso da licença.	1
id	Indica um identificador exclusivo do evento de uso.	8c2e20a5-ca3f-4401-ad69-d037933c40a0
Tipo	Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem.	Telemetria
st	Indica o carimbo de data/hora quando o evento é gerado no Studio.	2024-03-22T01:32:23.4056195Z

CAMPO	DESCRIÇÃO	EXEMPLO
Produção	Identifica o produto de origem e a implantação do evento de uso.	XenApp.Monitor
prodVer	Indica a versão do produto Director.	7.42.0.0

CARGA ÚTIL

CAMPO	DESCRIÇÃO	EXEMPLO
AdminLoginCount	Esta é uma seção da carga útil que fornece a contagem de logins de administrador.	tipo: AdminLogin estatísticas 0: 1 1: 7
FeatureUsageCount	Esta seção do payload contém a contagem de recursos principais usados no Director.	tipo: Uso de Recurso estatísticas 0: 15 1: 20 5: 10
OdataUsageCount	Esta seção do payload contém a contagem de uso da API Odata.	tipo: OData_v3 estatísticas 0: 1 2: 7 5: 9 tipo: OData_v4 estatísticas 0: 1

CAMPO	DESCRIÇÃO	EXEMPLO
		2: 8 6: 7
AppUsage	Indica as métricas de uso semanais dos aplicativos publicados.	tipo: AppUsage cabeçalhos: applicationName,processName,totalDurationInMinutes período: 01/05/24-07/05/24 valores: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	Indica a contagem de usuários únicos juntamente com o total de inicializações de aplicativos em um mês para aplicativos publicados.	tipo: UniqueAppUsers cabeçalhos: applicationName,totalLaunches,totalUniqueUsers período: 04/24 valores: [Calc_AWTSVDA-1907R,100,10,

CAMPO	DESCRIÇÃO	EXEMPLO
		Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	Indica as métricas de uso semanais de desktops publicados.	tipo: DesktopUsage cabeçalhos: desktopGroupName,sessionSupport,totalDurationInMinutes período: 01/05/24-07/05/24 valores: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	Indica a contagem de usuários únicos juntamente com o total de inicializações em um mês para desktops publicados.	tipo: UniqueDesktopUsers cabeçalhos: desktopGroupName,totalLaunches,totalUniqueUsers período: 04/24 valores: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	Indica a duração média do logon.	tipo: AvgLogonDuration cabeçalhos: totalUserLogons, avgLogonDurationInSeconds

CAMPO	DESCRIÇÃO	EXEMPLO
		período: 01/05/24-07/05/24 valores: [200,4]
CostSaved	Indica o custo economizado pelo cliente em um mês.	tipo: CostSaved cabeçalhos: hypervisor,costSaved,currency período: 04/24 valores: [1,221.02,1 2,301.02,2]

Administrador Delegado

Uso

CABEÇALHOS

CHAVE	DESCRIÇÃO	EXEMPLO
versão	Indica a versão do evento de uso da licença.	1
id	Indica um identificador exclusivo do evento de uso.	8c2e20a5-ca3f-4401-ad69-d037933c40a0
tipo	Indica o tipo de evento usado pelo Citrix Analytic Service para identificar eventos de uso da nuvem.	DelegatedAdmin.Usage
st	Indica o carimbo de data/hora quando o evento é gerado no Delegated Admin.	2024-03-22T01:32:23.4056195Z

CHAVE	DESCRIÇÃO	EXEMPLO
produção	Identifica o produto de origem e a implantação do evento de uso.	XenDesktop.DelegatedAdmin (Cloud)
		OnPrem.DelegatedAdmin (OnPrem)
prodVer	Indica a versão do produto Citrix DaaS ou Citrix Virtual Apps and Desktops.	7.42.0.0

CARGA ÚTIL

CHAVE	DESCRIÇÃO	EXEMPLO
TotalCustomScopes	Indica o número total de escopos personalizados.	2
TotalCustomRoles	Indica o número total de funções personalizadas.	4

Embaralhar dados de telemetria de licenciamento

Considerando a sensibilidade das informações enviadas na telemetria de licença, a Citrix oferece uma opção para embaralhar os dados.

A tabela a seguir lista os dados que podem ser embaralhados:

CAMPO	DESCRIÇÃO	EXEMPLO
usuário	Identifica o ID do Usuário para identificar de forma exclusiva um usuário que inicia o lançamento da sessão.	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • Nome Principal do Usuário:

CAMPO	DESCRIÇÃO	EXEMPLO
		`C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
dispositivo -> nome do dispositivo	Indica o nome amigável para o dispositivo.	`C758LH671A44B3F7`
workerSid	Indica um identificador exclusivo para o VDA usado na sessão.	`1E5LH671A44B3F7`
AdminLoginList	Indica a lista de administradores exclusivos SamAccountName	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

Para habilitar ou desabilitar a ofuscação, execute os seguintes comandos PowerShell no Delivery Controller.

Observação:

Para um cliente Citrix Service Provider™ (CSP), a ofuscação está sempre desabilitada. Clientes CSP não podem habilitar a ofuscação usando comandos PowerShell.

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute o comando `asnp citrix` para carregar os módulos PowerShell específicos da Citrix.

3. Execute o seguinte comando para habilitar ou desabilitar a ofuscação:

   Por padrão, o valor é `1`, ou `true`, o que habilita a ofuscação dos dados de telemetria de licença.

   Para desabilitar:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   Depois de desabilitar a ofuscação, você pode habilitá-la usando o seguinte comando:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

FAQ para licenciamento

Observação:

- Para recursos de continuidade de negócios relacionados à pandemia de COVID-19, consulte CTX27055.
- Para informações gerais sobre como manter a continuidade dos negócios, consulte Continuidade de negócios — sob demanda.
- Para obter mais informações sobre o Citrix License Server atual, consulte Licenciamento.

Licenciamento Citrix®

Como posso obter meu arquivo de licença?

Enviamos o código de acesso da licença por e-mail. Existem três maneiras de gerar arquivos de licença usando o código de acesso da licença:

- O **Gerenciar Licenças** na sua página Minha Conta em `citrix.com`. Para obter mais informações, consulte Gerenciar licenças em citrix.com.
- Web Studio para alocar sua compra e o arquivo de licença é instalado automaticamente no seu Citrix License Server.

- Citrix Licensing Manager dentro do Citrix License Server para alocar sua compra e instalar seu arquivo de licença. Para obter mais informações, consulte Instalar licenças.

Como alocar licença na minha conta?

Consulte Alocar licenças.

Como adicionar licenças alocadas ao servidor de licenças?

Consulte Modificar licenças.

Quais portas TCP o licenciamento Citrix usa?

- O número da porta do Servidor de Licenças é 27000
- O número da porta do daemon do fornecedor é 7279
- A porta do Serviço Web para Licenciamento é 8083

O que é o Citrix License Server?

O Citrix License Server é um sistema que permite que as licenças sejam compartilhadas pela rede. Para obter mais informações, consulte Visão geral das operações de licenciamento.

Posso virtualizar ou agrupar o Citrix License Server?

Sim. Você pode virtualizar ou agrupar o Citrix License Server. Para obter mais informações, consulte Servidores de Licenças em Cluster.

Quais benefícios estão disponíveis para mim se eu virtualizar o Citrix License Server?

A virtualização do Citrix License Server oferece uma solução redundante. Essa solução permite a mobilidade entre vários servidores físicos sem a necessidade de tempo de inatividade.

Existem limitações a serem consideradas se eu virtualizar o Citrix License Server?

Não.

O Citrix License Server gerencia todas as licenças para minha implantação do Citrix Virtual Apps and Desktops™?

O Citrix License Server gerencia todas as licenças que você recebe para o Citrix Virtual Apps™ e Desktop, exceto as licenças da Premium Edition usadas com o Citrix Gateway. Os servidores de licenças incorporados aos dispositivos de rede, conforme exigido para esses dispositivos de rede orientados à segurança, gerenciam essas licenças.

O que é o Citrix Licensing Manager?

O Citrix Licensing Manager permite o download e a alocação de arquivos de licença do License Server no qual você instalou o Citrix Licensing Manager. O Citrix Licensing Manager é o método de gerenciamento de License Server recomendado, que permite o seguinte:

- Registro de código curto do Servidor de Licenças no Citrix Cloud™ e fácil remoção do registro.
- Configurar contas de usuário e grupo.
- Usar o painel para exibir licenças instaladas, em uso, expiradas e disponíveis, e datas de Customer Success Services.
- Exportar dados de uso de licença para uso em relatórios.
- Configurar o período de retenção de dados de uso histórico. O período de retenção de dados padrão é de 180 dias.
- Instalação simplificada de arquivos de licença no Servidor de Licenças usando um código de acesso de licença ou arquivo baixado.
- Ativar e desativar o modo de intermitência de licença (License burst mode).
- Configurar o Programa de Melhoria da Experiência do Cliente (CEIP) e o Call Home.
- Verifica automaticamente ou manualmente as licenças de renovação do Customer Success Services e notifica você ou instala as licenças, se encontradas.
- Notifica você sobre o estado do Servidor de Licenças - Licença de inicialização ausente, problemas de tempo, falhas do carregador.
- Modificar estas portas:
  - Servidor de Licenças (padrão 27000)
  - Daemon do Fornecedor (padrão 7279)
  - Serviços Web para Licenciamento (padrão 8083)

Para obter mais informações, consulte Citrix Licensing Manager.

Onde está o Citrix License Administration Console?

O License Administration Console não é mais compatível e foi removido do License Server versão 11.16.6. Recomendamos que você use o Citrix Licensing Manager.

Você pode usar o Studio para gerenciar e rastrear o licenciamento, desde que o License Server esteja no mesmo domínio do Studio ou em um domínio confiável.

Para obter mais informações, consulte Citrix Licensing Manager.

Qual é o período de atribuição de licença?

O período de atribuição de licença é o termo em que uma licença do Citrix Virtual Apps and Desktops é atribuída a um usuário ou dispositivo. O período de atribuição de licença padrão é de 90 dias.

Como sei quantas licenças minha organização comprou?

Todas as licenças adquiridas estão disponíveis para revisão e acesso a qualquer momento (24 horas por dia, 7 dias por semana) em sua caixa de ferramentas segura **Gerenciar Licenças** em sua página **Minha Conta** em `<https://www.citrix.com>`.

Como sei quantas licenças estão em uso a qualquer momento?

O Citrix Licensing Manager e o Studio fornecem detalhes sobre o uso de licenças em tempo real.

Recuperação de desastres e manutenção do License Server

Para obter informações sobre recuperação de desastres e manutenção do seu License Server, consulte Recuperação de desastres e manutenção na documentação de Licenciamento Citrix.

Licenciamento do Citrix Virtual Apps and Desktops

Como o Citrix Virtual Apps and Desktops é licenciado?

O licenciamento do Citrix Virtual Apps and Desktops oferece modelos de licença por usuário/dispositivo e concorrentes.

Usuário/dispositivo:

O modelo flexível de usuário/dispositivo se alinha com:

- Uso de desktop em toda a empresa.
- Licenciamento subjacente de virtualização de desktop da Microsoft.
- Licenciamento simultâneo para clientes com usuários que precisam apenas de acesso ocasional aos seus desktops e aplicativos virtuais.

O licenciamento de usuário/dispositivo oferece aos usuários acesso aos seus desktops e aplicativos virtuais a partir de um número ilimitado de dispositivos. As licenças de dispositivo dão a um número ilimitado de usuários acesso aos seus desktops e aplicativos virtuais a partir de um único dispositivo. Essa abordagem oferece máxima flexibilidade e melhora o alinhamento com o licenciamento de virtualização de desktop da Microsoft.

> **Importante:**

> Você não pode alocar licenças manualmente para um usuário ou dispositivo. O License Server ou o serviço de nuvem atribui as licenças. Com o licenciamento de usuário/dispositivo, uma vez que uma licença é atribuída, ela não pode ser atribuída a outro usuário até depois de 90 dias de inatividade.

> **Simultâneo:**

As licenças simultâneas permitem uma conexão a um número ilimitado de aplicativos e desktops virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida apenas durante uma sessão ativa. Se a sessão for desconectada ou encerrada, a licença é devolvida ao pool.

Para obter mais informações sobre licenciamento de usuário/dispositivo, consulte Licença de usuário/dispositivo e licenças simultâneas, consulte Licença simultânea.

É possível experimentar o Citrix Virtual Apps and Desktops antes de comprar licenças?

Sim. Você pode baixar o software Citrix Virtual Apps and Desktops e executá-lo no modo de avaliação. O modo de avaliação permite que você use o Citrix Virtual Apps and Desktops no local por 30 dias, para 10 conexões, sem uma licença. Para obter mais informações, consulte Licenças de avaliação.

O Citrix DaaS™ (anteriormente serviço Citrix Virtual Apps and Desktops) para Citrix Cloud está disponível para serviço de avaliação mediante aprovação. Verifique com seu representante Citrix para obter mais detalhes.

Como a Citrix define simultaneidade para o Citrix Virtual Apps and Desktops?

O modelo simultâneo do Citrix Virtual Apps and Desktops permite uma conexão a um número ilimitado de aplicativos e desktops virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida apenas durante uma sessão ativa. Se a sessão for desconectada ou encerrada, a licença é devolvida ao pool para reemissão. Para obter mais informações, consulte Licença simultânea.

Posso implantar várias edições de licenças do Citrix Virtual Apps and Desktops em um Servidor de Licenças comum?

Sim. O Servidor de Licenças gerencia licenças para Citrix Virtual Apps e Desktops simultaneamente. Recomendamos que você instale a versão mais recente do Servidor de Licenças. Se você não tiver certeza se a versão do seu Servidor de Licenças está atualizada, verifique-a comparando sua versão com o número no site de downloads da Citrix.

Um único site pode usar licenças do Citrix Virtual Apps e do Citrix Virtual Apps and Desktops?

Dependendo da versão, um único site do Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode suportar ambos os modelos de licenciamento - usuário/dispositivo ou concorrente. Um único site do Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode suportar apenas uma edição. Para obter mais informações, consulte Licenciamento de vários tipos.

As versões mínimas que suportam licenciamento de vários tipos são XenApp e XenDesktop 7.15 Long Term Service Release (LTSR) e Citrix Virtual Apps and Desktops 7 1808.

Posso selecionar Citrix Virtual Apps concorrente como modelo de produto se tiver licenças de usuário/dispositivo do Citrix Virtual Apps and Desktops ou licenças concorrentes do Citrix Virtual Apps and Desktops instaladas no Servidor de Licenças?

Se você usa o Citrix Virtual Apps como um recurso do Citrix Virtual Apps and Desktops Advanced ou Premium Edition, o modelo de licença para ele é o mesmo da sua edição Advanced ou Premium do Citrix Virtual Apps and Desktops. Se você adquiriu o Citrix Virtual Apps and Desktops, configure seu licenciamento como Citrix Virtual Apps and Desktops mesmo que planeje usar apenas a funcionalidade do Virtual Apps. Selecione Citrix Virtual Apps como um modelo de produto somente se você tiver licenças autônomas concorrentes do Virtual Apps instaladas no Servidor de Licenças.

Quais componentes de produto estão incluídos em cada edição do Citrix Virtual Apps e do Citrix Virtual Apps and Desktops?

Para uma matriz completa de recursos por edição, consulte Recursos do Citrix Virtual Apps and Desktops.

Como licencio ambientes Citrix Virtual Desktops™ em conformidade com o EULA do Citrix Virtual Apps and Desktops?

Para implantar o Citrix Virtual Apps and Desktops sob o modelo de licença de usuário/dispositivo ou concorrente em conformidade com o EULA do Citrix Virtual Apps and Desktops, aplique os arquivos de licença ao seu Servidor de Licenças. O Servidor de Licenças então controla e monitora a conformidade da licença. Recomendamos que você configure seu produto com base no que você adquiriu. Por exemplo, se você adquirir o Citrix Virtual Apps and Desktops Premium, mas quiser usar apenas o recurso Citrix Virtual Apps, configure o produto para Citrix Virtual Apps and Desktops para atender à conformidade. Para obter mais informações, consulte o Centro de Conformidade de Licenças de Produto.

Como licencio ambientes Citrix Virtual Apps em conformidade com o EULA do Citrix Virtual Apps?

Para implantar o Citrix Virtual Apps sob o modelo de licença concorrente em conformidade com o EULA do Citrix Virtual Apps, aplique os arquivos de licença ao seu Servidor de Licenças. O Servidor de Licenças então controla e monitora a conformidade da licença.

Existe um requisito de licenciamento para as Opções de Manutenção do Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) ou Current Release (CR)?

As Opções de Manutenção do Citrix Virtual Apps and Desktops, como o Long-Term Service Release, são um benefício do programa Customer Success Services. Você deve ter Customer Success Services ativos para se qualificar para os benefícios do LTSR. Para obter mais informações, consulte [Citrix Virtual Apps, Citrix Virtual Apps and Desktops e XenServer Servicing Options.

Como funcionam as horas agrupadas do serviço de Isolamento de Navegador Remoto (RBI)?

Ao adquirir um mínimo de 25 usuários do serviço, você recebe 5000 horas de direitos para usar o serviço, agrupadas entre todos os usuários. Compras subsequentes de direitos de usuário não aumentam o direito a horas agrupadas. Para aumentar o direito a horas de serviço, compre pacotes de complementos.

Posso usar o Acesso Remoto a PC com licenças CCU?

Sim.

Para obter informações sobre o Acesso Remoto a PC, consulte Acesso Remoto a PC.

O que acontece quando a manutenção de software expira para o meu ambiente Citrix?

Quando sua Manutenção de Software (SWM) ou assinatura expira, o acesso a atualizações de software e suporte técnico é pausado. Além disso, dependendo do seu tipo de licença e versão do produto, usuários finais e administradores receberão notificações de aviso específicas indicando que o ambiente não é suportado.

Essas notificações são acionadas somente quando todas as licenças no servidor expiraram.

EXPERIÊNCIA DO USUÁRIO FINAL

Os usuários receberão uma mensagem de aviso após iniciar uma sessão. A mensagem indica:

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

EXPERIÊNCIA DO ADMINISTRADOR

Os administradores verão alertas de aviso no console do Citrix Studio, alertando-os sobre a expiração iminente ou ativa.

COMPORTAMENTO DE EXPIRAÇÃO POR TIPO DE LICENÇA

O momento dessas mensagens depende do tipo de licença e da versão do Citrix Virtual Apps and Desktops instalada.

LICENÇAS DE ASSINATURA LOCAIS

- Aviso ao Usuário Final: Aparece após a expiração da assinatura, durante o período de carência.
- Aviso ao Administrador: Aparece no Studio 30 dias antes da expiração da assinatura.
- Versões Suportadas:
  - Versão Atual: Citrix Virtual Apps and Desktops 2411 e superior.
  - LTSR: 2203 CU6, e 2402 CU1 e versões LTSR posteriores

Licenças de usuário ou dispositivo

Como a Citrix aloca licenças para usuários no modelo de licenciamento de usuário/dispositivo?

Com o modelo de licença de usuário/dispositivo, o License Server atribui a licença a um ID de usuário exclusivo. Ele permite que esse único usuário tenha conexões ilimitadas de dispositivos ilimitados. Se um usuário se conecta a um desktop ou dispositivo, o usuário requer uma licença atribuída a ele para acessar um desktop ou aplicativo virtual. O License Server ou o serviço de nuvem atribui a licença. Você não pode atribuir essas licenças manualmente. A licença é atribuída ao usuário, não ao dispositivo compartilhado. Uma vez atribuída, a licença não pode ser atribuída a outro usuário antes de 90 dias de inatividade. Para mais informações, consulte Licença de Usuário/Dispositivo.

Como a Citrix define um dispositivo licenciado no modelo de licenciamento de usuário/dispositivo?

Um dispositivo licenciado requer um ID de dispositivo de endpoint exclusivo. No modelo de usuário/dispositivo, um dispositivo é qualquer equipamento que você autorizou para uso por

qualquer indivíduo para acessar instâncias do Citrix Virtual Apps and Desktops. Para um dispositivo compartilhado, uma única licença de usuário/dispositivo do Citrix Virtual Apps and Desktops pode suportar vários usuários que compartilham o dispositivo. Por exemplo, um dispositivo compartilhado pode ser uma estação de trabalho de sala de aula ou uma estação de trabalho clínica em um hospital.

Posso converter minhas licenças concorrentes do Citrix Virtual Desktops Standard Edition para o modelo de usuário/dispositivo?

Você não pode converter licenças concorrentes do Citrix Virtual Desktops Standard Edition em licenças de usuário/dispositivo do Citrix Virtual Desktops Standard Edition. Da mesma forma, você não pode converter licenças de usuário/dispositivo do Citrix Virtual Desktops Standard Edition em licenças concorrentes do Citrix Virtual Desktops Standard Edition.

Se você tem licenças concorrentes do Citrix Virtual Desktops Standard Edition e deseja o modelo de licença de usuário/dispositivo, atualize para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.

DE	PARA CONCORRENTE PADRÃO	PARA USUÁRIO/ DISPOSITIVO STANDARD	PARA USUÁRIO/ DISPOSITIVO ADVANCED	PARA USUÁRIO/ DISPOSITIVO PREMIUM
Licenças simultâneas do Citrix Virtual Desktops Standard Edition	N/A	Conversão de simultâneo para usuário/ dispositivo NÃO permitida	Você não pode converter modelos de licença, mas pode fazer upgrade para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.	Você não pode converter modelos de licença, mas pode fazer upgrade para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.
Licenças de usuário/ dispositivo do Citrix Virtual Desktops	Conversão de usuário/ dispositivo para simultâneo NÃO permitida	N/A	N/A	N/A

DE	PARA CONCORRENTE E PADRÃO	PARA USUÁRIO/ DISPOSITIVO STANDARD	PARA USUÁRIO/ DISPOSITIVO ADVANCED	PARA USUÁRIO/ DISPOSITIVO PREMIUM
Standard Edition				

Como o licenciamento simultâneo funciona de forma diferente do licenciamento por usuário/dispositivo?

Baseamos o licenciamento simultâneo em conexões de dispositivos simultâneas. Uma licença simultânea é usada apenas quando um dispositivo estabelece uma conexão ativa. Assim que a conexão termina, a licença simultânea retorna ao pool de licenças para uso imediato. Recomendamos este modelo de licenciamento para uso ocasional. As licenças de usuário/dispositivo são alugadas por um período e não estão disponíveis para outros usuários até que o aluguel expire.

No modelo de usuário/dispositivo, podemos alocar licenças para usuários e dispositivos na mesma empresa?

Sim. Ambos os tipos podem estar presentes na mesma empresa. O License Server atribui licenças de forma otimizada a usuários ou dispositivos com base no uso. Você não pode atribuir essas licenças manualmente.

Como decido quantos usuários ou dispositivos licenciar?

Avalie os requisitos do caso de uso para determinar o número apropriado de licenças. O licenciamento por usuário/dispositivo permite acesso ilimitado a desktops virtuais e aplicativos virtuais ilimitados a partir de um número ilimitado de dispositivos. O licenciamento simultâneo permite acesso ilimitado a desktops virtuais e aplicativos virtuais ilimitados a partir de um único dispositivo que um número ilimitado de usuários pode usar. Considere a seguinte fórmula:

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only
```

```
Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

Sob o modelo de usuário/dispositivo, qual é o número máximo de dispositivos que um usuário licenciado pode usar para se conectar ao meu ambiente?

Cada usuário licenciado tem o direito de usar um número ilimitado de dispositivos conectados ou offline.

Sob o modelo de usuário/dispositivo, qual é o número máximo de usuários que podem acessar um dispositivo licenciado?

Cada dispositivo licenciado pode atender a um número ilimitado de usuários dentro de uma organização.

Sob o modelo de usuário/dispositivo, qual é o número máximo de desktops virtuais ou aplicativos web RBI que um usuário licenciado pode consumir a qualquer momento?

Cada usuário licenciado pode se conectar a um número ilimitado de desktops virtuais ou aplicativos web.

Posso adquirir licenças do Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados no meu ambiente Citrix Virtual Apps and Desktops existente?

Sim. Você pode adquirir licenças do Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados no seu ambiente Citrix Virtual Apps and Desktops existente.

Como faço para liberar uma licença de usuário/dispositivo autorizado?

Para liberar a atribuição de um usuário/dispositivo autorizado, use o utilitário `udadmin` de acordo com os termos do EULA. O Servidor de Licenças então atribui a licença ao próximo usuário/dispositivo apropriado. Para mais informações, consulte Exibir ou liberar licenças para usuários ou dispositivos.

O que acontece se eu exceder minha contagem de licenças de usuário/dispositivo adquiridas?

As licenças de usuário/dispositivo incluem um limite de 10% de excedente (overdraft), que é incluído quando as licenças são geradas. O excedente também é incluído na contagem de licenças instaladas. Se o pico de uso exceder a contagem instalada, incluindo o excedente, o

acesso para mais usuários será negado. Adquira e implante uma nova licença para permitir o acesso a mais usuários.

Se todas as licenças estiverem em uso, incluindo o excedente de licenças, o modo de intermitência de licenças (License burst mode) permite conexões ilimitadas a um produto. O modo de intermitência de licenças lhe dá tempo para determinar por que você excedeu a contagem máxima de licenças e para adquirir mais licenças sem interromper seus usuários. Este período dura até que 15 dias se passem ou você instale mais licenças de varejo, o que ocorrer primeiro. Para mais informações, consulte Modo de intermitência de licenças.

O Director exibe os estados do modo de cache de licenças. Para mais informações, consulte Painéis no Painel do Director.

Qual é o número máximo de aplicativos virtuais que um usuário licenciado pode consumir a qualquer momento?

Cada usuário licenciado pode se conectar a um número ilimitado de aplicativos virtuais.

O que acontece se um usuário licenciado sair da minha organização?

Quando um usuário licenciado existente sai da sua organização, você pode liberar a licença do usuário que está saindo sem notificar a Citrix. Use o utilitário `udadmin` para liberar a licença. Se você não liberar a licença, o Servidor de Licenças liberará automaticamente qualquer licença após 90 dias de inatividade. Esta informação está sujeita aos termos especificados no EULA.

O que acontece se um usuário licenciado estiver ausente por um período prolongado?

Se um usuário licenciado existente estiver ausente por um período prolongado, você pode liberar a licença sem notificar a Citrix, para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

O que acontece se substituirmos um dispositivo licenciado na minha organização?

Se você substituir um dispositivo licenciado existente, poderá liberar a licença sem notificar a Citrix para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

O que acontece se um dispositivo licenciado estiver fora de serviço por um período prolongado?

Quando um dispositivo licenciado existente estiver fora de serviço por um período prolongado, você pode liberar a licença sem notificar a Citrix, para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar as licenças. Se você não liberar a licença, o Servidor de Licenças liberará automaticamente qualquer licença após 90 dias de inatividade. Esta informação está sujeita aos termos especificados no EULA.

Posso alternar licenças de usuário para licenças de dispositivo e vice-versa depois de atribuir as licenças a um dispositivo ou usuário?

Sim. Essa alteração ocorre automaticamente. O Servidor de Licenças atribui licenças a usuários ou dispositivos com base nos padrões de uso. Se os padrões de uso mudarem, o Servidor de Licenças poderá alternar a atribuição com base no novo uso. O Servidor de Licenças sempre atribui licenças da forma mais econômica para o cliente. Além disso, o Servidor de Licenças monitora as licenças para identificar licenças **não utilizadas** após o período de atribuição de 90 dias. Você pode reatribuir licenças identificadas como não utilizadas após o período de atribuição de 90 dias para outros usuários ou dispositivos.

Licenças simultâneas

No modelo simultâneo, qual é o número máximo de desktops virtuais que um usuário licenciado do Citrix Virtual Apps and Desktops pode consumir a qualquer momento?

Um endpoint pode atender a muitos usuários e permite conexões ilimitadas.

Posso implantar licenças simultâneas de uma versão anterior do Citrix Virtual Apps and Desktops e novas licenças de usuário/dispositivo ou simultâneas em um único Servidor de Licenças?

Sim. Você pode continuar a usar o mesmo Servidor de Licenças para dar suporte a implantações licenciadas por usuário/dispositivo ou simultâneas.

Posso implantar licenças simultâneas e licenças de usuário/dispositivo ou simultâneas em um único Servidor de Licenças?

Sim. Você pode continuar a usar o mesmo Servidor de Licenças para dar suporte a implantações licenciadas simultâneas e por usuário/dispositivo ou simultâneas.

As edições Advanced e Premium do Citrix Virtual Apps and Desktops incluem licenças simultâneas do Citrix Virtual Apps?

As licenças de usuário/dispositivo Advanced e Premium do Citrix Virtual Apps and Desktops incluem licenças simultâneas do Citrix Virtual Apps apenas para compatibilidade. Essas licenças simultâneas são para uso apenas com versões anteriores do produto que são incompatíveis com licenças de usuário/dispositivo. O uso das licenças de compatibilidade simultâneas incluídas com as licenças de usuário/dispositivo é permitido apenas com estas versões - versões do XenApp anteriores a 6.5 e versões do XenDesktop anteriores ao Service Pack 1 de 5.0.

O que acontece se eu exceder minha contagem de licenças simultâneas adquiridas?

Se todas as licenças estiverem em uso, o modo de intermitência de licença (License burst mode) permite conexões ilimitadas a um produto. O modo de intermitência de licença (License burst mode) lhe dá tempo para determinar por que você excedeu a contagem máxima de licenças e para comprar mais licenças sem interromper seus usuários. Este período dura até que 15 dias se passem ou você instale mais licenças de varejo, o que ocorrer primeiro. Para obter mais informações, consulte Modo de intermitência de licença.

O Director exibe os estados do período de carência. Para obter mais informações, consulte Painéis no Painel do Director.

Licenças de overdraft

Como obtenho licenças de overdraft?

Produtos (excluindo Citrix Cloud) que suportam modelos de licença de usuário/dispositivo, usuário ou dispositivo incluem um recurso de overdraft de licença que permite usar um número limitado de licenças extras para evitar a negação de acesso. Oferecemos qualquer recurso de overdraft como uma conveniência, não como um direito de licença. Licenças simultâneas e de servidor não contêm overdraft. Quaisquer licenças de overdraft usadas devem ser adquiridas dentro de 30 dias do primeiro uso, mas o uso não é limitado a 30 dias. A Citrix reserva-se o direito de remover qualquer recurso de overdraft em novas versões de produtos. Para obter mais informações, consulte Overdraft de licença.

Como posso identificar um overdraft de licença?

Você pode visualizar informações de uso, incluindo o número de licenças em overdraft no Citrix Licensing Manager. O Studio também contém informações de uso de overdraft.

O que acontece quando uma licença de overdraft é consumida?

Uma licença é atribuída de suas licenças instaladas para permitir o acesso ao seu ambiente Citrix Virtual Apps and Desktops. Esta licença de overdraft oferece o mesmo acesso e funcionalidade que suas outras licenças.

Posso receber um alerta quando minhas licenças de overdraft forem consumidas?

Atualmente, não há alertas específicos fornecidos quando as licenças de overdraft são consumidas.

Por quanto tempo uma licença de overdraft pode ser consumida?

Adquira quaisquer licenças de overdraft usadas dentro de 30 dias do primeiro uso.

Outras informações de licenciamento específicas do produto

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer
- Citrix Licensing

Balancear carga de máquinas

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este recurso está disponível apenas no Web Studio.

> Este recurso se aplica a todos os seus catálogos — catálogos de SO de sessão única ou de SO de múltiplas sessões. O balanceamento de carga vertical se aplica apenas a máquinas de SO de múltiplas sessões.

> 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 ativado.

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 novas máquinas. Usuários que se desconectam de máquinas existentes liberam 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 da máquina ligada).

Exemplo: Você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com as primeiras 10 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 Número máximo de sessões.
>
> Alternativamente, você pode usar o PowerShell para habilitar ou desabilitar o balanceamento de carga vertical em todo o site. Use a configuração `UseVerticalScalingForRdsLaunches` no cmdlet `Set-BrokerSite`. Use `Get-BrokerSite` para exibir o valor da configuração `UseVerticalScalingForRdsLaunches`. Consulte a ajuda do cmdlet para obter detalhes.

- **Balanceamento de carga horizontal**. Atribui uma sessão de usuário de entrada à máquina ligada menos carregada 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 ativado.

  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 este recurso, no Web Studio, selecione **Configurações** no painel esquerdo. Selecione uma opção em **Balancear carga de catálogos de múltiplas sessões**.

Configurações de balanceamento de carga no nível do grupo de entrega

A configuração do balanceamento de carga no nível do grupo de entrega permite substituir as configurações de balanceamento de carga herdadas do nível do site. Você pode atingir a utilização máxima para cada máquina ao selecionar o balanceamento de carga vertical no nível do grupo de entrega. Isso ajudará a reduzir custos em nuvens públicas. Essa configuração pode ser feita durante a criação de um novo grupo de entrega ou edição de um grupo de entrega existente.

Balanceamento de carga horizontal. As sessões são distribuídas entre as máquinas ligadas. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina lida com cinco sessões simultâneas e a segunda máquina também lida com cinco.

Balanceamento de carga vertical. As sessões maximizam a capacidade da máquina ligada e economizam custos de máquina. Por exemplo, se você tiver duas máquinas configuradas para 10 sessões cada, a primeira máquina lida com as primeiras 10 sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

Cache de Host Local

Para garantir que o banco de dados do site Citrix Virtual Apps and Desktops esteja sempre disponível, a Citrix recomenda iniciar com uma implantação de SQL Server tolerante a falhas, seguindo as melhores práticas de alta disponibilidade da Microsoft. (Para recursos de alta disponibilidade do SQL Server suportados, consulte Bancos de Dados.) No entanto, problemas e interrupções de rede podem resultar na impossibilidade de os usuários se conectarem aos seus aplicativos ou desktops.

O recurso Local Host Cache permite que as operações de intermediação de conexão em um site continuem quando ocorre uma interrupção. Uma interrupção ocorre quando a conexão entre um Delivery Controller™ e o banco de dados do site falha em um ambiente Citrix® local. O Local Host Cache é ativado quando o banco de dados do site fica inacessível por 90 segundos.

A partir do XenApp e XenDesktop 7.16, o recurso de leasing de conexão (um recurso de alta disponibilidade predecessor em versões anteriores) foi removido do produto e não está mais disponível.

Conteúdo dos dados

O Local Host Cache inclui as seguintes informações, que são um subconjunto das informações no banco de dados principal:

- Identidades de usuários e grupos que têm direitos atribuídos a recursos publicados do site.
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados do site.
- Identidades de máquinas VDA (incluindo máquinas de Acesso Remoto para PC) configuradas no site.
- Identidades (nomes e endereços IP) de máquinas cliente Citrix Receiver™ sendo ativamente usadas para se conectar a recursos publicados.

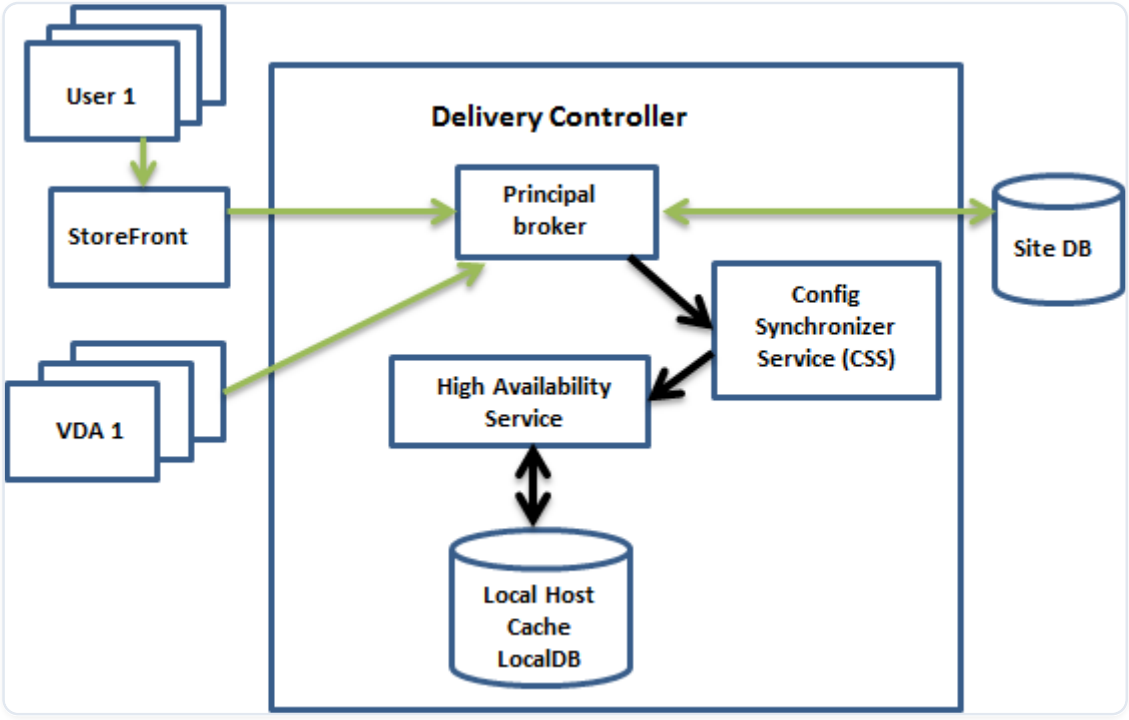
Ele também contém informações para conexões atualmente ativas que foram estabelecidas enquanto o banco de dados principal estava indisponível:

- Resultados de qualquer análise de endpoint de máquina cliente realizada pelo Citrix Receiver.

- Identidades de máquinas de infraestrutura (como servidores NetScaler Gateway e StoreFront™) envolvidas com o site.
- Datas, horários e tipos de atividade recente dos usuários.

Como funciona

O gráfico a seguir ilustra os componentes do Local Host Cache e os caminhos de comunicação durante as operações normais.



Durante operações normais

- O *broker principal* (Citrix Broker Service) em um Controller aceita solicitações de conexão do StoreFront. O broker se comunica com o banco de dados do site para conectar usuários a VDAs que estão registrados no Controller.
- O Citrix Config Synchronizer Service (CSS) verifica com o broker aproximadamente a cada 5 minutos para ver se alguma alteração foi feita. Essas alterações podem ser iniciadas pelo administrador (como a alteração de uma propriedade de grupo de entrega) ou ações do sistema (como atribuições de máquina).
- Se uma alteração de configuração ocorreu desde a verificação anterior, o CSS sincroniza (copia) as informações para um broker secundário no Controller. (O broker secundário também é conhecido como Serviço de Alta Disponibilidade.)

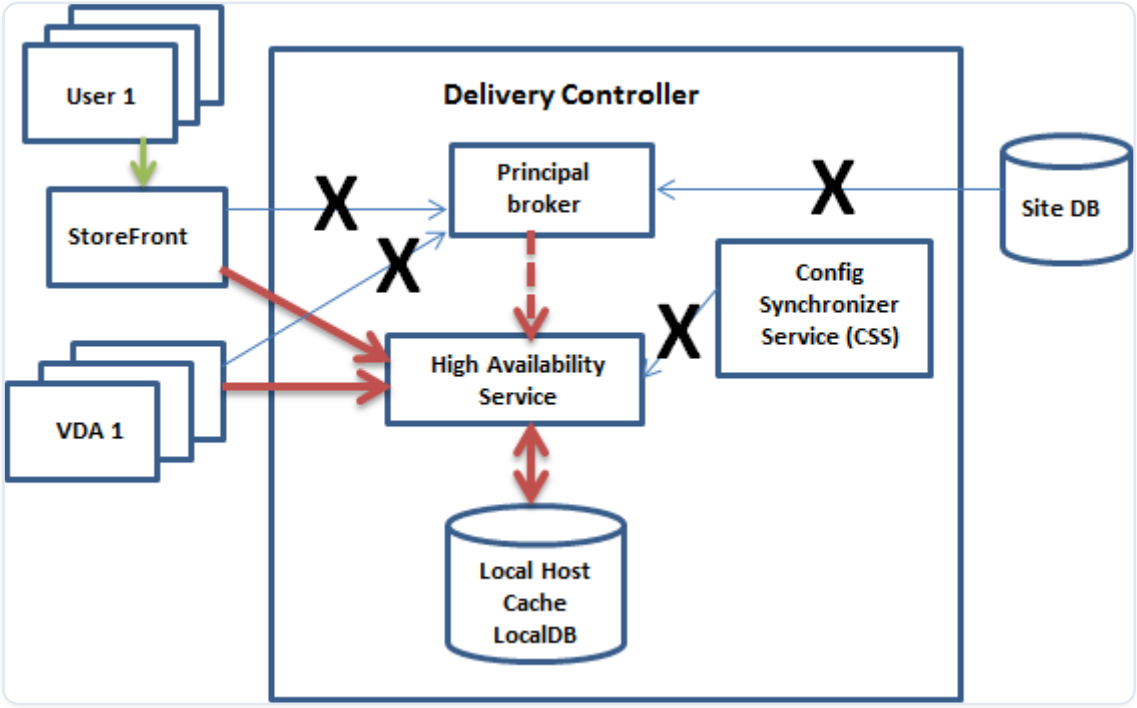
  Todos os dados de configuração são copiados, não apenas os itens que foram alterados desde a verificação anterior. O CSS importa os dados de configuração para um banco de

dados Microsoft SQL Server Express LocalDB no Controller. Este banco de dados é chamado de banco de dados Local Host Cache. O CSS garante que as informações no banco de dados Local Host Cache correspondam às informações no banco de dados do site. O banco de dados Local Host Cache é recriado cada vez que a sincronização ocorre.

O Microsoft SQL Server Express LocalDB (usado pelo banco de dados Local Host Cache) é instalado automaticamente quando você instala um Controller. (Você pode proibir esta instalação ao instalar um Controller a partir da linha de comando.) O banco de dados Local Host Cache não pode ser compartilhado entre Controllers. Você não precisa fazer backup do banco de dados Local Host Cache. Ele é recriado toda vez que uma alteração de configuração é detectada.

- Se nenhuma alteração ocorreu desde a última verificação, nenhum dado é copiado.

O gráfico a seguir ilustra as alterações nos caminhos de comunicação se o broker principal perder contato com o banco de dados do site (uma interrupção começa).



Durante uma interrupção

Quando uma interrupção começa:

- O broker secundário começa a escutar e processar as solicitações de conexão.
- Quando a interrupção começa, o broker secundário não tem dados de registro de VDA atuais, mas quando um VDA se comunica com ele, um processo de registro é acionado. Durante esse processo, o broker secundário também obtém informações de sessão atuais sobre esse VDA.

- Enquanto o broker secundário está lidando com as conexões, o Brokering Principal continua a monitorar a conexão. Quando a conexão é restaurada, o Brokering Principal instrui o broker secundário a parar de escutar as informações de conexão, e o Brokering Principal retoma as operações de brokering. Na próxima vez que um VDA se comunicar com o Brokering Principal, um processo de registro é acionado. O broker secundário remove quaisquer registros de VDA restantes da interrupção anterior. O CSS retoma a sincronização de informações quando descobre que ocorreram alterações de configuração na implantação.

No caso improvável de uma interrupção começar durante uma sincronização, a importação atual é descartada e a última configuração conhecida é usada.

O log de eventos fornece informações sobre sincronizações e interrupções.

Não há limite de tempo imposto para operar no modo de interrupção.

A transição entre o modo normal e o modo de interrupção não afeta as sessões existentes. Ela afeta apenas o lançamento de novas sessões.

Você também pode acionar intencionalmente uma interrupção. Consulte Forçar uma interrupção para obter detalhes sobre por que e como fazer isso.

Sites com vários Controllers

Entre suas outras tarefas, o CSS fornece rotineiramente ao broker secundário informações sobre todos os Controllers na zona. (Se sua implantação não contiver várias zonas, esta ação afeta todos os Controllers no site.) Com essas informações, cada broker secundário conhece todos os brokers secundários pares em execução em outros Controllers na zona.

Os brokers secundários se comunicam entre si em um canal separado. Esses brokers usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual broker secundário será responsável pelas operações de broker na zona se ocorrer uma interrupção. Durante a interrupção, todos os VDAs se registram no broker secundário eleito. Os brokers secundários não eleitos na zona rejeitam ativamente as solicitações de conexão de entrada e de registro de VDA.

Se um broker secundário eleito falhar durante uma interrupção, outro broker secundário é eleito para assumir, e os VDAs se registram no broker secundário recém-eleito.

Durante uma interrupção, se um Controller for reiniciado:

- Se esse Controller não for o broker eleito, a reinicialização não terá impacto.

- Se esse Controller for o broker eleito, um Controller diferente será eleito, fazendo com que os VDAs se registrem. Depois que o Controller reiniciado é ligado, ele assume automaticamente a função de broker, o que faz com que os VDAs se registrem novamente. Nesse cenário, o desempenho pode ser afetado durante os registros.

Se você desligar um Controller durante as operações normais e depois ligá-lo durante uma interrupção, o Local Host Cache não poderá ser usado nesse Controller se ele for eleito como o broker.

Os logs de eventos fornecem informações sobre as eleições.

O que está indisponível durante uma interrupção e outras diferenças

Não há limite de tempo imposto para operar no modo de interrupção. No entanto, a Citrix recomenda restaurar a conectividade o mais rápido possível.

Durante uma interrupção:

- Você não pode usar o Studio.
- Você tem acesso limitado ao SDK do PowerShell.
    - Você deve primeiro:
        - Adicione uma chave de registro `EnableCssTestMode` com o valor 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - Use a porta 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - Após executar esses comandos, você pode acessar:
        - Todos os cmdlets `Get-Broker*`.
- As credenciais do hipervisor não podem ser obtidas do Serviço de Host. Todas as máquinas estão em 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 pode ser usada somente se a atribuição ocorreu durante operações normais. Novas atribuições não podem ser feitas durante uma interrupção.

- O registro e a configuração automáticos de máquinas de Acesso Remoto a PC não são possíveis. No entanto, as máquinas que foram registradas e configuradas durante a operação normal são utilizáveis.
- Aplicativos hospedados em servidor e usuários de desktop podem usar mais sessões do que seus limites de sessão configurados, se os recursos estiverem em zonas diferentes.
- Os usuários podem iniciar aplicativos e desktops apenas a partir de VDAs registrados na zona que contém o broker secundário atualmente ativo/eleito. Lançamentos entre zonas (de um broker secundário em uma zona para um VDA em uma zona diferente) não são suportados durante uma interrupção.
- Se uma interrupção do banco de dados do site ocorrer antes do início de uma reinicialização agendada para VDAs em um grupo de entrega, as reinicializações começarão quando a interrupção terminar. Isso pode ter resultados não intencionais. Para obter mais informações, consulte Reinicializações agendadas atrasadas devido a interrupção do banco de dados.
- Preferência de zona não pode ser configurada. Se configurada, as preferências não são consideradas para o lançamento da sessão.
- Restrições de tag, onde as tags são usadas para designar zonas, não são suportadas para lançamentos de sessão. Quando tais restrições de tag são configuradas e a opção verificação avançada de integridade de uma loja StoreFront está ativada, as sessões podem falhar intermitentemente ao iniciar.

Suporte a aplicativos e desktops

O LHC suporta os seguintes tipos de VDAs e modelos de entrega:

TIPO DE VDA	MODELO DE ENTREGA	DISPONIBILIDADE DE VDA DURANTE EVENTOS LHC
SO multissessão	Aplicativos e desktops	Sempre disponível.
SO de sessão única estático (atribuído)	Desktops	Sempre disponível.
SO de sessão única gerenciado por energia aleatório (agrupado)	Desktops	Não disponível por padrão. Todas as tentativas de lançamento de sessão para VDAs

TIPO DE VDA	MODELO DE ENTREGA	DISPONIBILIDADE DE VDA DURANTE EVENTOS LHC	
		gerenciados por energia em grupos de entrega agrupados falharão por padrão. Você pode torná-los disponíveis para novas conexões durante eventos de LHC. Para obter mais informações, consulte Habilitar usando o Web Studio e Habilitar usando o PowerShell. **Importante:** Habilitar o acesso a máquinas agrupadas de sessão única com gerenciamento de energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.	

Observação:

> Habilitar o acesso a VDAs de desktop com gerenciamento de energia em grupos de entrega agrupados não afeta como a propriedade `ShutdownDesktopsAfterUse` configurada funciona durante as operações normais. Quando o acesso a esses desktops durante o LHC é habilitado, os VDAs não reiniciam automaticamente após a conclusão do evento de LHC. Os VDAs de desktop com gerenciamento de energia em grupos de entrega agrupados podem reter dados de sessões anteriores até que os VDAs reiniciem. Uma reinicialização do VDA pode ocorrer quando um usuário faz logoff do VDA durante operações sem LHC ou quando os administradores reiniciam o VDA.

Habilitar o LHC para VDAs agrupados de SO de sessão única com gerenciamento de energia usando o Web Studio

Usando o Web Studio, você pode disponibilizar essas máquinas para novas conexões durante eventos de LHC por grupo de entrega:

- Para habilitar esse recurso durante a criação do grupo de entrega, consulte Criar grupos de entrega.
- Para habilitar esse recurso para um grupo de entrega existente, consulte Gerenciar grupos de entrega.

> **Observação:**

> Essa configuração está disponível no Web Studio apenas para grupos de entrega de desktop agrupados que entregam VDAs com gerenciamento de energia.

Habilitar LHC para VDAs agrupados de SO de sessão única com gerenciamento de energia usando o PowerShell

Para habilitar o LHC para VDAs em um grupo de entrega específico, siga estas etapas:

1. Habilite esse recurso no nível do site executando este comando:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Habilite o LHC para um grupo de entrega executando este comando com o nome do grupo de entrega especificado:

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

Para alterar a disponibilidade padrão do LHC para grupos de entrega agrupados recém-criados com VDAs gerenciados por energia, execute o seguinte comando:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Considerações sobre o tamanho da RAM

O serviço LocalDB pode usar aproximadamente 1,2 GB de RAM (até 1 GB para o cache do banco de dados, mais 200 MB para executar o SQL Server Express LocalDB). O broker secundário pode usar até 1 GB de RAM se uma interrupção durar um intervalo estendido com muitos logons ocorrendo (por exemplo, 12 horas com 10 mil usuários). Esses requisitos de memória são adicionais aos requisitos normais de RAM para o Controller, portanto, pode ser necessário aumentar a quantidade total de capacidade de RAM.

Se você usar uma instalação do SQL Server Express para o banco de dados do site, o servidor terá dois processos sqlserver.exe.

Considerações sobre a configuração de núcleos de CPU e soquetes

A configuração da CPU de um Controller, particularmente o número de núcleos disponíveis para o SQL Server Express LocalDB, afeta diretamente o desempenho do Local Host Cache, ainda mais do que a alocação de memória. Essa sobrecarga da CPU é observada apenas durante o período de interrupção, quando o banco de dados está inacessível e o broker secundário está ativo.

Embora o LocalDB possa usar vários núcleos (até 4), ele é limitado a apenas um único soquete. Adicionar mais soquetes não melhorará o desempenho (por exemplo, ter 4 soquetes com 1 núcleo cada). Em vez disso, a Citrix recomenda usar vários soquetes com vários núcleos. Nos testes da Citrix, uma configuração 2x3 (2 soquetes, 3 núcleos) forneceu melhor desempenho do que as configurações 4x1 e 6x1.

Considerações sobre armazenamento

À medida que os usuários acessam recursos durante uma interrupção, o LocalDB cresce. Por exemplo, durante um teste de logon/logoff executado a 10 logons por segundo, o banco de dados cresceu 1 MB a cada 2-3 minutos. Quando a operação normal é retomada, o banco de dados local é recriado e o espaço é liberado. No entanto, espaço suficiente deve estar disponível na unidade onde o LocalDB está instalado para permitir o crescimento do banco de dados durante uma interrupção. O Local Host Cache também incorre em mais E/S durante uma interrupção: aproximadamente 3 MB de gravações por segundo, com várias centenas de milhares de leituras.

Considerações de desempenho

Durante uma interrupção, um broker secundário gerencia todas as conexões, então em sites (ou zonas) que fazem balanceamento de carga entre vários Controllers durante operações normais, o broker secundário eleito pode precisar manipular muito mais solicitações do que o normal durante uma interrupção. Portanto, as demandas da CPU serão maiores. Cada broker secundário no site (zona) deve ser capaz de manipular a carga adicional imposta pelo banco de dados do Local Host Cache e todos os VDAs afetados, porque o broker secundário eleito durante uma interrupção pode mudar.

Limites de VDI:

- Em uma implantação VDI de zona única, até 10.000 VDAs podem ser tratados efetivamente durante uma interrupção.
- Em uma implantação VDI multizona, até 10.000 VDAs em cada zona podem ser tratados de forma eficaz durante uma interrupção, até um máximo de 40.000 VDAs no site. Por exemplo, cada um dos seguintes sites pode ser tratado de forma eficaz durante uma interrupção:
  - Um site com quatro zonas, cada uma contendo 10.000 VDAs.
  - Um site com sete zonas, uma contendo 10.000 VDAs e seis contendo 5.000 VDAs cada.

Durante uma interrupção, o gerenciamento de carga dentro do site pode ser afetado. Os avaliadores de carga (e especialmente as regras de contagem de sessões) podem ser excedidos.

Durante o tempo que leva para todos os VDAs se registrarem em um broker secundário, esse serviço pode não ter informações completas sobre as sessões atuais. Assim, uma solicitação de conexão de usuário durante esse intervalo pode resultar no lançamento de uma nova sessão, mesmo que a reconexão a uma sessão existente fosse possível. Esse intervalo (enquanto o "novo" broker secundário adquire informações de sessão de todos os VDAs durante o novo registro) é inevitável. As sessões que estão conectadas quando uma interrupção começa não são afetadas durante o intervalo de transição, mas novas sessões e reconexões de sessão podem ser.

Este intervalo ocorre sempre que os VDAs devem se registrar:

- Uma interrupção começa: Ao migrar de um broker principal para um broker secundário.
- Falha do broker secundário durante uma interrupção: Ao migrar de um broker secundário que falhou para um broker secundário recém-eleito.
- Recuperação de uma interrupção: Quando as operações normais são retomadas e o broker principal retoma o controle.

Você pode diminuir o intervalo reduzindo o valor do registro `HeartbeatPeriodMs` do Citrix Broker Protocol (padrão = 600000 ms, que são 10 minutos). Este valor de heartbeat é o dobro do intervalo que o VDA usa para pings, então o valor padrão resulta em um ping a cada 5 minutos.

Por exemplo, o seguinte comando altera o heartbeat para cinco minutos (300000 milissegundos), o que resulta em um ping a cada 2,5 minutos:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Tenha cuidado ao alterar o valor do heartbeat. Aumentar a frequência resulta em maior carga nos Controllers durante os modos normal e de interrupção.

O intervalo não pode ser totalmente eliminado, não importa quão rapidamente os VDAs se registrem.

O tempo necessário para sincronizar entre brokers secundários aumenta com o número de objetos (como VDAs, aplicativos, grupos). Por exemplo, sincronizar 5000 VDAs pode levar 10 minutos ou mais para ser concluído.

Diferenças das versões do XenApp 6.x

Embora esta implementação do Cache de Host Local compartilhe o nome do recurso Cache de Host Local no XenApp 6.x e versões anteriores do XenApp, há melhorias significativas. Esta implementação é mais robusta e imune à corrupção. Os requisitos de manutenção são minimizados, como a eliminação da necessidade de comandos `dsmaint` periódicos. Este Cache de Host Local é uma implementação tecnicamente diferente.

Gerenciar Cache de Host Local

Para que o Cache de Host Local funcione corretamente, a política de execução do PowerShell em cada Controller deve ser definida como RemoteSigned, Unrestricted ou Bypass.

SQL Server Express LocalDB

O software Microsoft SQL Server Express LocalDB que o Cache de Host Local usa é instalado automaticamente quando você instala um Controller ou atualiza um Controller de uma versão anterior à 7.9. Apenas o broker secundário se comunica com este banco de dados. Você não pode usar cmdlets do PowerShell para alterar nada sobre este banco de dados. O LocalDB não pode ser compartilhado entre Controllers.

O software de banco de dados SQL Server Express LocalDB é instalado independentemente de o Cache de Host Local estar ativado.

Para evitar sua instalação, instale ou atualize o Controller usando o comando `XenDesktopServerSetup.exe` e inclua a opção `/exclude "Local Host Cache Storage (LocalDB)"`. No entanto, lembre-se de que o recurso Cache de Host Local não funcionará sem o banco de dados, e você não pode usar um banco de dados diferente com o broker secundário.

A instalação deste banco de dados LocalDB não tem efeito sobre se você instala o SQL Server Express para uso como banco de dados do site.

Para obter informações sobre como substituir uma versão anterior do SQL Server Express LocalDB por uma versão mais recente, consulte Substituir SQL Server Express LocalDB.

Configurações padrão após a instalação e atualização do produto

Durante uma nova instalação do Citrix Virtual Apps and Desktops (versão mínima 7.16), o Cache de Host Local é ativado.

Após uma atualização (para a versão 7.16 ou posterior), o Cache de Host Local é ativado se houver menos de 10.000 VDAs em toda a implantação.

Ativar e desativar Cache de Host Local

- Para ativar o Cache de Host Local, digite:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Para determinar se o Cache de Host Local está ativado, digite `Get-BrokerSite`. Verifique se a propriedade `LocalHostCacheEnabled` é `True`.

- Para desabilitar o Local Host Cache, digite:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Lembre-se: A partir do XenApp e XenDesktop 7.16, o leasing de conexão (o recurso que precedeu o Local Host Cache a partir da versão 7.6) foi removido do produto e não está mais disponível.

Verificar se o Local Host Cache está funcionando

Para verificar se o Local Host Cache está configurado e funcionando corretamente:

- 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 SQL Server Express LocalDB foi criado em cada Delivery Controller. Isso confirma que o broker secundário pode assumir, se necessário.

    - No servidor Delivery Controller, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
    - Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.

- Force uma interrupção nos Delivery Controllers. Depois de verificar se o Local Host Cache funciona, lembre-se de colocar todos os Controllers 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 de eventos, o modo de interrupção é referido como *modo HA*.*

Serviço de Sincronização de Configuração:

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados do Local Host Cache usando o broker do Local Host Cache.

- 503: O Serviço de Sincronização de Configuração do Citrix recebeu uma configuração atualizada. Este evento indica o início do processo de sincronização.
- 504: O Serviço de Sincronização de Configuração do Citrix importou uma configuração atualizada. A importação da configuração foi concluída com êxito.
- 505: O Serviço de Sincronização de Configuração do Citrix falhou em uma importação. A importação da configuração não foi concluída com êxito. Se uma configuração anterior bem-sucedida estiver disponível, ela será usada se ocorrer uma interrupção. No entanto, estará desatualizada em relação à configuração atual. Se não houver configuração anterior disponível, o serviço não poderá participar do balanceamento de sessão durante uma interrupção. Neste caso, consulte a seção Solução de problemas e entre em contato com o Suporte Citrix.
- 507: O Serviço de Sincronização de Configuração do Citrix abandonou uma importação porque o sistema está em modo de interrupção e o broker do Local Host Cache está sendo usado para balanceamento. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque ocorreu uma interrupção. Este é um comportamento esperado.
- 510: Nenhum dado de configuração do Serviço de Configuração recebido do Serviço de Configuração primário.
- 517: Houve um problema na comunicação com o Broker primário.

- 518: O script de sincronização de configuração foi abortado porque o Broker secundário (Serviço de Alta Disponibilidade) não está em execução.

Serviço de Alta Disponibilidade:

Este serviço também é conhecido como broker do Local Host Cache.

- 3502: Uma interrupção ocorreu e o broker do Local Host Cache está realizando operações de corretagem.
- 3503: Uma interrupção foi resolvida e as operações normais foram retomadas.
- 3504: Indica qual broker do Local Host Cache foi eleito, além de outros brokers do Local Host Cache envolvidos na eleição.
- 3507: Fornece uma atualização de status do Local Host Cache a cada 2 minutos, indicando que o modo Local Host Cache está ativo no broker eleito. Contém um resumo da interrupção, incluindo duração da interrupção, registro de VDA e informações da sessão.
- 3508: Anuncia que o Local Host Cache não está mais ativo no broker eleito e que as operações normais foram restauradas. Contém um resumo da interrupção, incluindo duração da interrupção, número de máquinas que se registraram durante o evento Local Host Cache e número de lançamentos bem-sucedidos durante o evento LHC.
- 3509: Notifica que o Local Host Cache está ativo no(s) broker(s) não eleito(s). Contém uma duração de interrupção a cada 2 minutos e indica o broker eleito.
- 3510: Anuncia que o Local Host Cache não está mais ativo no(s) broker(s) não eleito(s). Contém a duração da interrupção e indica o broker eleito.

Forçar uma interrupção

Você pode querer forçar deliberadamente uma interrupção.

- Se sua rede está oscilando 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 consequentes tempestades frequentes de registro de VDA).
- Para testar um plano de recuperação de desastres.
- Para ajudar a garantir que o Local Host Cache esteja funcionando corretamente.
- Ao substituir ou fazer a manutenção do servidor de banco de dados do site.

Para forçar uma interrupção, edite o registro de cada servidor que contém um Delivery Controller. Em `HKLM\Software\Citrix\DesktopServer\LHC`, crie e defina `OutageModeForced` como `REG_DWORD` para `1`. Essa configuração instrui o broker do Cache de Host Local a entrar no

modo de interrupção, independentemente do estado do banco de dados. Definir o valor como `0` tira o broker do 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 registrado.

Rastreamento CDF: Contém opções para os módulos `ConfigSyncServer` e `BrokerLHC`. Essas opções, juntamente com outros módulos de broker, provavelmente identificarão o problema.

Relatório: Se uma importação de sincronização falhar, você pode gerar um relatório. Este relatório para no objeto que causa o erro. Este recurso de relatório afeta a velocidade de sincronização, então a Citrix recomenda desativá-lo quando não estiver em uso.

Para habilitar e produzir um relatório de rastreamento CSS, digite 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.htm`

Após a geração do relatório, digite o seguinte comando para desabilitar o recurso de relatório:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

Exportar a configuração do broker: Fornece a configuração exata para fins de depuração.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Por exemplo, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Comandos PowerShell do Cache de Host Local

Você pode gerenciar o Cache de Host Local (LHC) em seus Delivery Controllers usando comandos PowerShell.

O módulo PowerShell está localizado no seguinte local nos Delivery Controllers:

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **Importante:**
>
> Execute este módulo apenas nos Delivery Controllers.

Importar módulo PowerShell

Para importar o módulo, execute o seguinte em seu Delivery Controller.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

Comandos PowerShell para gerenciar o LHC

Os comandos a seguir ajudam você a ativar e gerenciar o modo LHC nos Delivery Controllers.

CMDLETS	FUNÇÃO
`Enable-LhcForcedOutageMode`	Coloca o Broker no modo LHC. Os arquivos de banco de dados LHC devem ter sido criados com sucesso pelo Serviço ConfigSync para que `Enable-LhcForcedOutageMode` funcione corretamente. Este cmdlet apenas força o LHC no Delivery Controller onde foi executado. Para que o LHC se torne ativo, este comando deve ser executado em todos os Delivery Controllers dentro da zona.
`Disable-LhcForcedOutageMode`	Tira o Broker do modo LHC. Este cmdlet apenas desabilita o modo LHC no Delivery Controller onde foi executado. `Disable-LhcForcedOutageMode` deve ser executado em todos os Delivery Controllers dentro da zona.
`Set-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o Serviço de Sincronização de Configuração (CSS) da Citrix verifica as alterações de configuração dentro do site. O intervalo de tempo pode variar de 60 segundos (um minuto) a 3600 segundos (uma hora). Essa configuração se aplica apenas ao Delivery Controller no qual foi executada. Para

CMDLETS	FUNÇÃO
	consistência entre os Delivery Controllers, considere executar este cmdlet em cada Delivery Controller. Por exemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o Serviço de Sincronização de Configuração (CSS) da Citrix verifica as alterações de configuração dentro do site para o valor padrão de 300 segundos (cinco minutos). Essa configuração se aplica apenas ao Delivery Controller no qual foi executada. Para consistência entre os Delivery Controllers, considere executar este cmdlet em cada Delivery Controller.
`Enable-LhcHighAvailabilitySDK`	Habilita o acesso a todos os cmdlets `Get-Broker*` dentro do Delivery Controller onde foi executado.
`Disable-LhcHighAvailabilitySDK`	Desabilita o acesso aos cmdlets do Broker dentro do Delivery Controller onde foi executado.

Observação:

- Use a porta 89 ao executar os cmdlets `Get-Broker*` no Delivery Controller. Por exemplo:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- Quando não está no modo LHC, o Broker LHC no Delivery Controller contém apenas informações de configuração.
- Durante o modo LHC, o Broker LHC no Delivery Controller eleito contém as seguintes informações:
  - Estados dos recursos

- Detalhes da sessão
- Registros de VDA
- Informações de configuração

Máquinas e sessões

Observação:

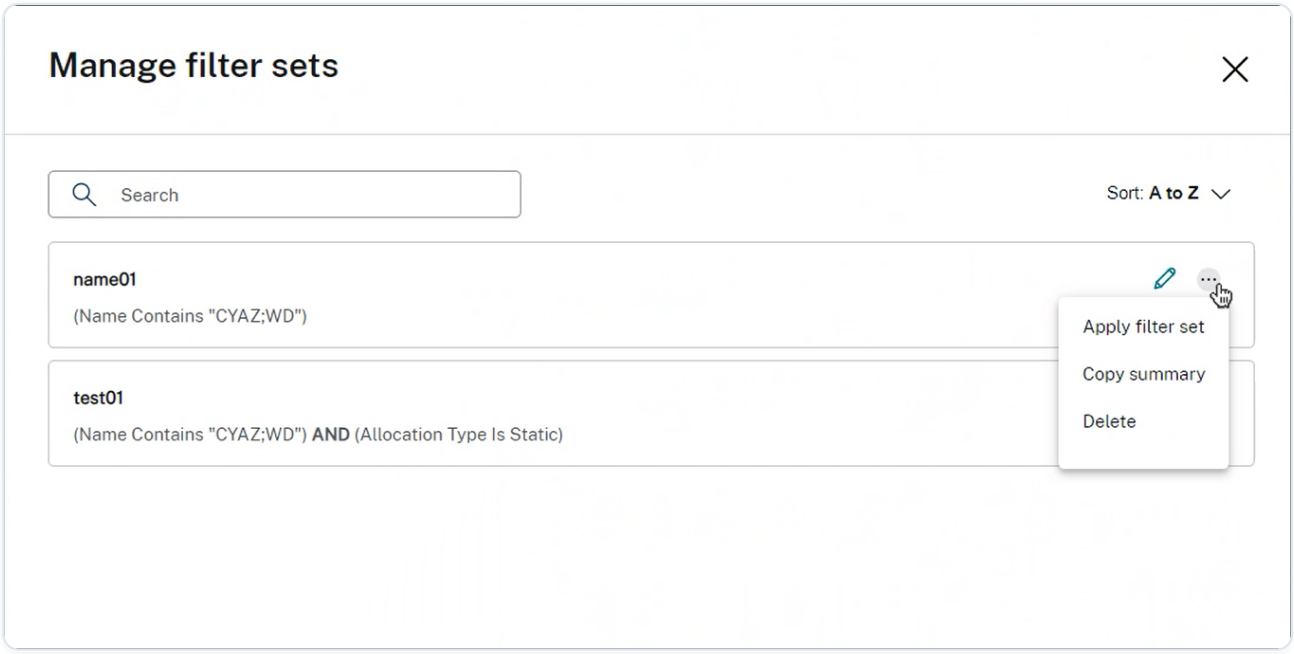
Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Use o recurso de pesquisa para visualizar informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou grupos de entrega específicos. Depois de selecionar **Pesquisar** no Web Studio, você tem várias opções:

- Use as guias para listar máquinas por tipo (SO de sessão única ou multi-sessão) ou listar todas as sessões.
- Digite o nome na caixa de pesquisa. Conforme você digita, filtros são fornecidos para uma pesquisa rápida.
- Refine a pesquisa usando filtros.
  - Por padrão, os seguintes filtros são fixados na visualização: **Nome**, **Estado da Sessão** e **Estado de Falha**. Selecione um filtro para construir uma expressão. Para personalizar seus filtros, clique nas reticências. Na janela que aparece, você pode fazer o seguinte:
    - Fixar ou desafixar filtros. Filtros desafixados são para uso único e não são salvos.
    - Clique em um filtro para adicioná-lo à visualização.
    - Limpe os filtros para limpar a pesquisa filtrada atual e remover os filtros desafixados.
  - Clique no operador para alternar entre **Corresponder a todos** (operador **E**) ou **Corresponder a qualquer um** (operador **OU**). Quando definido como **Corresponder a todos**, a pesquisa retorna resultados que correspondem a todos os critérios de filtro.

Quando definido como Corresponder a qualquer um, a pesquisa retorna resultados que correspondem a qualquer um dos critérios de filtro.

- Salve seus filtros em uso clicando no símbolo de estrela. O item salvo é conhecido como um conjunto de filtros. Os itens salvos aparecem na lista de Conjuntos de filtros salvos. (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 gerenciar conjuntos de filtros salvos, selecione a caixa de pesquisa e, em seguida, selecione **Gerenciar**.



Pesquisar sem filtros

Conforme você digita em uma caixa de pesquisa, um menu com sugestões aparece, fornecendo diferentes opções de pesquisa para ajudá-lo a refinar rapidamente sua pesquisa. Suponha que o conteúdo digitado seja *VM01*. Selecione uma das seguintes sugestões:

- Nome VM01. Pesquisa por nome.
- Catálogo de Máquinas VM01. Pesquisa por nome.
- Grupo de Entrega VM01. Pesquisa pelo nome do grupo de entrega.

Ao realizar uma pesquisa geral, o Citrix Virtual Apps and Desktops pesquisa correspondências nos seguintes critérios e fornece resultados relevantes:

- **Nome**. Pesquisa por nome da máquina ou nome DNS.
- **Catálogo de Máquinas**. Pesquisa pelo nome do catálogo de máquinas.
- **Grupo de Entrega**. Pesquisa pelo nome do grupo de entrega.
- **Usuário**. Pesquisa por nome de usuário da sessão.

- **Cliente**. Pesquisa por nome do cliente da sessão.
- **VM**. Pesquisa por nome da máquina hospedada. É o nome amigável da máquina hospedada usado pelo seu hipervisor.
- **Nome do Servidor de Hospedagem**. Pesquisa por nome do servidor de hospedagem.

Ao pesquisar um item específico, como usuário, grupo de desktops, catálogo ou máquina, a pesquisa geral oferece 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 Catálogo de Máquinas e Grupo de Entrega. A funcionalidade de pesquisa nesses nós oferece a mesma interface que o nó Pesquisar, proporcionando uma experiência de pesquisa contínua em todo o Citrix Virtual Apps and Desktops.

Você pode realizar pesquisas gerais e pesquisas baseadas em filtros. No Catálogo de Máquinas, os seguintes filtros estão disponíveis:

- **Nome do Catálogo**. Pesquisa pelo nome do catálogo de máquinas.
- **Tipo de Alocação**. Filtra por alocação estática (dedicada) ou aleatória (agrupada), ou ambas.
- **Tipo de Provisionamento**. Filtra por método de provisionamento manual ou MCS, ou ambos.
- **Suporte à Sessão**. Filtra por máquina de sessão única ou multi-sessão, ou ambas.
- **Contagem Alocada**. Filtra pelo número de máquinas alocadas.
- **Persistência**. Filtra por alterações de máquina não persistentes (descartar) ou persistentes (em disco local), ou ambas.
- **Tipo de Máquina**. Filtra por tipo de máquina física ou virtual, ou ambos.

Nos Grupos de Entrega, os seguintes filtros estão disponíveis:

- **Nome do Grupo**. Pesquisa pelo nome do grupo de entrega.
- **Descrição**. Filtra pela descrição do grupo de entrega especificada durante a criação do grupo de entrega.
- **Suporte à Sessão**. Filtra por máquina de sessão única ou multi-sessão, ou ambas.
- **Identidade da Máquina**. Filtra pela identidade da máquina.
- **Acesso Remoto a PC**. Filtra por máquina de Acesso Remoto a PC.

- **Modo de manutenção**. Filtra por máquinas em modo de manutenção (ativado, desativado ou ambos).
- **Estado do Grupo**. Filtra pelo estado do grupo. (A opção Habilitar grupo de entrega em Editar Grupo de Entrega > Configurações do Usuário controla se a entrega de aplicativos e desktops deve ser interrompida.)
- **Tipo de Alocação**. Filtra por tipo estático (dedicado) ou aleatório (agrupado), ou ambos.

Ao realizar uma pesquisa geral, o Citrix Virtual Apps and Desktops pesquisa itens nos seguintes critérios e fornece resultados relevantes:

- Catálogos de Máquinas:
  - Nome: Pesquisa catálogos 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.
- Grupos de Entrega:
  - Nome do grupo de entrega: Pesquisa grupos de entrega por nome.
  - Descrição: Pesquisa pela descrição do grupo de entrega especificada durante a criação do grupo de entrega.

Pesquisar Grupo de Aplicativos

Você pode realizar pesquisas gerais e pesquisas baseadas em filtro para grupos de aplicativos. No grupo de aplicativos, os seguintes filtros estão disponíveis:

- **Nome**. Filtra pelo nome do grupo de aplicativos.
- **Tag**. Filtra pela tag do grupo de aplicativos.
- **Descrição**. Filtra pela descrição do grupo de aplicativos especificada durante a criação do grupo de aplicativos.
- **Grupo de entrega**. Filtra pelo grupo de entrega do grupo de aplicativos.
- **Estado**. Filtra pelo estado do grupo de aplicativos.

Personalizar colunas a serem exibidas

Ao personalizar colunas, você pode ver colunas marcadas com o rótulo **Degrada o desempenho**. A seleção dessas colunas pode degradar o desempenho do console. Depois de concluir sua

personalização, a tabela é atualizada para exibir as colunas que você selecionou. A presença delas pode resultar em atrasos ao atualizar a tabela.

Se sua personalização contiver colunas que degradam o desempenho, você será solicitado a determinar se deseja preservá-las. O prompt aparece depois que você atualiza a janela do navegador ou sai do console e, em seguida, faz login. Esteja ciente das seguintes considerações se você 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: **Máquinas OS de sessão única**, **Máquinas OS de várias sessões** e **Sessões**. Se você precisar de atualizações mais frequentes, remova todas as colunas que degradam o desempenho.

Exportar resultados da pesquisa para um arquivo CSV

Você pode exportar seus resultados de pesquisa (até 10.000 itens) para um arquivo CSV. O arquivo é salvo no local de download padrão do seu navegador.

Este recurso está disponível para máquinas e sessões. Para exportar seus resultados de pesquisa, clique no ícone de exportação no canto superior direito. A exportação pode levar até 1 minuto para ser concluída.

Em cada guia do nó Pesquisar, você não pode realizar outra exportação enquanto uma exportação estiver em andamento.

Dicas para aprimorar uma pesquisa

Considere as seguintes dicas ao usar o recurso Pesquisar:

- No nó **Pesquisar**, selecione qualquer coluna para classificar os itens.
- Para mostrar mais características a serem incluídas na exibição onde você pode pesquisar e classificar, selecione **Colunas a Exibir** ou clique em qualquer coluna e selecione **Colunas a Exibir**. Na janela **Colunas a Exibir**, marque a caixa de seleção ao lado dos itens que você deseja exibir e selecione **Salvar** para sair.

> **Observação:**
>
> Os itens que degradam o desempenho são marcados com o rótulo **Degrada o desempenho**.

- Para localizar um dispositivo de usuário conectado a uma máquina, use **Cliente (IP)** e **É**, e insira o endereço IP do dispositivo.
- Para localizar sessões ativas, use **Estado da Sessão**, **É** e **Conectado**.
- Para listar todas as máquinas em um grupo de entrega, selecione **Grupos de Entrega** no painel esquerdo. Selecione o grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações ou no menu de contexto.

Tenha as seguintes considerações em mente ao realizar operações de classificação:

- Enquanto o número de itens não exceder 5.000, você pode clicar em qualquer coluna para classificar os itens nela. Quando o número exceder 5.000, você só poderá classificar por nome ou por usuário atual (dependendo da guia em que você está). Para habilitar a classificação, use filtros para reduzir o número de itens para 5.000 ou menos.
- Quando o número de itens é maior que 500, mas não mais que 5.000:
  - Armazenamos todos os dados em cache localmente para melhorar o desempenho da classificação. Nas guias **Máquinas OS de sessão única** e **Máquinas OS de várias sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Nome**) para classificar. Na guia **Sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Usuário Atual**) para classificar. Como resultado, a classificação leva mais tempo para ser concluída. Para um desempenho mais rápido, classifique por nome ou usuário atual, ou use filtros para reduzir o número de itens.
  - A seguinte mensagem abaixo da tabela indica que os dados estão em cache: Última atualização: `<the time when you refreshed the table>`. Nesse caso, as operações de classificação são baseadas em itens que foram carregados anteriormente. Esses itens podem não estar atualizados. Para atualizá-los, clique no ícone de atualização.

Ações e colunas da máquina

Este artigo lista ações e colunas de máquina com descrições para sua referência.

Ações

Visualize as ações que você pode realizar em máquinas e suas descrições.

AÇÃO	DESCRIÇÃO	APLICA-SE A
Remover do Grupo de Entrega	Remove uma máquina do grupo de entrega.	Sessão única e multissessão

AÇÃO	DESCRIÇÃO	APLICA-SE A
Adicionar ao Grupo de Entrega	Adiciona uma máquina a um grupo de entrega.	Sessão única e multissessão
Exibir Sessões	Exibir as sessões em execução em uma máquina	Sessão única e multissessão
Gerenciar Tags	Adicione e gerencie tags para uma máquina. Para obter mais informações sobre casos de uso típicos de tags, consulte Tags.	Sessão única e multissessão
Ativar Modo de Manutenção	Coloque uma máquina em modo de manutenção antes de aplicar patches ou para solução de problemas. Este modo impede que novas conexões sejam feitas a essa máquina. Os usuários podem se conectar a sessões existentes nessa máquina, mas não podem iniciar novas sessões nela.	Sessão única e multissessão
Desativar Modo de Manutenção	Desative o modo de manutenção para uma máquina.	Sessão única e multissessão
Atualizar VDA	Atualizar VDA para uma máquina.	Máquinas de SO de sessão única ou multissessão que atendem a determinados requisitos: Saiba mais.
Fazer logoff	Forçar logoff de uma máquina	Sessão única e multissessão
Excluir	Excluir uma VM de um catálogo de máquinas, deixando-a intacta no	Sessão única e multissessão

AÇÃO	DESCRIÇÃO	APLICA-SE A
	hipervisor ou serviço de nuvem.	
Alterar Usuário	Atribuir uma máquina a um usuário específico.	máquinas *estáticas* de sessão única.
Iniciar	Iniciar uma máquina.	Sessão única e multissessão
Desligar	Desligar uma máquina.	Sessão única e multissessão
Reiniciar	Reiniciar uma máquina	Sessão única e multissessão
Suspender	Coloque uma máquina em estado de hibernação ou suspensão. Ao suspender uma máquina, os Delivery Controllers armazenam o conteúdo da memória da máquina em um arquivo e, em seguida, desligam a máquina.	Máquinas OS de sessão única
Retomar	Retome uma máquina suspensa. Ao retomar uma máquina suspensa, os Delivery Controllers iniciam a máquina e a restauram para o estado anterior.	Máquinas OS de sessão única
Forçar Reinicialização	Forçar a reinicialização de uma máquina.	Máquinas OS de sessão única
Forçar Desligamento	Forçar o desligamento de uma máquina.	Máquinas OS de sessão única

Colunas

Visualize todas as colunas da máquina e suas descrições por tipo:

- Máquina
- Detalhes da máquina

- Aplicativos
- Hospedagem
- Conexão
- Registro
- Detalhes da Sessão
- Sessão

Máquina

Colunas na categoria **Máquina**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Nome	O nome de host DNS da máquina.	Sessão única e multissessão
Catálogo de Máquinas	O nome do catálogo ao qual a máquina pertence.	Sessão única e multissessão
Grupo de Entrega	O nome do grupo de entrega ao qual a máquina pertence.	Sessão única e multissessão
Nome de Exibição do Usuário	Os nomes completos dos usuários associados à máquina (geralmente no formato `Firstname Lastname`). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas.	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
Usuário	Os nomes de usuário dos usuários associados à máquina (no formato “domínio\usuário”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas.	Sessão única e multissessão
Nome Principal do Usuário	Os Nomes Principais de Usuário dos usuários associados à máquina (no formato “usuário@domínio”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas.	Sessão única e multissessão
Nome de Exibição da Área de Trabalho	O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix Workspace™ ou no StoreFront. **Nota:** Para alterar a exibição de um desktop, você	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	precisa da permissão **Perform Machine Update** porque a alteração do nome de exibição envolve a atualização da propriedade da máquina.	
Condições do Desktop	A lista de condições pendentes do desktop para a máquina. Valores possíveis: Unknown, CPU, ICALatency e UPMLogonTime.	Sessão única e multissessão
Tipo de Alocação	O tipo de alocação da máquina: **Permanente**, quando alocada a um usuário permanentemente. **Aleatória**, quando alocada aleatoriamente.	Sessão única e multissessão
Modo de Manutenção	Indica se a máquina está no modo de manutenção.	Sessão única e multissessão
Configuração de Conexão do Windows	Modo de logon relatado pelo Windows.	Somente multissessão
	Valores possíveis: LogonEnabled, Draining, DrainingUntilRestart e LogonDisabled.	

COLUNA	DESCRIÇÃO	APLICA-SE A
Está Atribuído	Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/endereço). Os usuários podem ser atribuídos explicitamente ou por atribuição no primeiro uso da máquina.	Sessão única e multissessão
É Físico	Indica se a máquina é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada por energia pelos Delivery Controllers. `False` indica o contrário.	Sessão única e multissessão
Tipo de Provisionamento	Como a máquina foi provisionada. Valores possíveis: • Manual: Não provisionado usando PVS ou MCS. PVS: Provisionado usando PVS (máquinas físicas, blade e virtuais)	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	MCS: Provisionado usando MCS (somente VMs)	
Reinicialização Agendada	O estado de qualquer operação de reinicialização agendada para a máquina. Valores possíveis	Sessão única e multissessão
	Nenhum: Nenhuma reinicialização está agendada.	
	Pendente: Aguardando reinicialização, mas está disponível para uso. • Drenando: Aguardando reinicialização e está indisponível para novas sessões. No entanto, reconexões a conexões existentes ainda são permitidas. • Em Andamento: Em andamento ativo de uma	

COLUNA	DESCRIÇÃO	APLICA-SE A
	reinicialização agendada. • Natural: Reinicialização natural em andamento. A máquina está aguardando uma reinicialização.	
Zona	O nome da zona onde a máquina está localizada.	Sessão única e multissessão
Estado	O estado geral da área de trabalho associada à máquina, derivado de vários estados específicos, como estado da sessão, estado de registro e estado de energia.	Sessão única e multissessão
	Estados possíveis: Desligado, Não Registrado, Disponível, Desconectado, EmUso e Preparando.	
Tags	A lista de tags associadas à máquina.	Sessão única e multissessão
Atualização do VDA	O estado da máquina para ações	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	de atualização de pacote VDA.	
	Valores possíveis: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate e Unknown.	
Capaz de Suspender	Indica se a máquina suporta ações de energia (Suspender e Retomar).	Sessão única e multissessão
Índice de Carga	O índice de carga atual. Para obter mais informações, consulte Saiba mais.	Somente multissessão
Estado de Esvaziamento	Indica se a máquina está esvaziando e será desligada após o término de todas as sessões na máquina. 'True' aparece apenas para máquinas multissessão gerenciadas por energia.	Somente multissessão
	Nota: A máquina não desliga se estiver em modo de manutenção. Ela desliga somente depois de sair do modo de manutenção.	

Detalhes da máquina

Colunas na categoria **Detalhes da máquina**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Versão do Agente	A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina.	Sessão única e multi-sessão
Endereço IP	O endereço IP da máquina.	Sessão única e multi-sessão
Atribuído	Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/endereço). Os usuários podem ser atribuídos explicitamente ou por atribuição no primeiro uso da máquina.	Sessão única e multi-sessão
Tipo de SO	O tipo de sistema operacional em execução na máquina.	Somente sessão única

Aplicativos

Colunas na categoria **Aplicativos**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Aplicativo em Uso	A lista de aplicativos em uso na máquina (exibidos como nomes de navegador).	Sessão única e multissessão
Aplicativos Publicados	A lista de aplicativos publicados pela máquina (exibidos como nomes de navegador).	Sessão única e multissessão

Conexões

Colunas na categoria **Conexões**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Cliente (IP)	O endereço IP do cliente conectado à máquina.	Somente sessão única
Cliente	O nome do host do cliente conectado à máquina.	Somente sessão única
Versão do Plug-In	A versão do aplicativo Citrix Workspace no cliente conectado.	Somente sessão única
Conectado Via	O nome do host da conexão de entrada, geralmente um gateway, roteador ou cliente.	Somente sessão única
Conectado Via (IP)	O endereço IP da conexão de entrada, geralmente um gateway, roteador ou cliente.	Somente sessão única
Tipo de Conexão	O protocolo usado para a sessão. Valores possíveis: HDX, RDP e Console. Nota: O campo é deixado em branco para sessões de console em VDAs do XenDesktop® 5.	Somente sessão única
Hora da Última Conexão (UTC)	A hora da última tentativa de conexão detectada que falhou ou foi bem-sucedida.	Sessão única e multissessão
Último Usuário de Conexão	O nome SAM (no formato “DOMÍNIO\usuário”) do usuário que tentou uma conexão com a máquina pela última vez. Se o nome SAM não estiver disponível, o SID será usado.	Sessão única e multissessão
Secure ICA® Ativo	Indica se o SecureICA está ativo na sessão atual.	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	Sempre nulo para máquinas multissessão.	

Hospedagem

Colunas na categoria **Hospedagem**.

COLUNA	DESCRIÇÃO	APLICA-SE A
VM	O nome amigável de uma máquina hospedada executando a sessão, conforme usado por seu hipervisor. Não corresponde necessariamente ao nome DNS ou AD da máquina.	Sessão única e multi-sessão
Nome do Servidor de Hospedagem	O nome DNS do hipervisor que está hospedando a máquina, se gerenciado.	Sessão única e multi-sessão
Conexão	O nome da conexão do host atribuída à máquina que hospeda a sessão.	Sessão única e multi-sessão
Atualização Pendente	Indica se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina.	Sessão única e multi-sessão

COLUNA	DESCRIÇÃO	APLICA-SE A
Persistência de Alterações do Usuário	Como as alterações do usuário são tratadas, indicando se as alterações são persistentes: • OnLocal: Persistente. As alterações do usuário são salvas localmente. • Descartar: Não persistente. As alterações do usuário são descartadas.	Sessão única e multi-sessão
Ação de Energia Pendente	Indica se há alguma ação de energia pendente para a máquina.	Sessão única e multi-sessão
Estado de Energia	O estado de energia da máquina. Valores possíveis: Não gerenciado, Desconhecido, Indisponível, Desligado, Ligado, Suspenso, Ligando, Desligando, Suspendendo e Retomando.	Sessão única e multi-sessão
Será Desligado Após o Uso	Aplicável apenas a máquinas de sessão única gerenciadas	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	por energia. Indica se a máquina está comprometida e será desligada após o término de todas as sessões.	
	Observação: A máquina não será desligada se estiver em modo de manutenção. Ela será desligada somente depois que for retirada do modo de manutenção.	

Registro

Colunas na categoria **Registro**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Última Falha de Registro	O motivo da última desativação do registro da máquina com o broker.	Sessão única e multissessão
	Os valores possíveis são: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationC	

COLUNA	DESCRIÇÃO	APLICA-SE A
	apabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError e BrokerRegistrationLimitReached.	
Hora da Última Falha de Registro (UTC)	A hora da última desativação do registro da máquina.	Sessão única e multissessão
Estado do Registro	O estado de registro da máquina. Valores possíveis: Não registrado, Inicializando,	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	Registrado e Erro do Agente.	
Estado de Falha	O estado de resumo de qualquer estado de falha atual da máquina. Valores possíveis: • Nenhum: Nenhuma falha. A máquina está íntegra. • FalhaAoIniciar: A última operação de inicialização da máquina falhou. • TravadoNaInicialização: A máquina não conseguiu iniciar após ser ligada. • Não registrado. A máquina falhou ao registrar dentro do período esperado ou seu registro foi rejeitado. • Capacidade Máxima. A máquina está se	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	reportando com capacidade máxima.	

Detalhes da sessão

Colunas na categoria **Detalhes da sessão**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Iniciado por	O nome do host do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão.	Sessão única e multissessão
Iniciado por (IP)	O endereço IP do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão.	Sessão única e multissessão
Hora da Alteração da Sessão (UTC)	A hora da última alteração de estado da sessão atual.	Somente sessão única
Filtros SmartAccess	Tags Smart Access para a sessão atual. Sempre nulo para máquinas multissessão.	Sessão única e multissessão

Sessão

Colunas na categoria **Sessão**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Estado da Sessão	O estado da sessão atual. Valores possíveis: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting,	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	NonBrokeredSession e Unknown.	
Usuário Atual	O nome do usuário da sessão atual (no formato “DOMÍNIO\usuário”).	Somente sessão única
Hora de Início (UTC)	A hora de início da sessão atual.	Somente sessão única
Contagem de Sessões	O número de sessões na máquina.	Somente multissessão

Ações e colunas da sessão

Este artigo lista as ações e colunas da máquina com descrições para sua referência.

Ações

Visualize as ações que você pode realizar nas sessões e suas descrições.

AÇÃO	DESCRIÇÃO	APLICA-SE A SESSÕES EM
Fazer logoff	Desconectar um usuário de uma sessão.	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões
Enviar Mensagem	Envie uma mensagem para o usuário de uma sessão.	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões
Visualizar máquinas	Visualize a máquina host de uma sessão.	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões
Desconectar	Desconectar uma sessão. Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões

AÇÃO	DESCRIÇÃO	APLICA-SE A SESSÕES EM
	estará mais se comunicando com os Delivery Controllers.	
Desligar Máquina	Desliga a máquina associada a uma sessão.	Máquinas OS de sessão única
Reiniciar Máquina	Reinicia a máquina associada a uma sessão.	Máquinas OS de sessão única

Colunas

Exibir colunas da sessão e suas descrições.

COLUNA	DESCRIÇÃO
Usuário atual	O nome do usuário; o Nome Principal do Usuário (UPN) do usuário.
Nome	O nome do host DNS da máquina que hospeda a sessão.
Grupo de Entrega	O nome do grupo de entrega que contém a máquina que hospeda a sessão.
Catálogo de Máquinas	O nome do catálogo de máquinas que contém a máquina que hospeda a sessão.
Versão do Agente	A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina que hospeda a sessão.
Aplicativo em Uso	A lista de aplicativos em uso na sessão, identificados por seus nomes administrativos.

COLUNA	DESCRIÇÃO
Intermediação Autônoma	Indica se esta é uma sessão HDX™ estabelecida por uma conexão direta sem intermediação.
Hora da Intermediação (UTC)	A hora em que a sessão foi intermediada.
Nome de Usuário do Intermediador	O nome do usuário intermediador.
Cliente (IP)	O endereço IP do cliente conectado à sessão.
Cliente	O nome do host do cliente conectado à sessão.
Versão do Plug-In	A versão do aplicativo Citrix Workspace™ em execução no cliente conectado à sessão.
Conectado Via	O nome do host das conexões de entrada, tipicamente um gateway, roteador ou cliente.
Conectado Via (IP)	O endereço IP da conexão de entrada, geralmente um gateway, roteador ou cliente.
Tipo de Alocação	Se a sessão é compartilhada ou dedicada.
Oculto	Se a sessão está oculta para o usuário e não deve ser reconectada.
VM	O nome amigável da VM que hospeda a sessão, conforme usado pelo seu hipervisor. Não corresponde

COLUNA	DESCRIÇÃO
	necessariamente ao nome DNS ou AD da máquina.
Nome do Servidor de Hospedagem	O nome DNS do hipervisor que está hospedando a máquina que hospeda a sessão.
Conexão	O nome da conexão do host atribuída à máquina que hospeda a sessão.
Atualização Pendente	Se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina.
Modo de Manutenção	Se a máquina que hospeda a sessão está em modo de manutenção.
Endereço IP	O endereço IP da máquina que hospeda a sessão.
É Físico	Se a máquina que hospeda a sessão é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada por energia pelos Delivery Controllers. `False` indica o contrário.
Iniciado por	O nome do host do servidor StoreFront™ usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace.

COLUNA	DESCRIÇÃO
Iniciado por (IP)	O endereço IP do servidor StoreFront usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace.
Tipo de SO	A string de identificação do sistema operacional que hospeda a sessão.
Persistência de Alterações do Usuário	Como as alterações do usuário são tratadas, indicando se as alterações são persistentes: • OnLocal: Persistente. As alterações do usuário são salvas localmente. • Descartar: Não persistente. As alterações do usuário são descartadas.
Tipo de Conexão	O protocolo usado para a sessão, como HDX, RDP ou Console. **Nota:** O campo fica em branco para sessões de console em VDAs do XenDesktop® 5.
Tipo de Provisionamento	Como a máquina que hospeda a sessão foi provisionada:

COLUNA	DESCRIÇÃO
	• Manual: Não provisionado usando PVS ou MCS. • PVS: Provisionado por PVS (Máquinas físicas, blade e virtuais). • MCS: Provisionado por MCS (Somente VMs).
Secure ICA® Ativo	Se o SecureICA está ativo na sessão.
Estado da Sessão	O estado da sessão. Valores possíveis: Conectado, Ativo ou Desconectado. Outros estados podem ocorrer para sessões em máquinas com níveis funcionais anteriores a L7, como PreparingSession, Reconnecting, NonBrokeredSession, Other e Unknown.
Hora da Alteração da Sessão	A hora da alteração de estado mais recente para a sessão.
Estado do Aplicativo	O estado dos aplicativos na sessão. Valores possíveis: PreLogon, PreLaunched, Active, Desktop, Lingering e NoApps.
Suporte a Sessão	Se a máquina que hospeda a sessão suporta sessões múltiplas ou únicas.

COLUNA	DESCRIÇÃO
Zona	Nome da zona onde a máquina que hospeda a sessão está localizada.
Filtros SmartAccess	Tags de Acesso Inteligente para a sessão.
Hora de Início (UTC)	Quando a sessão foi iniciada.
Estado	O estado de resumo da máquina. Valores possíveis: Não Registrado, Desconectado ou Em Uso.
Tempo no Estado (UTC)	Há quanto tempo a sessão está em seu estado atual.
Delivery Controller™	O nome de host DNS do controlador com o qual a máquina que hospeda a sessão está registrada.
Nome de Exibição do Usuário	O nome completo do usuário.
Nome de Exibição da Área de Trabalho	O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix Workspace ou StoreFront. Para sessões de aplicativo, é o nome do primeiro aplicativo iniciado na sessão, mesmo que esse aplicativo já tenha sido encerrado. O nome permanece inalterado mesmo que o recurso seja posteriormente renomeado ou removido.

Chaves de segurança

Importante:

- 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 Citrix Gateway versão 12.1 e posterior.

Nota:

Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Este recurso permite que você permita que apenas máquinas StoreFront e Citrix Gateway aprovadas se comuniquem com os Delivery Controllers. Depois de habilitar este recurso, quaisquer solicitações que não contenham a chave são bloqueadas. Use este recurso para adicionar uma camada extra de segurança para proteger contra ataques originados da rede interna.

Um fluxo de trabalho geral para usar este recurso é o seguinte:

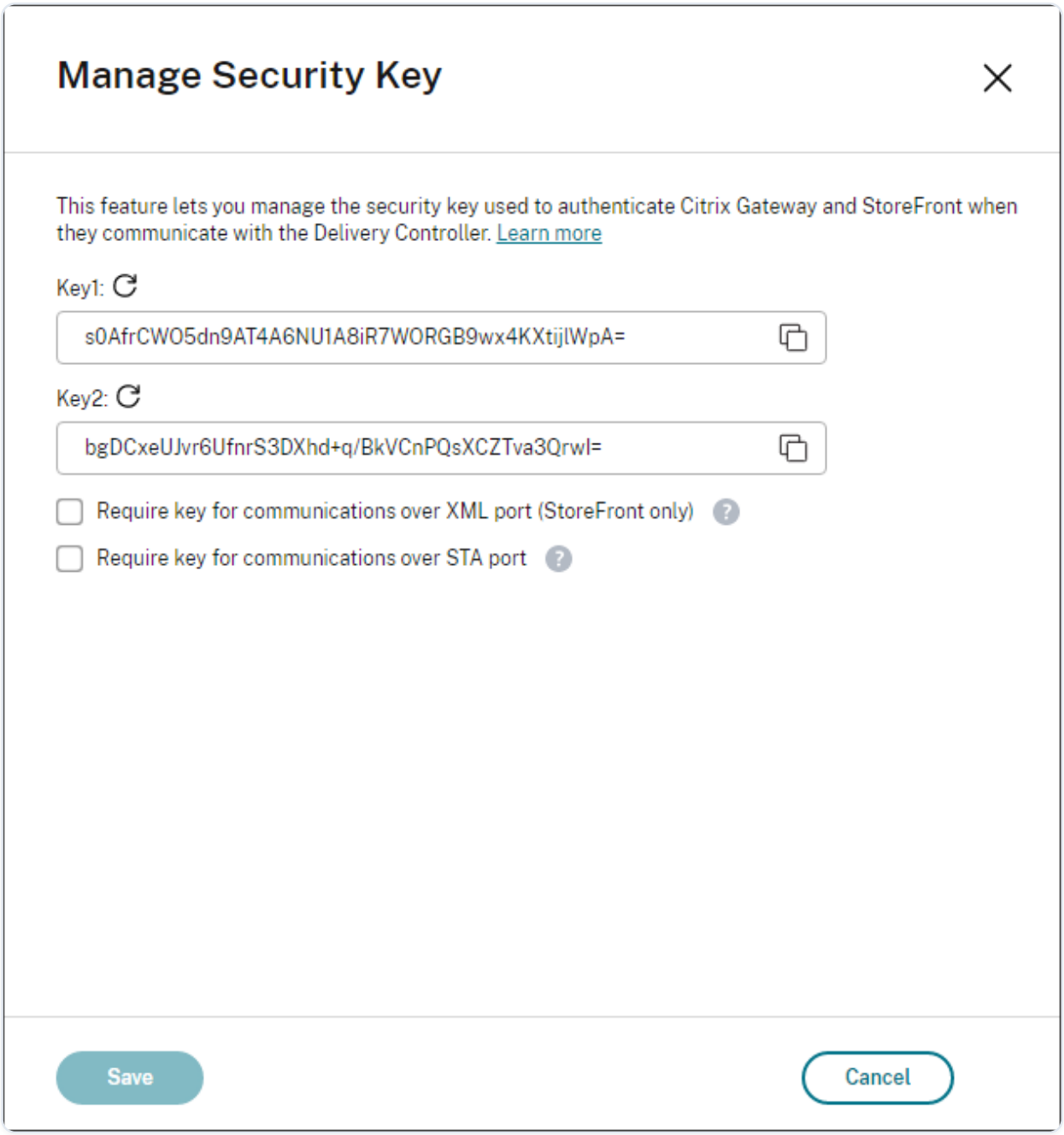
1. Habilite o Web Studio para mostrar as configurações do recurso.
2. Configure as configurações para o seu site.
3. Configure as configurações para o StoreFront.
4. Configure as configurações para o Citrix ADC.

Configurar as configurações para o site

Você pode usar o Web Studio ou o PowerShell para configurar as configurações da chave de segurança para o seu site.

Usar o Web Studio

1. Faça login no Web Studio, selecione **Configurações** no painel esquerdo.
2. Localize o bloco **Gerenciar chave de segurança** e clique em **Editar**. A página **Gerenciar Chave de Segurança** é exibida.



3. Clique no ícone de atualização para gerar as chaves.

> **Importante:**

- Existem duas chaves disponíveis para uso. Você pode usar a mesma chave ou chaves diferentes para comunicações pelas portas XML e STA. Recomendamos que você use apenas uma chave por vez. A chave não utilizada é usada apenas para rotação de chaves.
- Não clique no ícone de atualização para atualizar a chave já em uso. Se o fizer, ocorrerá interrupção do serviço.

4. Selecione onde uma chave é necessária para as comunicações:
   - **Exigir chave para comunicações pela porta XML (somente StoreFront)**. Se selecionado, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta XML, consulte o artigo da Central de Conhecimento CTX127945.
   - **Exigir chave para comunicações pela porta STA**. Se selecionado, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta STA, consulte o artigo da Central de Conhecimento CTX101988.
5. Clique em **Salvar** para aplicar suas alterações e fechar a janela.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações do Web Studio.

1. Execute o SDK do PowerShell Remoto do Citrix Virtual Apps and Desktops.
2. Em uma janela de comando, execute o seguinte comando:
   - `Add-PSSnapIn Citrix*`
3. Execute os seguintes comandos para gerar uma chave e configurar a Chave1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Execute os seguintes comandos para gerar uma chave e configurar a Chave2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. Execute um ou ambos os comandos a seguir para habilitar o uso de uma chave na autenticação de comunicações:
    - Para autenticar comunicações pela porta XML:
        - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
    - Para autenticar comunicações pela porta STA:
        - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

Configurar definições para o StoreFront

Após concluir a configuração do seu site, você precisa configurar as definições relevantes para o StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos PowerShell:

Para configurar a chave para comunicações pela porta XML, use o comando . Por exemplo:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Insira os valores apropriados para os seguintes parâmetros:

- `Path to store`
- `Resource feed name`
- `secret`

Para configurar a chave para comunicações sobre a porta STA, use os comandos `New-STFSecureTicketAuthority` e `Set-STFRoamingGateway`. Por exemplo:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]
```

```
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Insira os valores apropriados para os seguintes parâmetros:

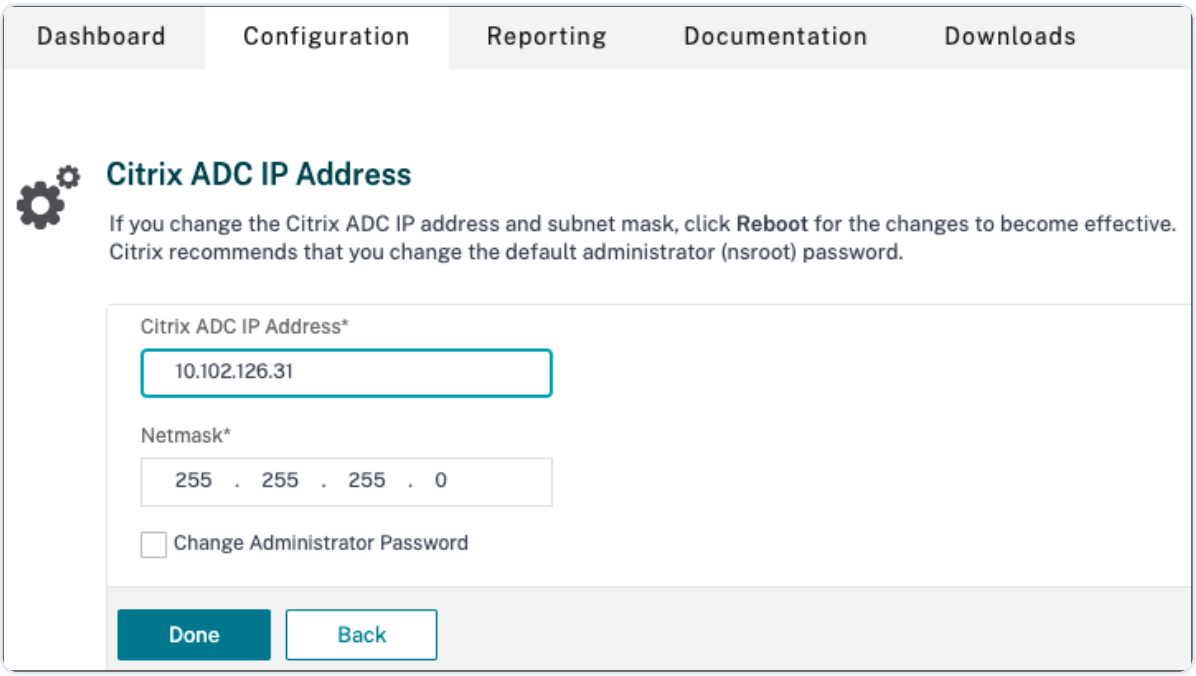
- `Gateway name`
- `STA URL`
- `Secret`

Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

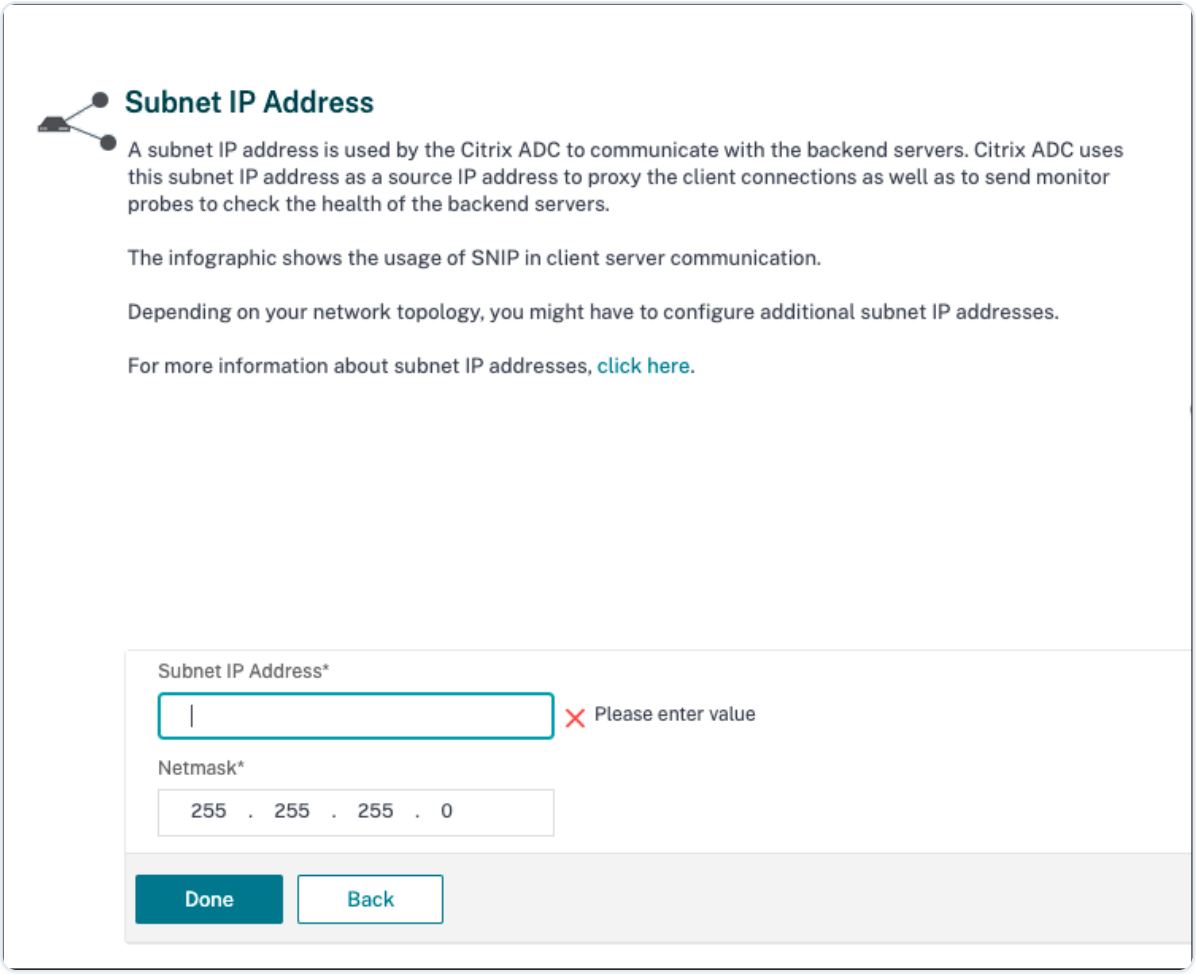
Configurar definições para o Citrix ADC

> **Observação:**
>
> A configuração desse recurso para o Citrix ADC não é necessária, a menos que você use o Citrix ADC como seu gateway. Se você usar o Citrix ADC, siga estas etapas:

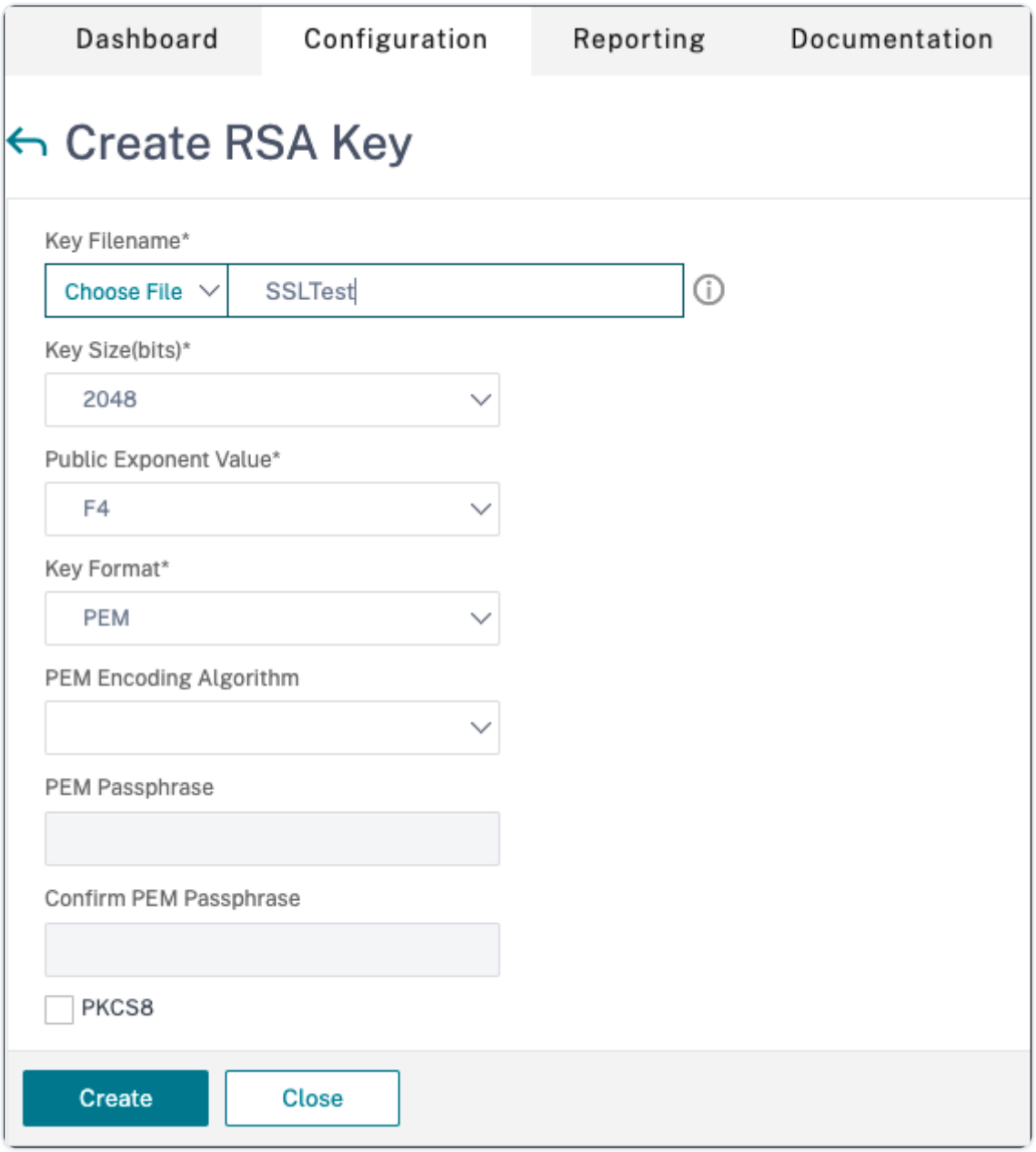
1. Certifique-se de que a seguinte configuração de pré-requisito já esteja em vigor:
    - Os seguintes endereços IP relacionados ao Citrix ADC estão configurados.
        - Endereço IP de Gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



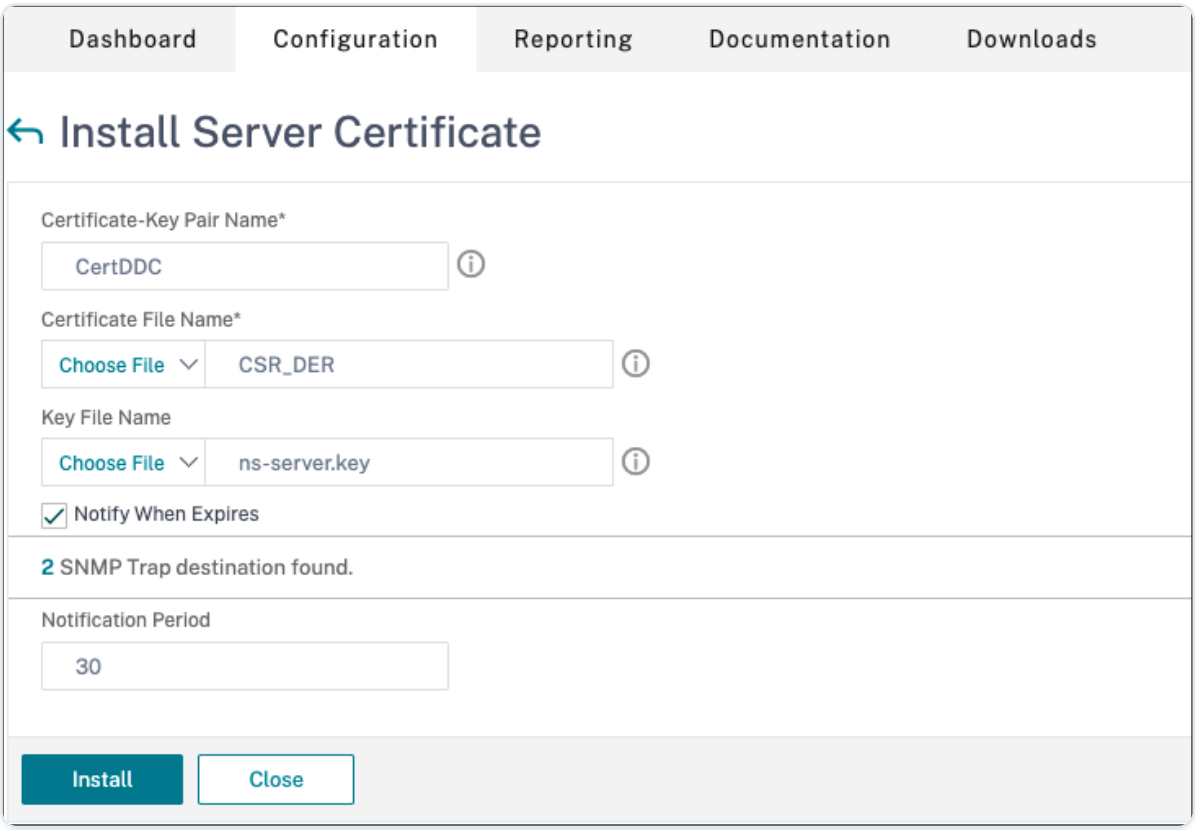
- Endereço IP de sub-rede (SNIP) para habilitar a comunicação entre o dispositivo Citrix ADC e os servidores de back-end. Para obter detalhes, consulte Configuring Subnet IP Addresses.
- Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no dispositivo ADC para o lançamento da sessão. Para obter detalhes, consulte Create a virtual server.

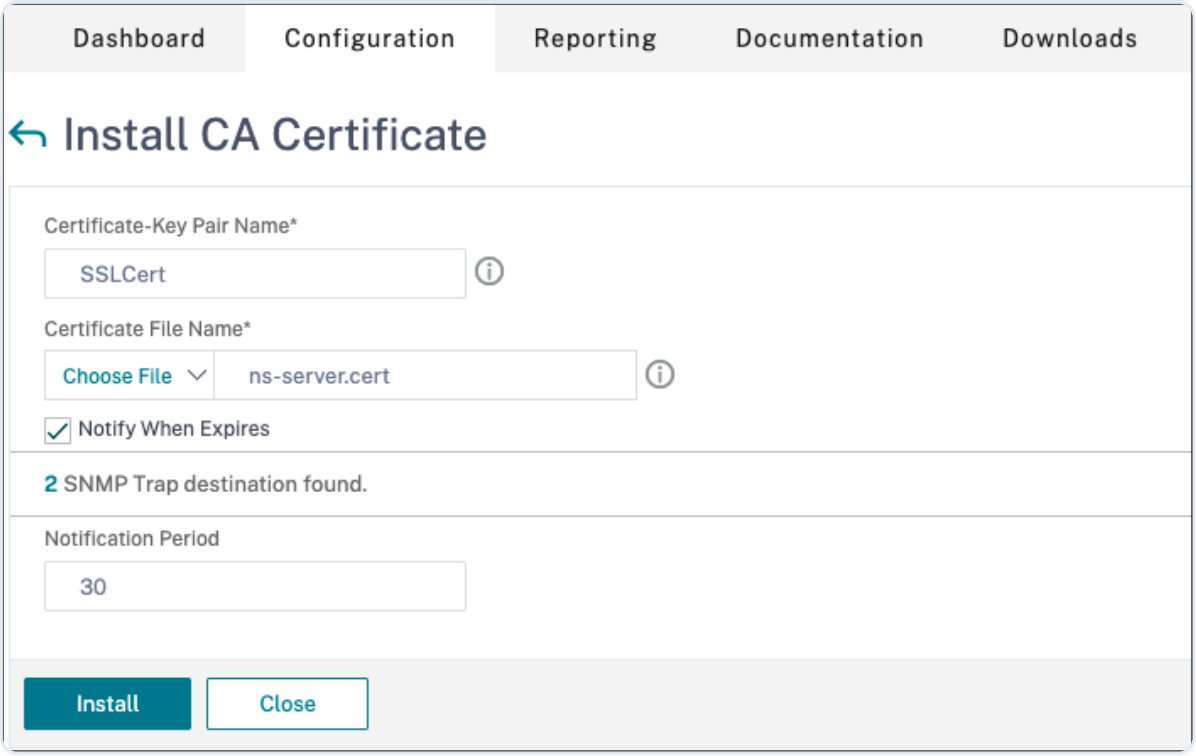


- Os modos e recursos necessários no dispositivo Citrix ADC estão habilitados.
  - Para habilitar os modos, na GUI do Citrix ADC, vá para **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, vá para **System > Settings > Configure Basic Features**.
- As configurações relacionadas a certificados estão concluídas.
  - A Solicitação de Assinatura de Certificado (CSR) é criada. Para obter detalhes, consulte Create a certificate.

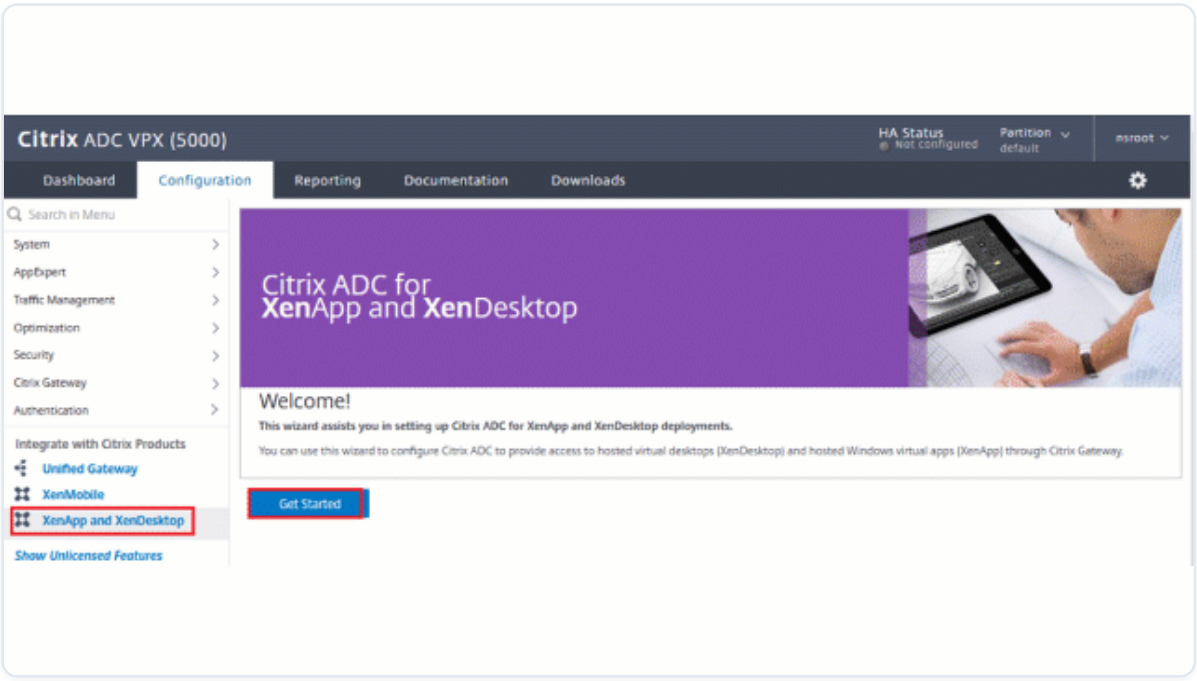


- Os certificados de servidor e CA e os certificados raiz são instalados. Para obter detalhes, consulte Install, link, and updates.





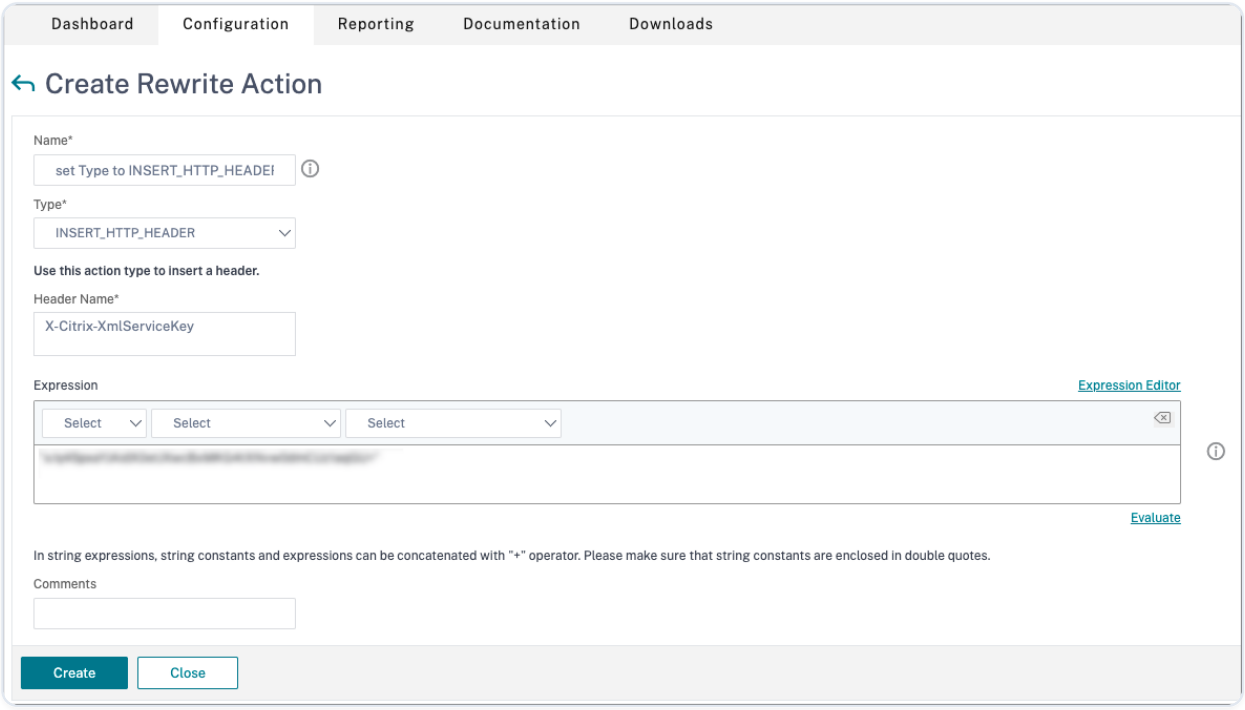
- Um Citrix Gateway foi criado para o Citrix Virtual Desktops. Teste a conectividade clicando no botão **Testar Conectividade STA** para confirmar que os servidores virtuais estão online. Para obter detalhes, consulte Configurando o Citrix ADC para Citrix Virtual Apps and Desktops.



2. Adicione uma ação de reescrita. Para obter detalhes, consulte Configuring a Rewrite Action.

   a. Vá para **AppExpert > Rewrite > Actions**.

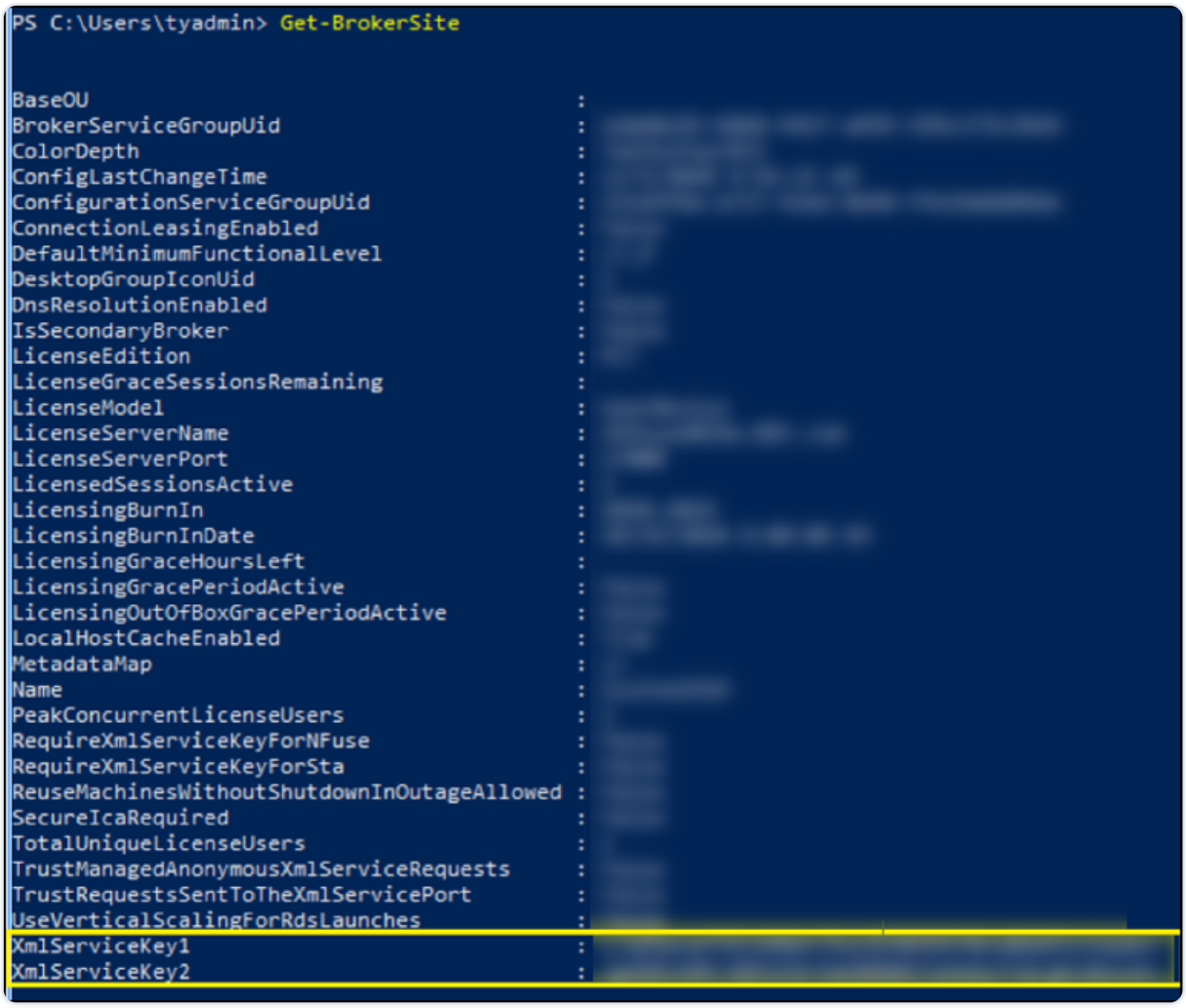
   b. Clique em **Adicionar** para adicionar uma nova ação de reescrita. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".



   a. Em **Tipo**, selecione **INSERT_HTTP_HEADER**.

   b. Em **Nome do Cabeçalho**, insira X-Citrix-XmlServiceKey.

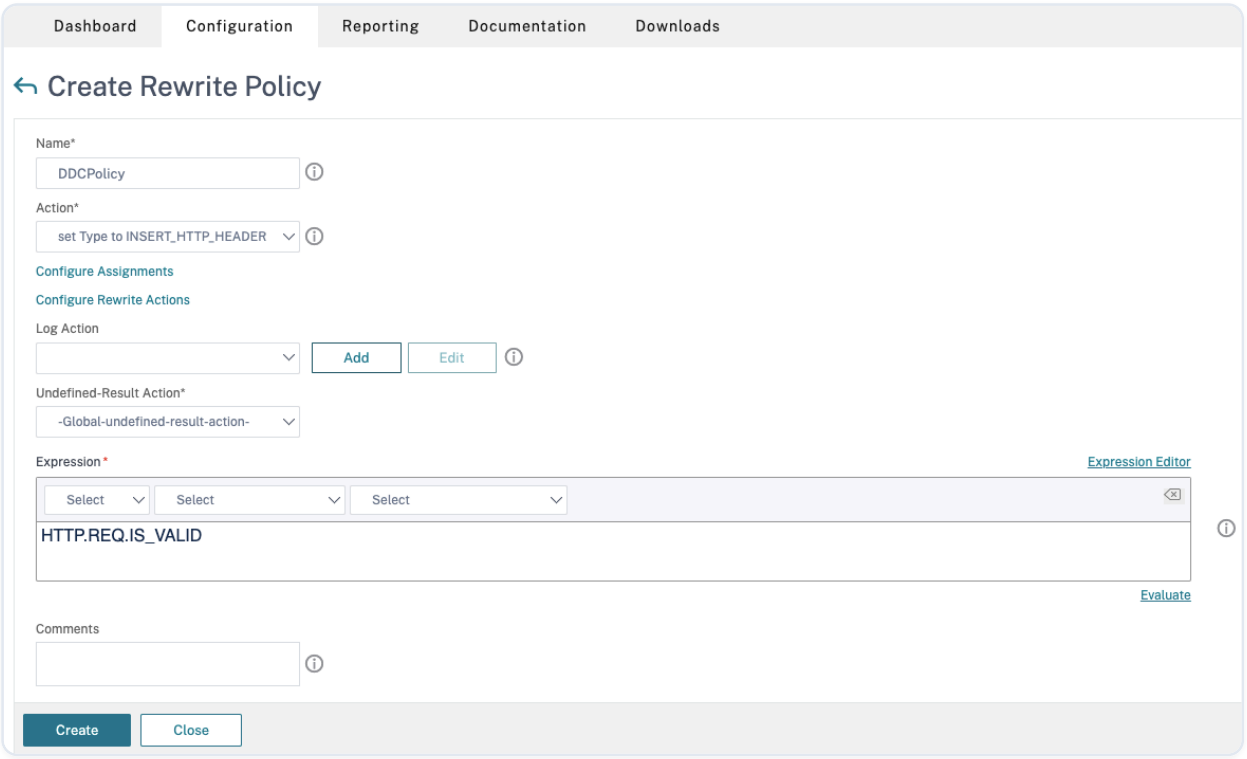
   c. Em **Expressão**, adicione `<XmlServiceKey1 value>` com as aspas. Você pode copiar o valor XmlServiceKey1 da sua configuração do Desktop Delivery Controller™.



3. Adicione uma política de reescrita. Para obter detalhes, consulte Configurando uma Política de Reescrita.

   a. Vá para **AppExpert > Rewrite > Policies**.

   b. Clique em **Adicionar** para adicionar uma nova política.



a. Em **Ação**, selecione a ação criada na etapa anterior.

b. Em **Expressão**, adicione HTTP.REQ.IS_VALID.

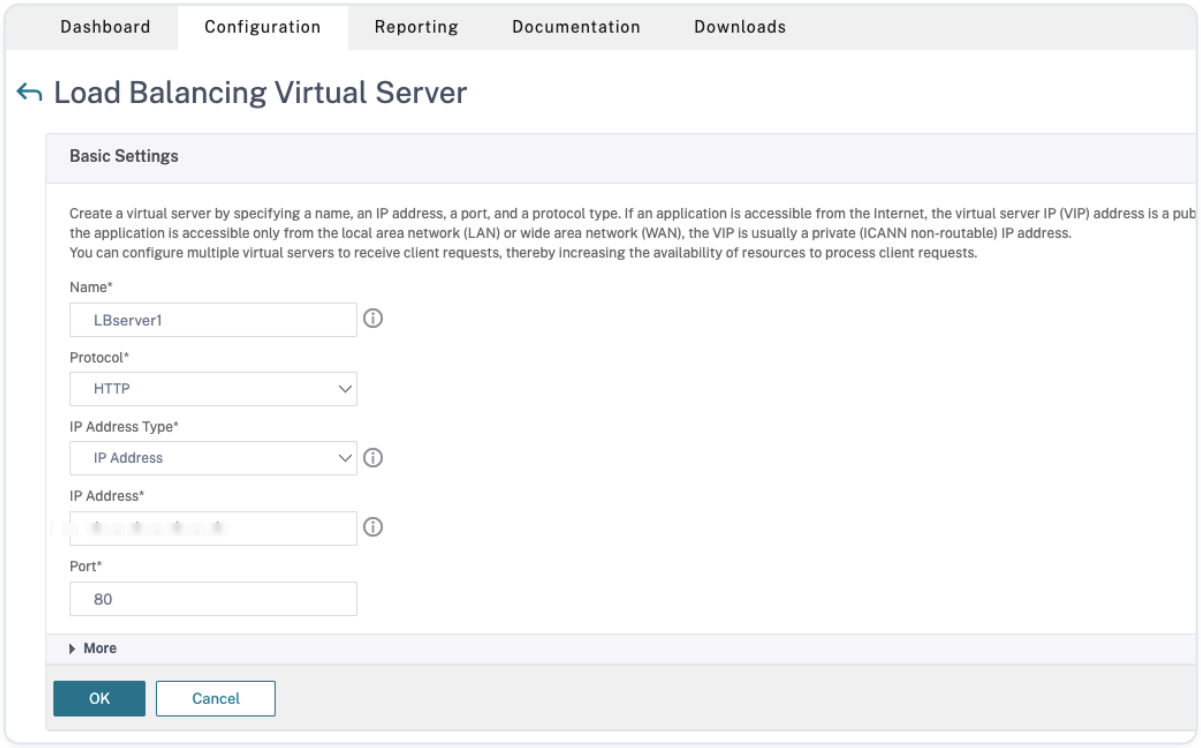
c. Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões não serão iniciadas.

   Para obter detalhes, consulte Configurar balanceamento de carga básico.

   a. Crie um servidor virtual de balanceamento de carga.

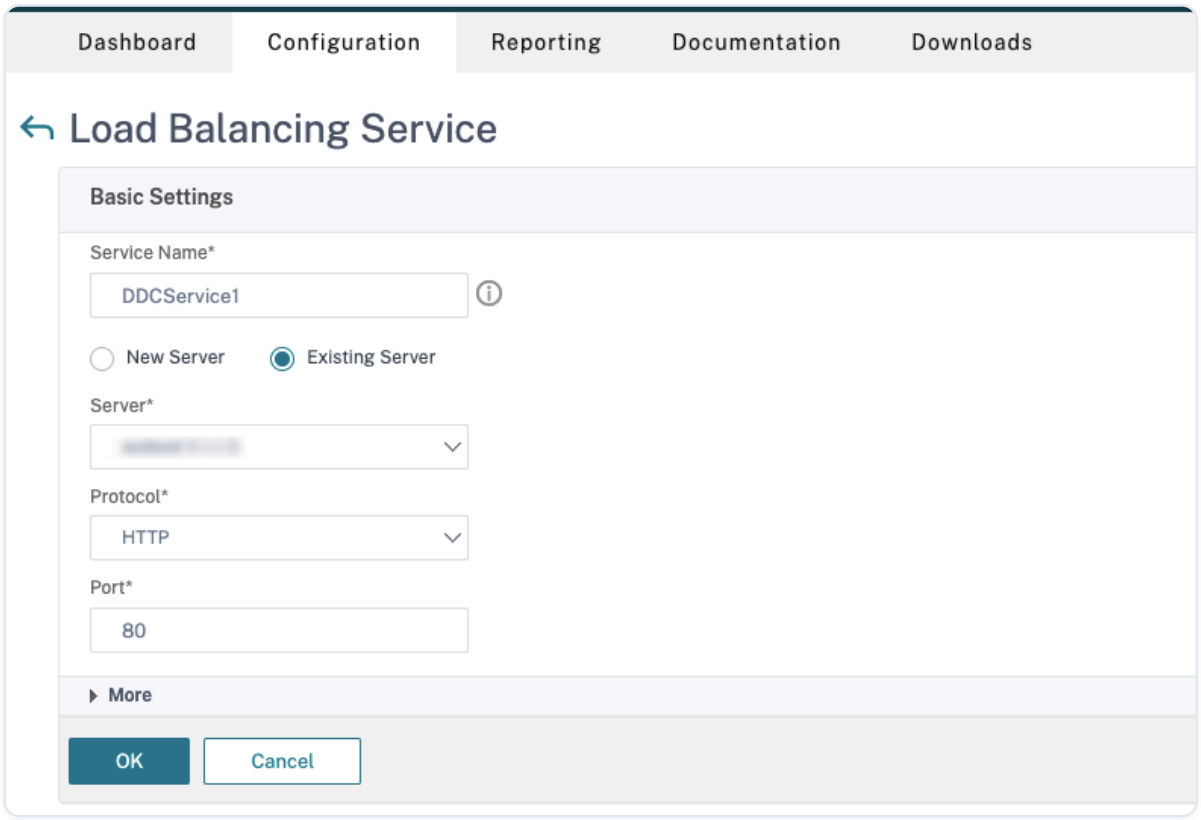
      - Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**.
      - Na página **Servidores Virtuais**, clique em **Adicionar**.



- Em **Protocolo**, selecione **HTTP**.
- Adicione o endereço IP virtual de balanceamento de carga e em **Porta** selecione **80**.
- Clique em **OK**.

b. Crie um serviço de balanceamento de carga.

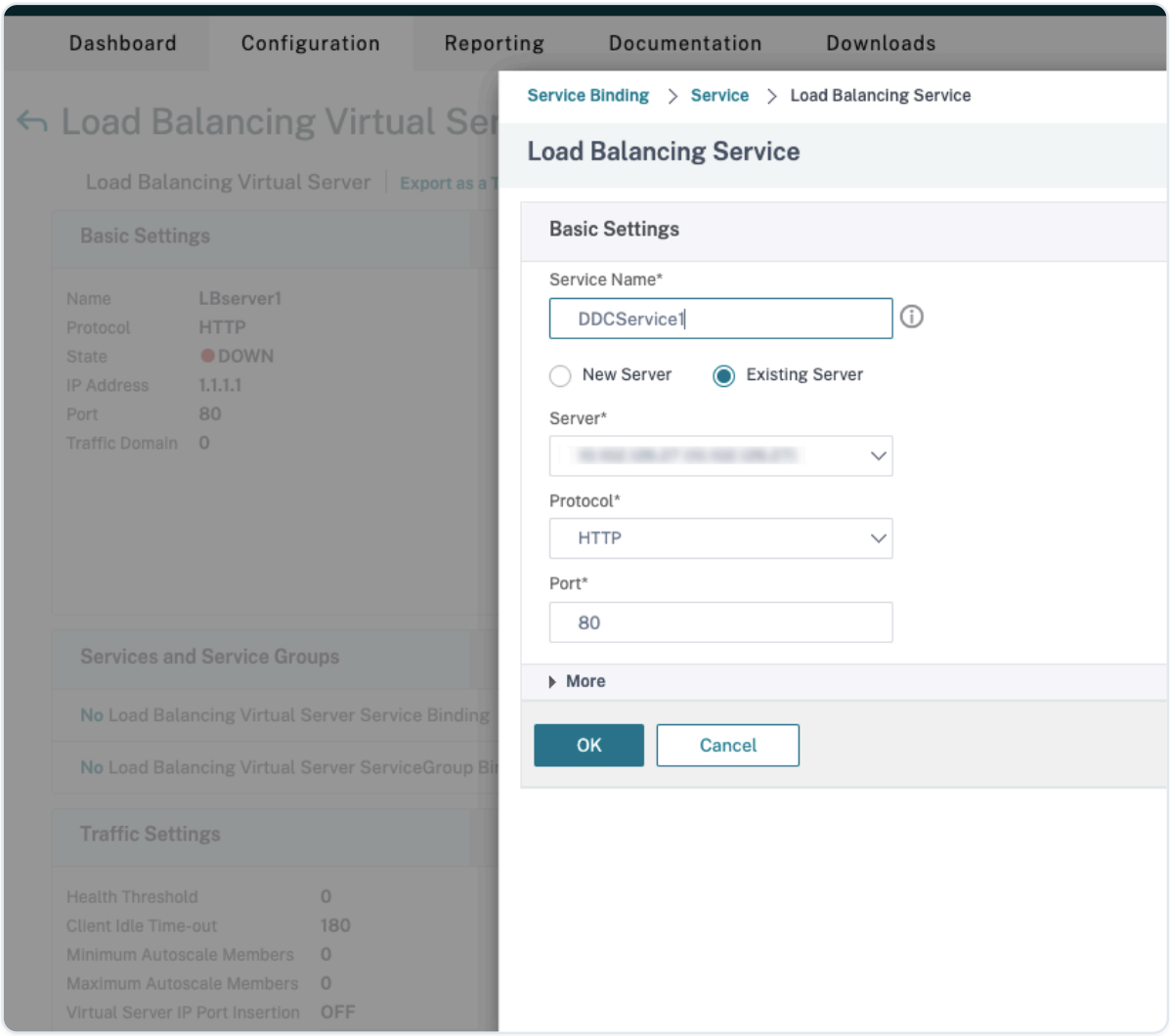
- Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Serviços**.



- Em **Servidor Existente**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocolo**, selecione **HTTP** e em **Porta** selecione **80**.
- Clique em **OK** e, em seguida, clique em **Concluído**.

c. Vincule o serviço ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Serviços e Grupos de Serviço**, clique em **Nenhuma Vinculação de Serviço de Servidor Virtual de Balanceamento de Carga**.

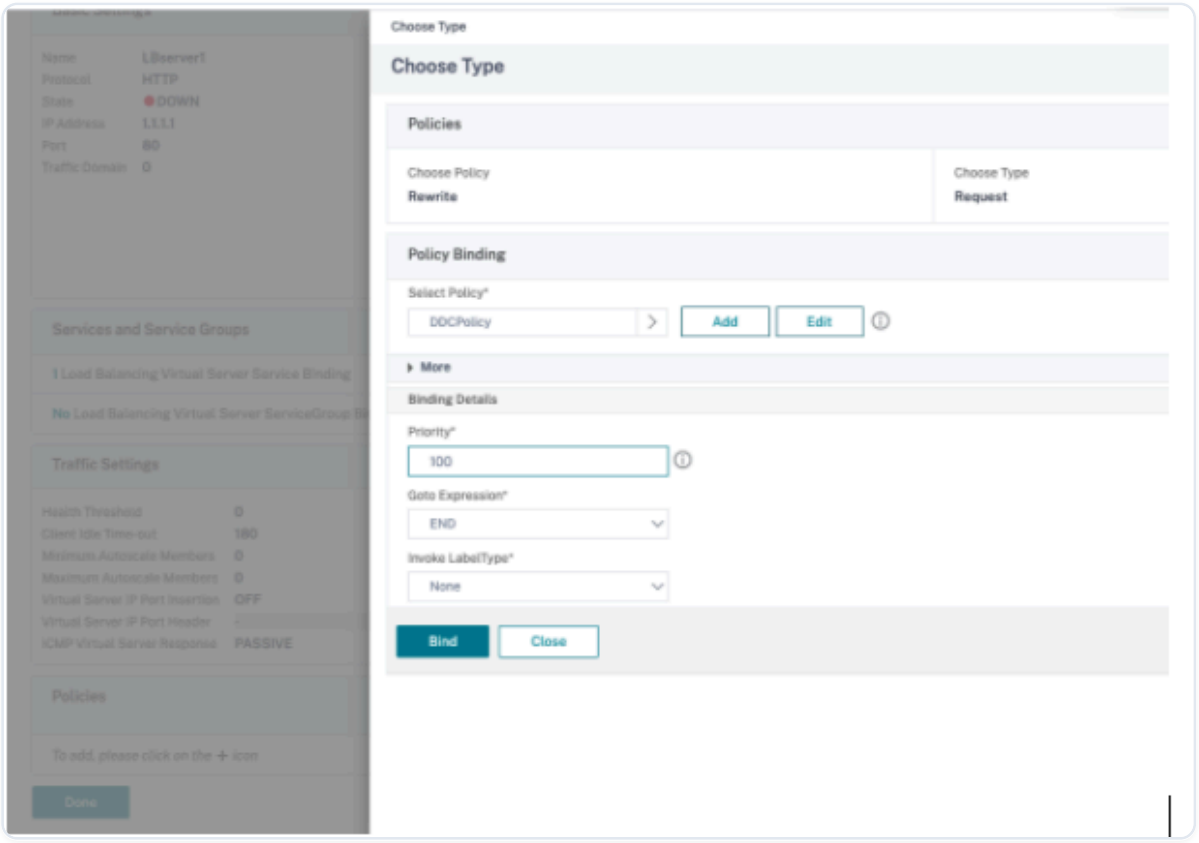


- Em **Associação de Serviço**, selecione o serviço criado anteriormente.
- Clique em **Vincular**.

d. Vincule a política de reescrita criada anteriormente ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.

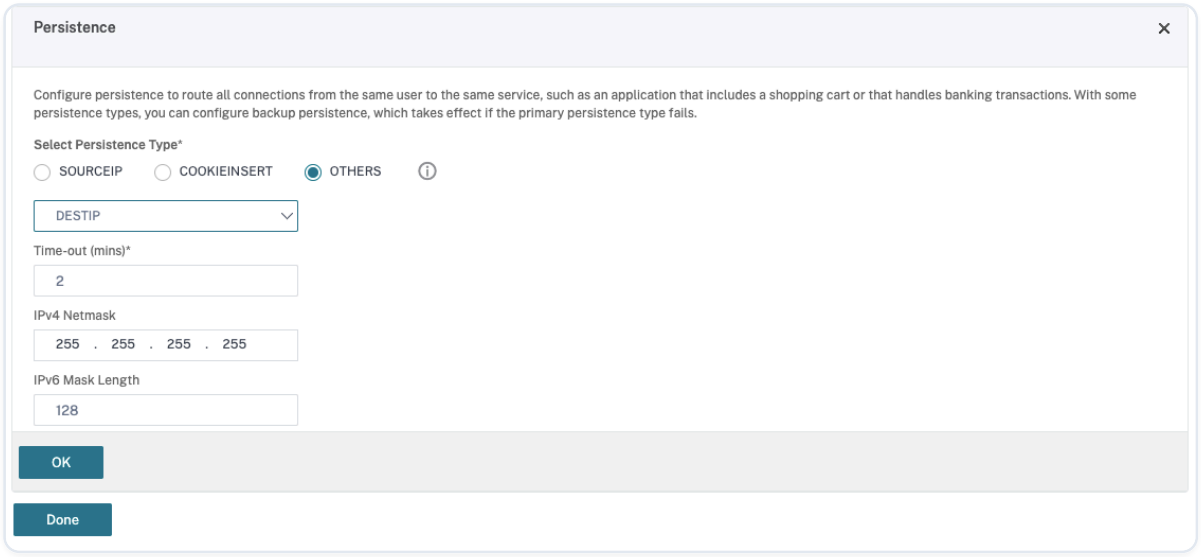
- Em **Configurações Avançadas**, clique em **Políticas,** e, em seguida, na seção **Políticas**, clique em **+**.



- Em **Escolher Política**, selecione **Reescrever** e em **Escolher Tipo**, selecione **Solicitação**.
- Clique em **Continuar**.
- Em **Selecionar Política**, selecione a política de reescrita criada anteriormente.
- Clique em **Vincular**.
- Clique em **Concluído**.

e. Configure a persistência para o servidor virtual, se necessário.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Configurações Avançadas**, clique em **Persistência**.



- Selecione o tipo de persistência como **Outros**.
- Selecione **DESTIP** para criar sessões de persistência com base no endereço IP do serviço selecionado pelo servidor virtual (o endereço IP de destino)
- Em **Máscara de Rede IPv4**, adicione a máscara de rede igual à do DDC.
- Clique em **OK**.

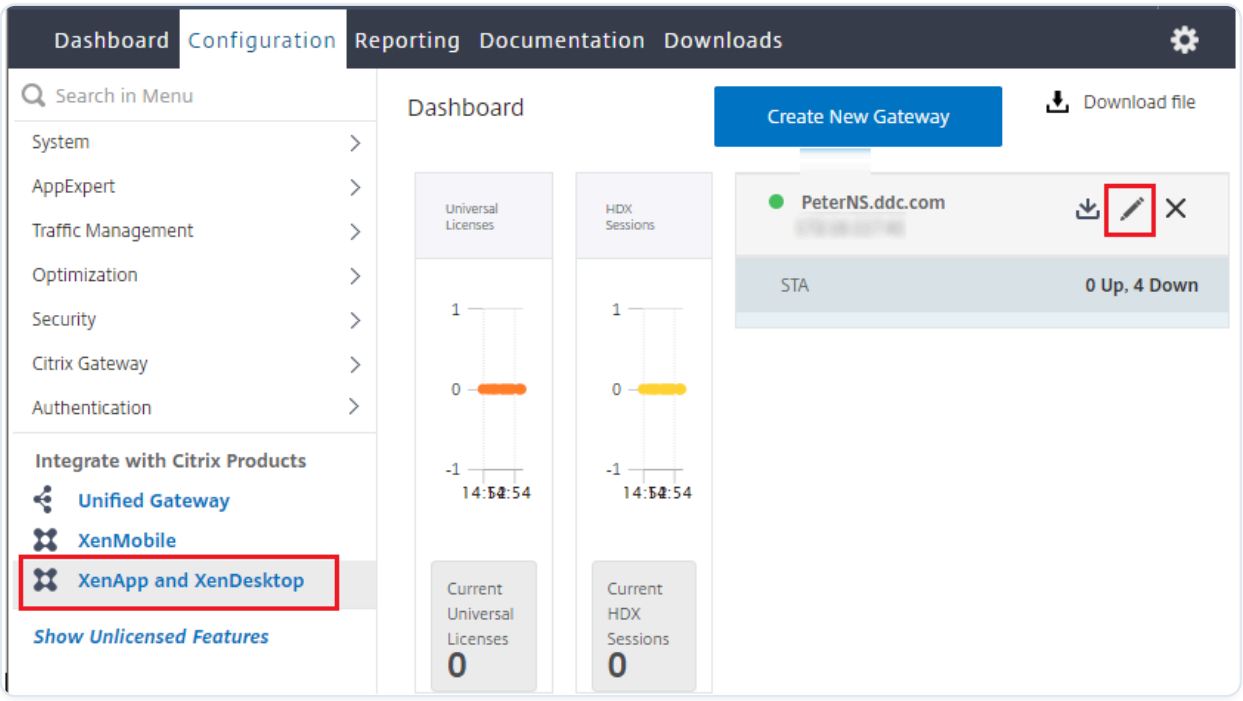
f. Repita estas etapas para o outro servidor virtual também.

Alterações de configuração se o dispositivo Citrix ADC já estiver configurado com o Citrix Virtual Desktops™

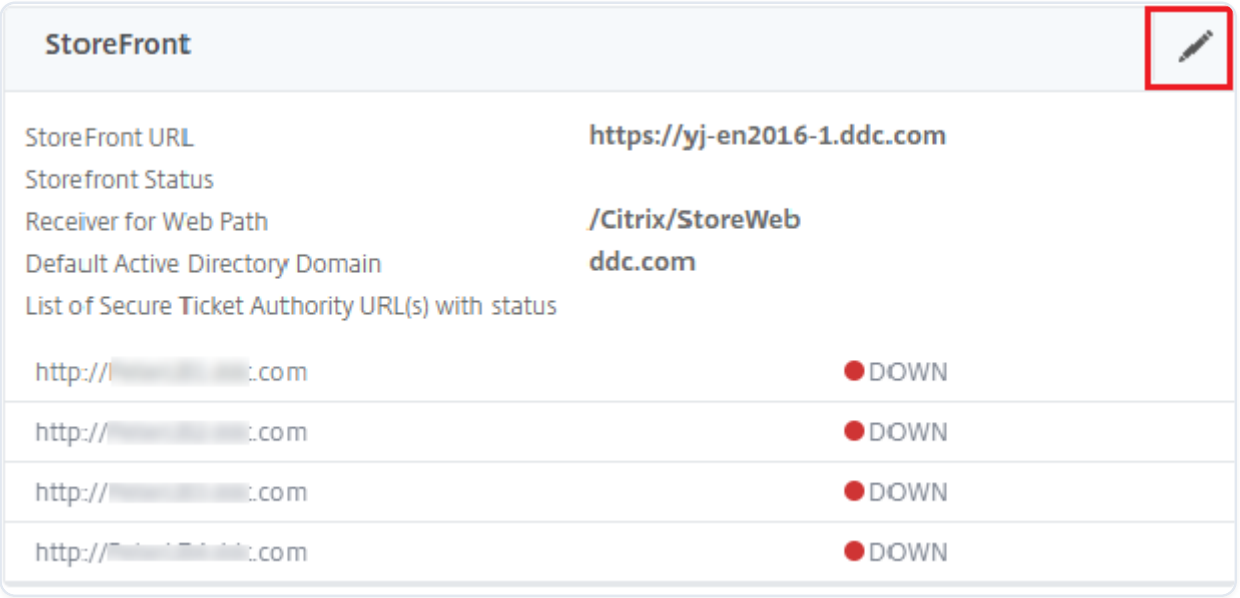
Se você já configurou o dispositivo Citrix ADC com o Citrix Virtual Desktops, para usar o recurso XML Seguro, você deve fazer as seguintes alterações de configuração.

- Antes do lançamento da sessão, altere a **URL da Autoridade de Ticket de Segurança** do gateway para usar os FQDNs dos servidores virtuais de balanceamento de carga.
- Certifique-se de que o parâmetro `TrustRequestsSentToTheXmlServicePort` esteja definido como False. Por padrão, o parâmetro `TrustRequestsSentToTheXmlServicePort` é definido como False. No entanto, se o cliente já configurou o Citrix ADC para o Citrix Virtual Desktops, então o `TrustRequestsSentToTheXmlServicePort` é definido como True.

1. Na GUI do Citrix ADC, vá para **Configuração > Integrar com Produtos Citrix** e clique em **XenApp and XenDesktop®**.
2. Selecione a instância do gateway e clique no ícone de edição.

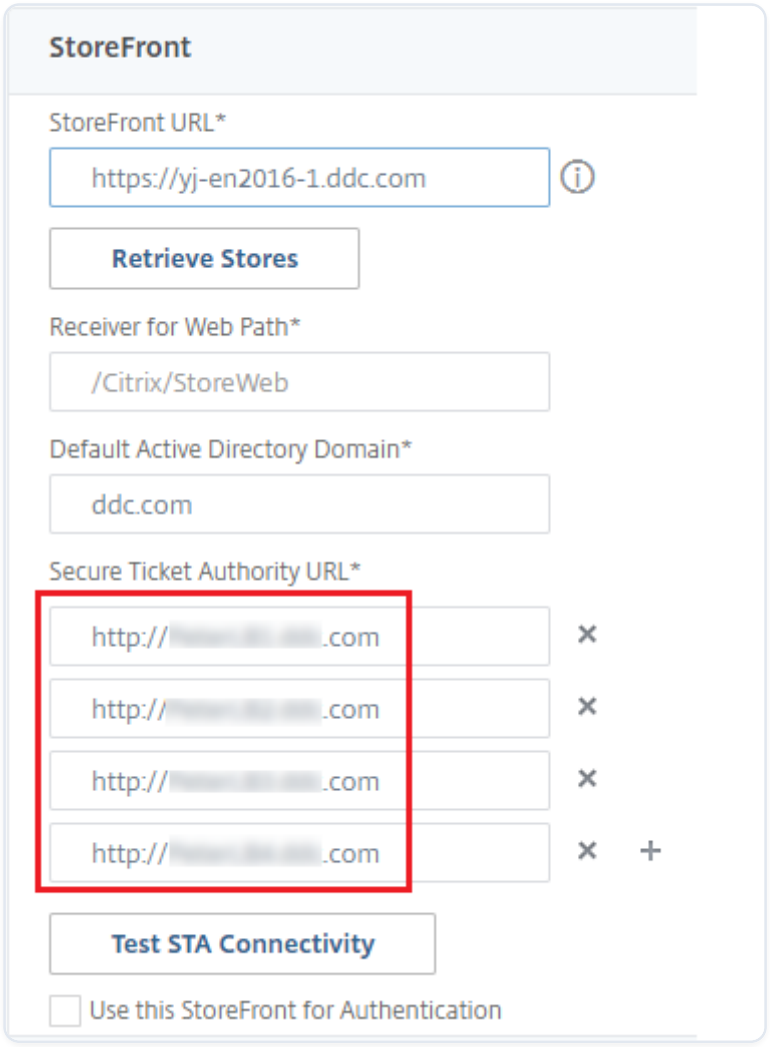


3. No painel StoreFront, clique no ícone de edição.



4. Adicione a **URL da Secure Ticket Authority**.

   - Se o recurso Secure XML estiver ativado, a URL do STA deve ser a URL do serviço de balanceamento de carga.
   - Se o recurso XML Seguro estiver desabilitado, a URL do STA deve ser a URL do STA (endereço do DDC) e o parâmetro `TrustRequestsSentToTheXmlServicePort` no DDC deve ser definido como True.



Configurações de resiliência da sessão

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência ao usuário. Perder a conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode levar à frustração do usuário. Mover-se rapidamente entre dispositivos e acessar os mesmos aplicativos a cada logon é uma prioridade para muitos trabalhadores móveis, como profissionais de saúde.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões, reduzem inconvenientes, tempo de inatividade e perda de produtividade; usando esses recursos, os usuários móveis podem se deslocar de forma rápida e fácil entre os dispositivos.

Confiabilidade da sessão

A Confiabilidade da Sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Este recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel ferroviário e perde momentaneamente a conectividade. Normalmente, a sessão é desconectada e desaparece da tela do usuário, e o usuário precisa se reconectar à sessão desconectada. Com a Confiabilidade da Sessão, a sessão permanece ativa na máquina. Para indicar a perda de conectividade, a tela do usuário congela e o cursor muda para uma ampulheta giratória até que a conectividade seja retomada do outro lado do túnel. O usuário continua a acessar a tela durante a interrupção e pode retomar a interação com o aplicativo quando a conexão de rede for restaurada. A Confiabilidade da Sessão reconecta os usuários sem solicitações de reautenticação.

Os usuários do aplicativo Citrix Workspace™ não podem substituir a configuração do Controller.

Você pode usar a Confiabilidade da Sessão com o Transport Layer Security (TLS). O TLS criptografa apenas os dados enviados entre o dispositivo do usuário e o Citrix Gateway.

Habilite e configure a Confiabilidade da Sessão com as seguintes configurações de política:

- A configuração de política de conexões de confiabilidade da sessão permite ou impede a confiabilidade da sessão.
- A configuração de política de tempo limite de confiabilidade da sessão tem um padrão de 180 segundos, ou três minutos. Embora você possa estender o tempo que a confiabilidade da sessão mantém uma sessão aberta, esse recurso foi projetado para a conveniência do usuário. Portanto, ele não solicita reautenticação ao usuário. À medida que você estende o tempo em que uma sessão é mantida aberta, aumentam as chances de um usuário se distrair e se afastar do dispositivo do usuário. Essas ações podem potencialmente deixar a sessão acessível a usuários não autorizados.
- As conexões de confiabilidade de sessão de entrada usam a porta 2598, a menos que você altere o número da porta na configuração de política de número da porta de confiabilidade da sessão.
- Para evitar que os usuários se reconectem a sessões interrompidas sem precisar se reautenticar, use o recurso Auto Client Reconnect. Você pode configurar a configuração de política de autenticação do Auto Client Reconnect para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usar a Confiabilidade da Sessão e o Auto Client Reconnect, os dois recursos funcionarão em sequência. A Confiabilidade da Sessão fecha, ou desconecta, a sessão do usuário após o tempo especificado na configuração de política de tempo limite de confiabilidade da sessão. Depois disso, as configurações de política do Auto Client Reconnect entram em vigor, tentando reconectar o usuário à sessão desconectada.

Auto Client Reconnect

Com o recurso Auto Client Reconnect, o aplicativo Citrix Workspace pode detectar desconexões não intencionais de sessões ICA® e reconectar os usuários às sessões afetadas automaticamente. Quando esse recurso está ativado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Para sessões de aplicativo, o aplicativo Citrix Workspace tenta se reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de desktop, o aplicativo Citrix Workspace tenta se reconectar à sessão por um 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 a seguinte configuração de registro no dispositivo do usuário (onde `seconds` é o número de segundos após o qual nenhuma outra tentativa é feita para reconectar a sessão).

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

Habilite e configure o Auto Client Reconnect com as seguintes configurações de política:

- **Auto Client Reconnect:** Habilita ou desabilita a reconexão automática pelo aplicativo Citrix Workspace após uma conexão ter sido interrompida.
- **Autenticação de Auto Client Reconnect:** Habilita ou desabilita a exigência de autenticação do usuário após a reconexão automática.
- **Registro de Auto Client Reconnect:** Habilita ou desabilita o registro de eventos de reconexão no log de eventos. O registro é desabilitado por padrão. Quando ativado, o log do sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Cada servidor armazena informações sobre eventos de reconexão em seu próprio log do sistema. O site não fornece um log combinado de eventos de reconexão para todos os servidores.

> **Observação:**
>
> O Auto Client Reconnect sem reautenticação é suportado apenas para autenticação por senha. Se você usar o Federated Authentication Service ou a autenticação por cartão inteligente, o Auto Client Reconnect sem reautenticação não será suportado. Nesses casos, os usuários são redirecionados para a tela de login.

> O Auto Client Reconnect incorpora um mecanismo de autenticação baseado em credenciais de usuário criptografadas. Quando um usuário faz login inicialmente, o servidor criptografa e armazena as credenciais do usuário na memória. O servidor também cria e envia um cookie contendo a chave de criptografia para o aplicativo Citrix Workspace. O aplicativo Citrix Workspace envia a chave para o servidor para reconexão. O servidor descriptografa as credenciais e as envia para o logon do Windows para autenticação. Quando os cookies expiram, os usuários devem se reautenticar para se reconectar às sessões.

Os cookies não são usados se você habilitar a configuração de autenticação do Auto Client Reconnect. Em vez disso, os usuários são apresentados a uma caixa de diálogo solicitando credenciais quando o aplicativo Citrix Workspace tenta se reconectar automaticamente.

Para proteção máxima das credenciais e sessões do usuário, use criptografia para toda a comunicação entre os clientes e o site.

Desative o Auto Client Reconnect no aplicativo Citrix Workspace para Windows usando o arquivo icaclient.adm. Para obter mais informações, consulte a documentação da sua versão do aplicativo Citrix Workspace para Windows.

As configurações para conexões também afetam o Auto Client Reconnect:

- Por padrão, o Auto Client Reconnect é habilitado por meio de configurações de política no nível do site, conforme descrito anteriormente. A reautenticação do usuário não é necessária. No entanto, se a conexão ICA TCP de um servidor estiver configurada para redefinir sessões com um link de comunicação interrompido, a reconexão automática não ocorrerá. O Auto Client Reconnect funciona apenas se o servidor desconectar as sessões quando houver uma conexão interrompida ou com tempo limite. Nesse contexto, a conexão ICA TCP refere-se a uma 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 configurada para desconectar sessões com conexões interrompidas ou com tempo limite. As sessões desconectadas permanecem intactas na memória do sistema e estão disponíveis para reconexão pelo aplicativo Citrix Workspace.
- A conexão pode ser configurada para redefinir ou desconectar sessões com conexões quebradas ou expiradas. Quando uma sessão é redefinida, tentar reconectar inicia uma nova sessão. Em vez de restaurar um usuário para o mesmo ponto no aplicativo em uso, o aplicativo é reiniciado.

- Se o servidor estiver configurado para redefinir sessões, o Auto Client Reconnect criará uma nova 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 muito tempo se passou desde que detectou a conexão quebrada.

ICA Keep-Alive

A ativação do recurso ICA Keep-Alive impede que conexões quebradas sejam desconectadas. Quando ativado, se o servidor não detectar atividade, esse recurso impede que os Serviços de Área de Trabalho Remota desconectem essa sessão. Exemplos de nenhuma atividade incluem nenhuma alteração de relógio, nenhum movimento do mouse, nenhuma atualização de tela. O servidor envia pacotes keep-alive a cada poucos segundos para detectar se a sessão está ativa. Se a sessão não estiver mais ativa, o servidor a marca como desconectada.

> **Importante:**
>
> O ICA Keep-Alive funciona apenas se você não estiver usando a Confiabilidade da Sessão. A Confiabilidade da Sessão tem seus próprios mecanismos para evitar que conexões quebradas sejam desconectadas. Configure o ICA Keep-Alive apenas para conexões que não usam a Confiabilidade da Sessão.

> As configurações do ICA Keep-Alive substituem as configurações de keep-alive configuradas na Política de Grupo do Windows.

Habilite e configure o ICA Keep-Alive com as seguintes configurações de política:

- **Tempo limite de keep-alive do ICA:** Especifica o intervalo (1-3600 segundos) usado para enviar mensagens keep-alive do ICA. Não configure esta opção se você quiser que seu software de monitoramento de rede feche conexões inativas em ambientes onde as conexões quebradas são tão infrequentes que permitir que os usuários se reconectem às sessões não é uma preocupação.

  O intervalo padrão é de 60 segundos: os pacotes ICA Keep-Alive são enviados para os dispositivos do usuário a cada 60 segundos. Se um dispositivo de usuário não responder em 60 segundos, o status das sessões ICA muda para desconectado.
- **Keep-alives do ICA:** Envia ou impede o envio de mensagens keep-alive do ICA.

Controle de workspace

O controle de workspace permite que desktops e aplicativos sigam um usuário de um dispositivo para outro. Essa capacidade de roaming permite que um usuário acesse todos os desktops ou aplicativos abertos de qualquer lugar simplesmente fazendo logon, sem ter que reiniciar os desktops ou aplicativos em cada dispositivo. Por exemplo, o controle de workspace pode ajudar profissionais de saúde em um hospital que precisam se mover rapidamente entre diferentes estações de trabalho e acessar o mesmo conjunto de aplicativos cada vez que fazem logon. Se você configurar as opções de controle de workspace para permitir, esses trabalhadores podem se desconectar de vários aplicativos em um dispositivo cliente e, em seguida, reconectar-se para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle de workspace afeta as seguintes atividades:

- **Fazer logon:** Por padrão, o controle de workspace permite que os usuários se reconectem automaticamente a todos os desktops e aplicativos em execução ao fazer logon, ignorando a necessidade de reabri-los manualmente. Através do controle de workspace, os usuários podem abrir desktops ou aplicativos desconectados, além de quaisquer que estejam ativos em outro dispositivo cliente. Desconectar-se de um desktop ou aplicativo o deixa em execução no servidor. Se você tiver usuários em roaming que devem manter alguns desktops ou aplicativos em execução em um dispositivo cliente enquanto se reconectam a um subconjunto de seus desktops ou aplicativos em outro dispositivo cliente, você pode configurar o comportamento de reconexão de logon para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Reconectando:** Após fazer logon no servidor, os usuários podem se reconectar a todos os seus desktops ou aplicativos a qualquer momento clicando em Reconectar. Por padrão, Reconectar abre desktops ou aplicativos que estão desconectados, além de quaisquer outros que estejam sendo executados atualmente em outro dispositivo cliente. Você pode configurar o Reconectar para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Fazendo logoff:** Para usuários que abrem desktops ou aplicativos através do StoreFront™, você pode configurar o comando **Log Off** para desconectar o usuário do StoreFront e de todas as sessões ativas, ou apenas do StoreFront.
- **Desconectando:** Os usuários podem se desconectar de todos os desktops e aplicativos em execução de uma só vez, sem precisar se desconectar de cada um individualmente.

O controle de espaço de trabalho está disponível apenas para usuários do aplicativo Citrix Workspace que acessam desktops e aplicativos por meio de uma conexão Citrix StoreFront. Por padrão, o controle de espaço de trabalho é desabilitado para sessões de desktop virtual, mas é

habilitado para aplicativos hospedados. O compartilhamento de sessão não ocorre por padrão entre desktops publicados e quaisquer aplicativos publicados em execução dentro desses desktops.

As políticas de usuário, mapeamentos de unidade cliente e configurações de impressora mudam apropriadamente quando um usuário se move para um novo dispositivo cliente. As políticas e mapeamentos são aplicados de acordo com o dispositivo cliente onde o usuário está conectado à sessão. Por exemplo, um profissional de saúde faz logoff de um dispositivo na sala de emergência e, em seguida, faz logon em uma estação de trabalho no laboratório de raios-X. As políticas, mapeamentos de impressora e mapeamentos de unidade cliente apropriados para a sessão no laboratório de raios-X entram em vigor no início da sessão.

Você pode personalizar quais impressoras aparecem para os usuários quando eles mudam de local. Você também pode controlar se os usuários podem imprimir em impressoras locais, quanta largura de banda é consumida quando os usuários se conectam remotamente e outros aspectos de suas experiências de impressão.

Para obter informações sobre como habilitar e configurar o controle de espaço de trabalho para usuários, consulte a documentação do StoreFront.

Roaming de sessão

> **Observação:**
>
> As informações a seguir o guiam para configurar o roaming de sessão usando o PowerShell. Você pode usar o Web Studio em vez disso. Para obter mais informações, consulte Gerenciar grupos de entrega.
>
> Por padrão, as sessões fazem roaming entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos estão disponíveis em ambos os dispositivos. Os aplicativos seguem, independentemente do dispositivo ou se existem sessões atuais. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem.

Embora esse comportamento padrão ofereça muitas vantagens, ele pode não ser ideal em todos os casos. Você pode impedir o roaming de sessão usando o SDK do PowerShell.

Exemplo 1: Um profissional de saúde está usando dois dispositivos, preenchendo um formulário de seguro em um PC desktop e consultando informações do paciente em um tablet.

- Se o roaming de sessão estiver habilitado, ambos os aplicativos aparecem em ambos os dispositivos (um aplicativo iniciado em um dispositivo é visível em todos os dispositivos em uso). Isso pode não atender aos requisitos de segurança.
- Se o roaming de sessão estiver desabilitado, o registro do paciente não aparece no PC desktop, e o formulário de seguro não aparece no tablet.

Exemplo 2: Um gerente de produção inicia um aplicativo no PC em seu escritório. O nome e a localização do dispositivo determinam quais impressoras e outros recursos estão disponíveis para essa sessão. Mais tarde no dia, ele vai a um escritório no prédio ao lado para uma reunião que exigirá o uso de uma impressora.

- Quando o roaming de sessão está ativado, o gerente de produção provavelmente não conseguiria acessar as impressoras perto da sala de reunião, porque os aplicativos que ele iniciou anteriormente em seu escritório resultaram na atribuição de impressoras e outros recursos perto daquele local.
- Quando o roaming de sessão está desativado, ao fazer login em uma máquina diferente (usando as mesmas credenciais), uma nova sessão é iniciada, e impressoras e recursos próximos estarão disponíveis.

Configurar o roaming de sessão

Para configurar o roaming de sessão, use os seguintes cmdlets de regra de política de direito com a propriedade "SessionReconnection". Opcionalmente, você também pode especificar a propriedade "LeasingBehavior".

Para sessões de desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões de aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Always:** As sessões sempre fazem roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.

- **DisconnectedOnly:** Reconectar apenas a sessões que já estão desconectadas; caso contrário, iniciar uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente, primeiro desconectando-as ou usando o Workspace Control para fazer o roaming explicitamente.) Uma sessão ativa conectada 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 apenas ao mesmo dispositivo que foi usado anteriormente na sessão.

A propriedade "LeasingBehavior" é descrita abaixo.

Efeitos de outras configurações:

A desativação do roaming de sessão é afetada pelo limite de aplicativo **Permitir apenas uma instância do aplicativo por usuário** nas propriedades do aplicativo no grupo de entrega.

- Se você desativar o roaming de sessão, desative o limite de aplicativo "Permitir apenas uma instância ...".
- Se você ativar o limite de aplicativo "Permitir apenas uma instância ...", não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos.

Intervalo de logon

Se uma máquina virtual contendo um VDA de desktop fechar antes que o processo de logon seja concluído, você pode alocar mais tempo para o processo. O padrão para as versões 7.6 e posteriores é de 180 segundos (o padrão para 7.0-7.5 é de 90 segundos).

Na máquina (ou na imagem mestre usada em um catálogo de máquinas), defina a seguinte chave de registro:

Chave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique um tempo decimal em segundos, no intervalo de 0 a 3600.

Se você alterar uma imagem mestre, atualize o catálogo.

Essa configuração se aplica apenas a VMs com VDAs de desktop. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor.

Configurações

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado em Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Você pode usar o Web Studio para gerenciar estas configurações:

- Gerenciar Autenticação
- Programa de Melhoria da Experiência do Cliente Citrix
- Remover Delivery Controllers
- Alterar o banco de dados de log
- Definir data e hora
- Centralizar o gerenciamento do site
- Habilitar atribuição automática de vários usuários para Acesso Remoto a PC
- Habilitar resolução de DNS
- Habilitar confiança XML
- Gerenciar chave de segurança
- Definir o tempo limite de inatividade para o console do Studio

Gerenciar autenticação

Por padrão, os usuários fazem logon no Web Studio usando seu nome de usuário e senha de domínio. Você também pode escolher um método de autenticação diferente para os usuários, como a autenticação por cartão inteligente ou a autenticação integrada do Windows.

Para escolher um método de autenticação para usuários, siga estas etapas:

1. Faça login no Web Studio e selecione Configurações no painel esquerdo.
2. Localize o bloco Autenticação e clique em Editar para selecionar uma opção:
    - Credenciais de domínio

- Credenciais de domínio ou autenticação integrada do Windows

  Com a autenticação integrada do Windows ativada, os usuários podem acessar o Web Studio usando suas credenciais do Windows (Kerberos/NTLM) ou um certificado de cliente.

  Quando o Web Studio e o Delivery Controller™ são instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, ative Permitir acesso entre origens e adicione o URL do servidor Web Studio à lista de permissões.

  > **Importante**
  >
  > A autenticação integrada do Windows não funciona quando o Web Studio está configurado como um proxy para Delivery Controllers.

- Autenticação por cartão inteligente.
- Credenciais de domínio ou autenticação por cartão inteligente

  A ativação da autenticação por cartão inteligente requer configuração adicional. Para obter mais informações, consulte Configurar a autenticação por cartão inteligente para o Web Studio.

Depois de ativar a opção **Autenticação integrada do Windows**, na próxima vez que seus usuários fizerem logon, eles serão conectados automaticamente. Se, como usuário, você não conseguir fazer login automaticamente, siga estas etapas para configurar seu navegador da web para permitir a autenticação integrada do Windows.

Para o Google Chrome:

1. No Painel de Controle, selecione Opções da Internet.
2. Selecione a guia **Avançado**.
3. Selecione **Habilitar Autenticação Integrada do Windows**.
4. Selecione a guia **Segurança**.
5. Selecione **Intranet Local > Sites > Avançado**.
6. Na caixa **Adicionar este site à zona**:

   - Se o Web Studio e o Delivery Controller residirem no mesmo servidor, digite o URL do host que executa o Web Studio.

- Caso contrário, digite um domínio curinga. Exemplo: se o Delivery Controller estiver em `ddc.domain.com`, digite `*.domain.com`.

7. Clique em **Adicionar > Fechar**

Para Mozilla Firefox:

1. No navegador, digite `about:config` na caixa de URL.
2. Na caixa **Pesquisar**, digite `network negotiate`.
3. Clique com o botão direito em **network.negotiate-auth.trusted-uris** e selecione **Modificar**.
4. Na caixa **Inserir valor da string**:

   - Se o Web Studio e o Delivery Controller residirem no mesmo servidor, adicione uma lista de URLs e/ou aliases separados por vírgulas, fazendo referência ao nome do servidor que hospeda o Web Studio.
   - Caso contrário, adicione os URLs desta forma. Exemplo: se o Delivery Controller estiver em `ddc.domain.com`, digite `*.domain.com`.

Depois de configurar seu navegador, você pode clicar em **Logon integrado do Windows** na página de logon para tentar novamente.

Quando o Web Studio e o Delivery Controller são instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, você precisa habilitar **Permitir acesso entre origens**.

Siga estas etapas para habilitar **Permitir acesso entre origens**:

1. Selecione a caixa de seleção **Permitir acesso entre origens**.
2. Adicione a URL do servidor Web Studio à lista de permissões.
3. No campo **Inserir URL**, insira a URL. Clique em **Adicionar** para adicionar mais, se necessário.

> **Observação**
>
> - A URL deve seguir o formato correto: `<scheme>://<hostname>`. Certifique-se de que ela não inclua nenhum caminho ou barra final.
> - Endereços IP e FQDNs são suportados. Ao adicionar uma URL, certifique-se de que ela corresponda à forma como você acessa o Web Studio. Por exemplo, se estiver

> acessando o Web Studio usando um endereço IP, adicione a URL baseada em endereço IP à lista.
> - Se você usar uma porta não padrão, certifique-se de incluir o número da porta.

4. Clique em **Adicionar** para adicionar mais, se necessário.
5. Depois de terminar, clique em **Concluído** para salvar e sair.

Configurar o fuso horário

Para personalizar o formato de data e hora para atender às suas preferências, siga estas etapas:

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Localize o bloco **Data e hora** e clique em **Editar** para configurar as seguintes opções:
   - **Formato da hora:**
     - Selecione para exibir a hora usando um relógio de 12 horas (09:00 pm, por exemplo) ou um relógio de 24 horas (21:00, por exemplo).
   - **Formato da data:**
     - Configure o formato da data para corresponder às suas preferências, como aaaa/MM/dd.
   - **Fuso horário:**
     - **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 essas informações no seu fuso horário local.
     - **Fuso horário local:** Exibe 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 essas informações em UTC.

> **Observação:**
>
> Essas configurações são específicas para cada conta de usuário.

Habilitar resolução de DNS

Para apresentar nomes DNS em vez de endereços IP no arquivo ICA®, siga estas etapas:

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Ative a configuração **Habilitar resolução de DNS**.

Definir o tempo limite de inatividade para o console do Studio

Você pode definir a duração da inatividade após a qual os administradores são automaticamente desconectados do console do Studio.

1. Faça login no Web Studio e selecione **Configurações** no painel esquerdo.
2. Digite uma duração que varia de 10 minutos a 24 horas.
3. Para aplicar esta configuração, atualize a página ou saia e entre novamente.

Centralizar o gerenciamento de sites

Este recurso permite que você use um console do Web Studio para gerenciar vários sites do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Habilitar o gerenciamento de vários sites.

Tags

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Tags são strings que identificam itens como máquinas, aplicativos, desktops, grupos de entrega, grupos de aplicativos e políticas. Depois de criar uma tag e adicioná-la a um item, você pode adaptar certas operações para que se apliquem apenas a itens que possuem uma tag especificada.

- Personalizar exibições de pesquisa no Web Studio.

  Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma tag chamada "test" e adicione-a (aplique-a) a esses aplicativos. Agora você pode filtrar a pesquisa do Web Studio com a tag "test".

- Publicar aplicativos de um grupo de aplicativos ou desktops específicos de um grupo de entrega, considerando apenas um subconjunto das máquinas nos grupos de entrega selecionados. Isso é chamado de *restrição de tag*.

  Com as restrições de tag, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de mais máquinas. Uma restrição de tag pode ser pensada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Sua funcionalidade é semelhante, mas não idêntica, aos grupos de trabalho em versões do XenApp anteriores a 7.x.

  Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.
- Agendar reinícios periódicos para um subconjunto de máquinas em um grupo de entrega.

  Usar uma restrição de tag para máquinas permite que você use novos cmdlets do PowerShell para configurar vários agendamentos de reinício para subconjuntos de máquinas em um grupo de entrega. Para exemplos e detalhes, consulte Gerenciar grupos de entrega.
- Adaptar a aplicação (atribuição) de políticas Citrix a um subconjunto de máquinas em grupos de entrega, tipos de grupo de entrega ou UOs que possuem (ou não possuem) uma tag especificada.

  Por exemplo, se você quiser aplicar uma política Citrix apenas às estações de trabalho mais potentes, adicione uma tag chamada "high power" a essas máquinas. Em seguida, na página **Atribuir Política** do assistente Criar Política, selecione essa tag e a caixa de seleção **Habilitar**. Você também pode adicionar uma tag a um grupo de entrega e, em seguida, aplicar uma política Citrix a esse grupo. Para obter detalhes, consulte Criar políticas.

Você pode aplicar tags a:

- Máquinas
- Aplicativos
- Catálogos de máquinas (somente PowerShell; consulte Tags em catálogos de máquinas)
- Grupos de entrega
- Grupos de aplicativos

Uma restrição de tag pode ser configurada ao criar ou editar o seguinte no Web Studio:

- Um desktop em um grupo de entrega compartilhado
- Um grupo de aplicativos

Importante:

Uma tag pode ser aplicada explicitamente a uma máquina ou pode ser aplicada explicitamente no nível do catálogo de máquinas ou do grupo de entrega. Quando uma tag é aplicada no nível do catálogo de máquinas ou do grupo de entrega, todas as máquinas dentro desse catálogo ou grupo de entrega herdam implicitamente a tag. Essas tags herdadas não podem ser removidas no nível da máquina. Para remover o efeito da tag, a tag deve ser removida do nível do catálogo de máquinas ou do grupo de entrega.

Restrições de tag para um desktop ou um grupo de aplicativos

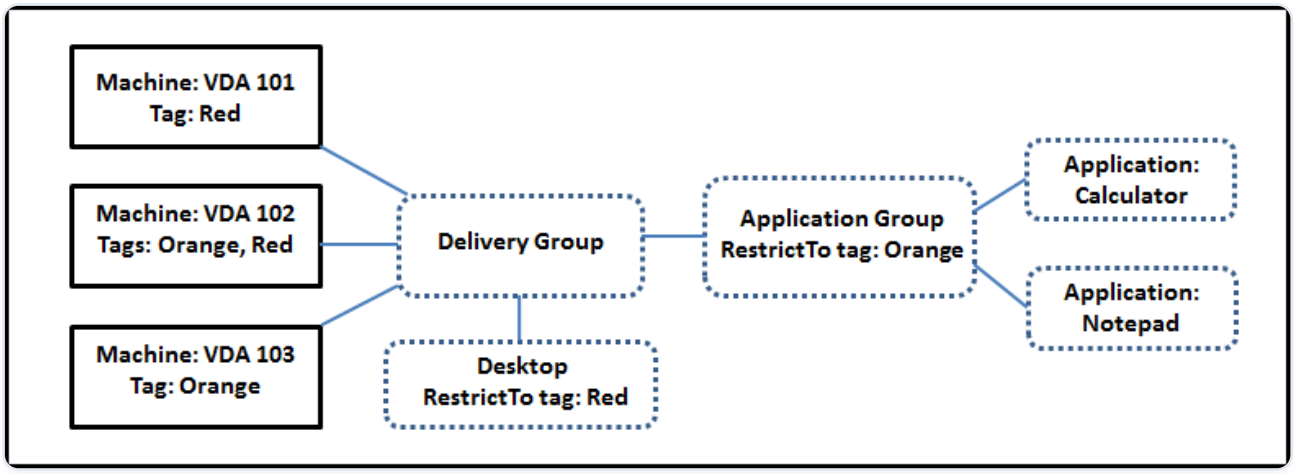
Uma restrição de tag envolve várias etapas:

- Crie a tag e, em seguida, adicione-a (aplique-a) às máquinas.
- Crie ou edite um grupo com a restrição de tag (em outras palavras, "restringir inicializações a máquinas com a tag x").

Uma restrição de tag estende o processo de seleção de máquina do broker. O broker seleciona uma máquina de um grupo de entrega associado, sujeito à política de acesso, listas de usuários configuradas, preferência de zona e prontidão de inicialização, além da restrição de tag (se presente). Para aplicativos, o broker recorre a outros grupos de entrega em ordem de prioridade, aplicando as mesmas regras de seleção de máquina para cada grupo de entrega considerado.

Exemplo 1: Layout simples

Este exemplo apresenta um layout simples que usa restrições de tag para limitar quais máquinas são consideradas para determinados lançamentos de desktop e aplicativos. O site possui um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.



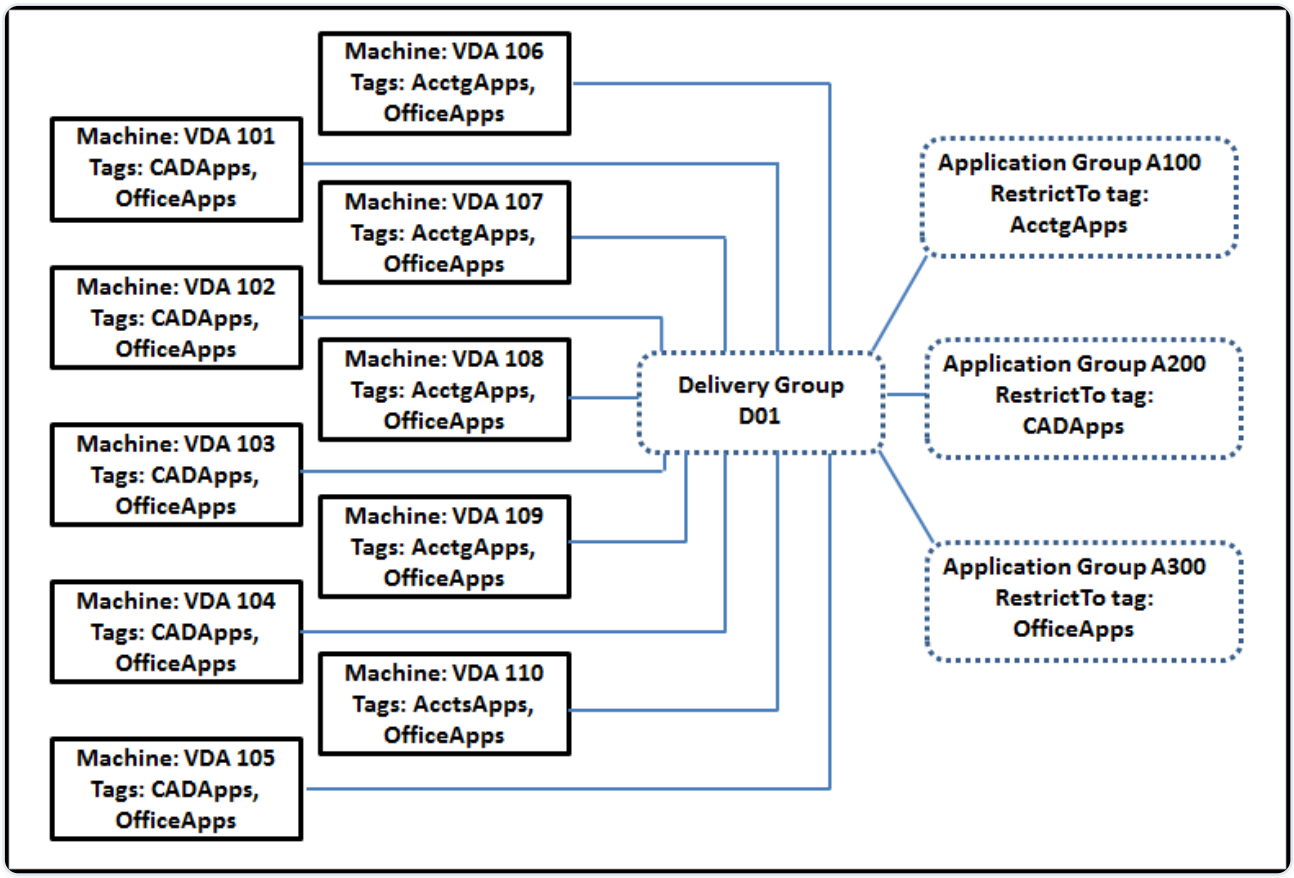
- Tags foram adicionadas a cada uma das três máquinas (VDA 101–103).
- O desktop no grupo de entrega compartilhado foi criado com uma restrição de tag chamada "Red". Um desktop pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Red": VDA 101 e 102.
- O grupo de aplicativos foi criado com a restrição de tag "Orange", então cada um de seus aplicativos (Calculadora e Bloco de Notas) pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Orange": VDA 102 e 103.

A máquina VDA 102 possui ambas as tags (Red e Orange), então pode ser considerada para o lançamento dos aplicativos e do desktop.

Exemplo 2: Layout mais complexo

Este exemplo contém vários grupos de aplicativos que foram criados com restrições de tag. Isso resulta na capacidade de entregar mais aplicativos com menos máquinas do que seria necessário se você usasse apenas grupos de entrega.

Como configurar o exemplo 2 mostra as etapas usadas para criar e aplicar as tags e, em seguida, configurar as restrições de tag neste exemplo.



Este exemplo usa 10 máquinas (VDA 101–110), um grupo de entrega (D01) e três grupos de aplicativos (A100, A200, A300). Ao aplicar tags a cada máquina e, em seguida, especificar restrições de tag ao criar cada grupo de aplicativos:

- Usuários de contabilidade no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 101–105)
- Designers de CAD no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 106-110)
- Usuários no grupo que precisam de aplicativos do Office podem acessar os aplicativos do Office em 10 máquinas (VDA 101–110)

Apenas 10 máquinas são usadas, com apenas um grupo de entrega. Usar apenas grupos de entrega (sem grupos de aplicativos) exigiria o dobro de máquinas, porque uma máquina pode pertencer a apenas um grupo de entrega.

Gerenciar tags e restrições de tag

As tags são criadas, adicionadas (aplicadas), editadas e excluídas de itens selecionados por meio da ação **Gerenciar Tags** no Web Studio.

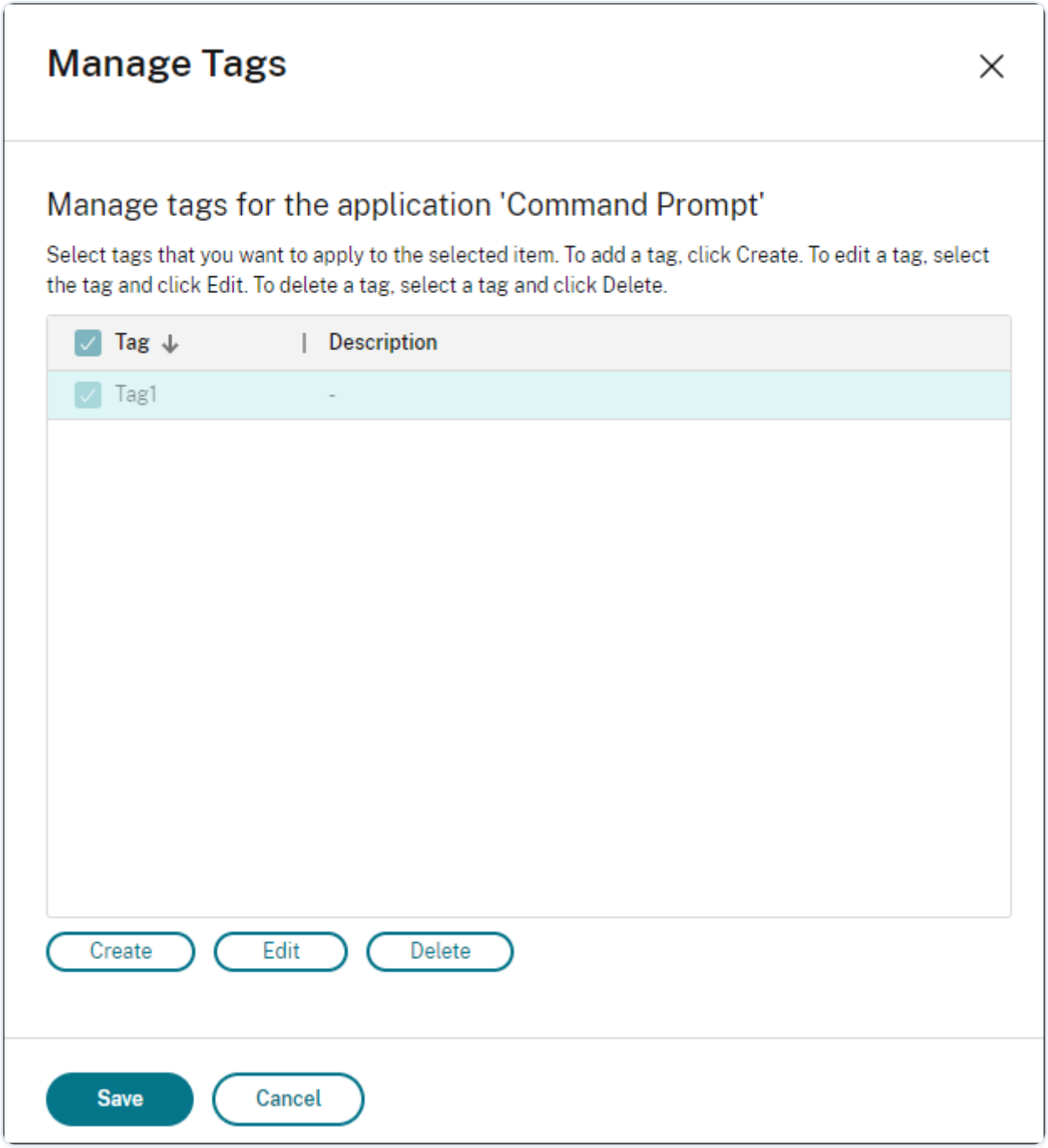
(Exceção: As tags usadas para atribuições de política são criadas, editadas e excluídas por meio da ação **Gerenciar Tags** no Web Studio. No entanto, as tags são aplicadas (atribuídas) quando você cria a política. Consulte Criar políticas para obter detalhes.)

As restrições de tag são configuradas ao criar ou editar desktops em grupos de entrega e ao criar e editar grupos de aplicativos.

Usar as caixas de diálogo Gerenciar Tags no Web Studio

No Web Studio, selecione os itens aos quais você deseja aplicar uma tag (uma ou mais máquinas, aplicativos, um desktop, um grupo de entrega ou um grupo de aplicativos) e, em seguida, selecione **Gerenciar Tags** na barra de ações. A caixa de diálogo lista todas as tags que foram criadas no Site, não apenas para os itens selecionados.

- Uma caixa de seleção contendo uma marca de seleção indica que a tag já foi adicionada aos itens selecionados. (Na captura de tela abaixo, a máquina selecionada tem a tag chamada "Tag1" aplicada.)
- Se você selecionou mais de um item, uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados, têm essa tag adicionada.



As seguintes ações estão disponíveis na caixa de diálogo **Gerenciar Tags**. Certifique-se de revisar Precauções ao trabalhar com tags.

- **Para criar uma tag:**

  Clique em **Criar.** Insira um nome e uma descrição. Os nomes das tags devem ser exclusivos e não diferenciam maiúsculas de minúsculas. Em seguida, clique em **OK**. (A criação de uma tag não a aplica automaticamente a nenhum item selecionado. Use as caixas de seleção para aplicar a tag.)

- **Para adicionar (aplicar) uma ou mais tags:**

Marque a caixa de seleção ao lado do nome da tag. Se você selecionou vários itens e a caixa de seleção ao lado de uma tag contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a tag aplicada), alterá-la para uma marca de seleção afeta todas as máquinas selecionadas.

Se você tentar adicionar uma tag a uma ou mais máquinas, e essa tag estiver sendo usada como uma restrição em um grupo de aplicativos, você será avisado de que a ação pode resultar em tornar essas máquinas disponíveis para inicialização. Se for isso que você pretendia, prossiga.

- **Para remover uma ou mais tags:**

  Desmarque a caixa de seleção ao lado do nome da tag. Se você selecionou vários itens e a caixa de seleção ao lado de uma tag contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a tag aplicada), desmarcar a caixa de seleção remove a tag de todas as máquinas selecionadas.

  Se você tentar remover uma tag de uma máquina que está usando essa tag como uma restrição, você será avisado de que a ação pode afetar quais máquinas são consideradas para inicialização. Se for isso que você pretendia, prossiga.

- **Para editar uma tag:**

  Selecione uma tag e clique em **Editar**. Insira um novo nome, descrição ou ambos. Você pode editar apenas uma tag por vez.

- **Para excluir uma ou mais tags:**

  Selecione as tags e clique em **Excluir**. A caixa de diálogo Excluir Tag indica quantos itens usam as tags selecionadas atualmente (por exemplo, "2 máquinas"). Clique em um item para exibir mais informações. Por exemplo, clicar em um item "2 máquinas" exibe os nomes das duas máquinas que têm essa tag aplicada. Confirme se deseja excluir as tags.

  Você não pode usar o Web Studio para excluir uma tag que é usada como restrição. Primeiro, edite o grupo de aplicativos e remova a restrição da tag ou selecione uma tag diferente.

Quando terminar na caixa de diálogo **Gerenciar Tags**, clique em **Salvar**.

Para ver se uma máquina tem alguma tag aplicada: Selecione **Grupos de Entrega** no painel esquerdo. Selecione um grupo de entrega no painel central e, em seguida, selecione **Exibir Máquinas** na barra de ações. Selecione uma máquina no painel central e, em seguida, selecione a guia **Tags** no painel **Detalhes**.

Gerenciar restrições de tag

Configurar uma restrição de tag é um processo de várias etapas: Primeiro, você cria a tag e a adiciona/aplica às máquinas. Em seguida, você adiciona a restrição ao grupo de aplicativos ou à área de trabalho.

- **Criar e aplicar a tag:**

  Crie a tag e, em seguida, adicione (aplique)-a às máquinas afetadas pela restrição de tag, usando as ações de **Gerenciar Tags** descritas anteriormente.

- **Para adicionar uma restrição de tag a um grupo de aplicativos:**

  Crie ou edite o grupo de aplicativos. Na página **Grupos de Entrega**, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista.

- **Para alterar ou remover a restrição de tag em um grupo de aplicativos:**

  Edite o grupo. Na página **Grupos de Entrega**, selecione uma tag diferente da lista ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

- **Para adicionar uma restrição de tag a uma área de trabalho:**

  Crie ou edite um grupo de entrega. Clique em **Adicionar** ou **Editar** na página **Áreas de Trabalho**. Na caixa de diálogo Adicionar Área de Trabalho, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag no menu.

- **Para alterar ou remover a restrição de tag em um grupo de entrega:**

  Edite o grupo. Na página Áreas de Trabalho, clique em **Editar**. Na caixa de diálogo, selecione uma tag diferente das listas ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

Precauções ao trabalhar com tags

Uma tag aplicada a um item pode ser usada para diferentes propósitos, então tenha em mente que adicionar, remover e excluir uma tag pode ter efeitos não intencionais. Você pode usar uma tag para classificar exibições de máquinas no campo de pesquisa do Web Studio. Você pode usar a mesma tag como uma restrição ao configurar um grupo de aplicativos ou um desktop. A tag limita a consideração de inicialização apenas às máquinas em grupos de entrega especificados que possuem essa tag.

Ao tentar adicionar uma tag a máquinas depois que essa tag foi configurada como uma restrição de tag para um desktop ou um grupo de aplicativos, um aviso aparece. Adicionar essa tag pode tornar as máquinas disponíveis para iniciar aplicativos ou desktops adicionais. Se era isso que você pretendia, prossiga. Caso contrário, você pode cancelar a operação.

Por exemplo, digamos que você crie um grupo de aplicativos com a restrição de tag "Vermelho". Mais tarde, você adiciona várias outras máquinas nos mesmos grupos de entrega usados por esse grupo de aplicativos. Se você tentar adicionar a tag "Vermelho" a essas máquinas, o Web Studio exibirá uma mensagem semelhante a: "A tag "Vermelho" é usada como restrição nos seguintes grupos de aplicativos. Adicionar esta tag pode tornar as máquinas selecionadas disponíveis para iniciar aplicativos neste grupo de aplicativos." Você pode então confirmar ou cancelar a adição dessa tag a essas máquinas adicionais.

Da mesma forma, se um grupo de aplicativos usa uma tag para restringir inicializações, o Web Studio avisa que você não pode excluir a tag até editar o grupo para removê-la como uma restrição. (Se você tivesse permissão para excluir uma tag que é usada como restrição em um grupo de aplicativos, isso poderia resultar em permitir que os aplicativos fossem iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição de exclusão de uma tag se aplica se a tag estiver sendo usada como restrição para inicializações de desktop. Depois de editar o grupo de aplicativos ou os desktops no grupo de entrega para remover essa restrição de tag, você pode excluir a tag.

Nem todas as máquinas podem ter os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada um com uma restrição de tag diferente e conjuntos de máquinas diferentes ou sobrepostos de grupos de entrega. A tabela a seguir lista como as considerações da máquina são decididas.

QUANDO UM APLICATIVO FOI ADICIONADO A	ESTAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO
Um grupo de aplicativos sem restrição de tag	Qualquer máquina.
Um grupo de aplicativos com restrição de tag A	Máquinas que têm a tag A aplicada.
Dois grupos de aplicativos, um com restrição de tag A e o outro com restrição de tag B	Máquinas que têm a tag A e a tag B. Se nenhuma estiver disponível, então máquinas que têm a tag A ou a tag B.

QUANDO UM APLICATIVO FOI ADICIONADO A	ESTAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO
Dois grupos de aplicativos, um com restrição de tag A e o outro sem restrição de tag	Máquinas que têm a tag A. Se nenhuma estiver disponível, então qualquer máquina.

Se você usou uma restrição de tag em um agendamento de reinicialização de máquina, quaisquer alterações que você fizer que afetem as aplicações ou restrições de tag afetarão o próximo ciclo de reinicialização da máquina. Isso não afeta nenhum ciclo de reinicialização que esteja em andamento enquanto as alterações estão sendo feitas.

Como configurar o exemplo 2

A sequência a seguir mostra as etapas para criar e aplicar tags e, em seguida, configurar restrições de tag para os grupos de aplicativos ilustrados no segundo exemplo.

VDAs e aplicativos já foram instalados nas máquinas e o grupo de entrega foi criado.

Crie e aplique tags às máquinas:

1. No Web Studio, selecione o grupo de entrega D01 e, em seguida, selecione **Exibir Máquinas** na barra de ações.
2. Selecione as máquinas VDA 101–105 e, em seguida, selecione **Gerenciar Tags** na barra de ações.
3. Na caixa de diálogo Gerenciar Tags, clique em **Criar** e, em seguida, crie uma tag chamada `CADApps`. Clique em **OK**.
4. Clique em **Criar** novamente e crie uma tag chamada OfficeApps. Clique em **OK**.
5. Ainda na caixa de diálogo **Gerenciar Tags**, adicione (aplique) as tags recém-criadas às máquinas selecionadas, marcando as caixas de seleção ao lado do nome de cada tag (`CADApps` e `OfficeApps`). Quando terminar, feche a caixa de diálogo.
6. Selecione o grupo de entrega D01, selecione **Exibir Máquinas** na barra de ações.
7. Selecione as máquinas VDA 106–110 e, em seguida, selecione **Gerenciar Tags** na barra de ações.
8. Na caixa de diálogo **Gerenciar Tags**, clique em **Criar**. Crie uma tag chamada `AcctgApps`. Clique em **OK**.

9. Aplique a tag `AcctgApps` recém-criada e a tag `OfficeApps` às máquinas selecionadas, clicando nas caixas de seleção ao lado do nome de cada tag e, em seguida, feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de tag.

1. No Web Studio, selecione **Aplicativos** no painel esquerdo, selecione a guia **Grupos de Aplicativos** e, em seguida, selecione **Criar Grupo de Aplicativos** na barra de ações. O assistente Criar Grupo de Aplicativos é iniciado.
2. Na página **Grupos de Entrega** do assistente, selecione o grupo de entrega D01. Selecione **Restringir inicializações a máquinas com tag** e, em seguida, selecione a tag `AcctgApps` na lista.
3. Conclua o assistente, especificando os usuários de contabilidade e os aplicativos de contabilidade. (Ao adicionar o aplicativo, escolha a origem **Do menu Iniciar**, que pesquisa o aplicativo nas máquinas que têm a tag `AcctgApps`.) Na página **Resumo**, nomeie o grupo `A100`.
4. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando as máquinas que têm a tag `CADApps`, além dos usuários e aplicativos apropriados.
5. Repita as etapas para criar o grupo de aplicativos `A300`, especificando as máquinas que têm a tag `OfficeApps`, além dos usuários e aplicativos apropriados.

Tags em catálogos de máquinas

Você pode usar tags em catálogos de máquinas. A sequência geral de criação de uma tag e sua aplicação a um catálogo é a mesma descrita anteriormente. No entanto, a aplicação de tags a catálogos é suportada apenas por meio da interface PowerShell. Você não pode usar o Web Studio para aplicar uma tag a um catálogo ou remover uma tag de um catálogo. As exibições de catálogo no Web Studio não indicam se uma tag foi aplicada.

Resumo: Você pode usar o Web Studio ou o PowerShell para criar ou excluir uma tag para uso em um catálogo. Use o PowerShell para aplicar a tag ao catálogo.

Aqui estão alguns exemplos de uso de tags com catálogos:

- Um grupo de entrega tem máquinas de vários catálogos, mas você deseja que uma operação (como um agendamento de reinicialização) afete apenas as máquinas em um catálogo específico. A aplicação de uma tag a esse catálogo consegue isso.
- Em um grupo de aplicativos, você deseja limitar as sessões de aplicativos a máquinas em um catálogo específico. A aplicação de uma tag a esse catálogo consegue isso.

Cmdlets PowerShell afetados:

- Você pode passar objetos de catálogo para cmdlets como `Add-BrokerTag` e `Remove-BrokerTag`.
- `Get-BrokerTagUsage` mostra quantos catálogos contêm tags.
- `Get-BrokerCatalog` tem uma propriedade chamada `Tags`.

Por exemplo, os seguintes cmdlets adicionam uma tag chamada `fy2018` ao catálogo chamado `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (A tag foi criada anteriormente usando o Web Studio ou o PowerShell.)

Consulte a ajuda do cmdlet PowerShell para obter mais orientação e sintaxe.

Tags automáticas (Pré-visualização)

A marcação automática permite que os administradores definam e removam tags em vários objetos do Citrix Virtual Apps and Desktops automaticamente, com base em regras personalizadas. Esse aprimoramento elimina a necessidade de manter diferentes scripts que são executados periodicamente para otimização do ambiente.

Casos de uso

Com a marcação automática, você pode implementar regras relevantes para os seus impulsionadores de negócios, como redução de custos, otimização da infraestrutura e impulsionamento do consumo. A seguir 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 para o pool disponível.
- **Remover desordem de aplicativos** - Para reduzir a desordem de aplicativos identificando os aplicativos que não foram usados por mais de um número pré-configurado de dias.
- **DGs com nível funcional inferior a X** - Para encontrar grupos de entrega com um nível funcional inferior a um específico.
- **Usuários inativos** - Para recuperar recursos de usuários que não fizeram logon por mais de um número pré-configurado de dias.

Comandos PowerShell

Você pode criar autotags usando comandos PowerShell. Depois que uma regra de autotag é criada, ela é avaliada com uma frequência de 600 segundos. Para obter mais informações, consulte New-BrokerAutoTagRule.

Exemplos

`New-BrokerAutoTagRule` usa o mesmo tipo de objeto e parâmetros de filtro que o cmdlet `Get-BrokerMachine`. Para obter mais informações, consulte GetBrokerMachine.

1. Marcar VDIs dedicados que não foram usados por mais de 30 dias com o ID 123:
    a. Defina uma tag para marcar os VDIs não utilizados com, 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 para a regra.
        - Tipo de objeto : Máquina.
        - Texto da regra : Máquinas estáticas e atribuídas cujo último tempo de conexão é > 30 dias ou nenhum valor.
        - ID da Tag : O ID da tag que você deseja 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 nível funcional inferior a X (usando **L7_20** como o nível funcional limite):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup' -RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid 123
```

1. 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: Como atribuir desktops a servidores específicos.

Perfis de usuário

Por padrão, o Citrix Profile Management é instalado silenciosamente em imagens mestre quando você instala o Virtual Delivery Agent, mas você não precisa usar o Profile Management como uma solução de perfil.

Para atender às diversas necessidades dos seus usuários, você pode usar as políticas do Citrix Virtual Apps and Desktops™ para aplicar diferentes comportamentos de perfil às máquinas em cada Grupo de Entrega. Por exemplo, um Grupo de Entrega pode exigir perfis obrigatórios do Citrix, cujo modelo é armazenado em um local de rede, enquanto outro Grupo de Entrega exige perfis móveis do Citrix armazenados em outro local com várias pastas redirecionadas.

- Se outros administradores em sua organização forem responsáveis pelas políticas do Citrix Virtual Apps and Desktops, trabalhe com eles para garantir que eles definam quaisquer políticas relacionadas a perfis em seus Grupos de Entrega.
- As políticas do Profile Management também podem ser definidas na Política de Grupo, no arquivo .ini do Profile Management e localmente em máquinas virtuais individuais. Essas múltiplas formas de definir o comportamento do perfil são lidas na seguinte ordem:

  a. Política de Grupo (arquivos .adm ou .admx)
  b. Políticas do Citrix Virtual Apps and Desktops no nó de Política
  c. Políticas locais na máquina virtual à qual o usuário se conecta
  d. Arquivo .ini do Profile Management

  Por exemplo, se você configurar a mesma política tanto na Política de Grupo quanto no nó de Política, o sistema lê a configuração da política na Política de Grupo e ignora a configuração da política do Citrix Virtual Apps and Desktops.

Qualquer que seja a solução de perfil que você escolher, os administradores do Director podem acessar informações de diagnóstico e solucionar problemas de perfis de usuário. Para obter mais informações, consulte a documentação do Director.

Configuração automática

O tipo de desktop é detectado automaticamente, com base na instalação do Virtual Delivery Agent e, além das escolhas de configuração que você faz no Studio, define os padrões do Profile Management de acordo.

As políticas que o Profile Management ajusta são mostradas na tabela a seguir. Quaisquer configurações de política não padrão são preservadas e não são sobrescritas por este recurso.

Consulte a documentação do Profile Management para obter informações sobre cada política. Os tipos de máquinas que criam perfis afetam as políticas que são ajustadas. Os fatores primários são se as máquinas são persistentes ou provisionadas, e se são compartilhadas por vários usuários ou dedicadas a apenas um usuário.

Sistemas persistentes possuem algum tipo de armazenamento local, cujo conteúdo pode ser esperado para persistir quando o sistema é desligado. Sistemas persistentes podem empregar tecnologia de armazenamento como SANs para fornecer uma emulação de disco local. Em contraste, sistemas provisionados são criados "em tempo real" a partir de um disco base e algum tipo de disco de identidade. O armazenamento local é geralmente emulado por um disco RAM ou disco de rede, sendo este último frequentemente fornecido por uma SAN com um link de alta velocidade. A tecnologia de provisionamento é geralmente Citrix Provisioning ou Machine Creation Services™ (ou um equivalente de terceiros). Às vezes, sistemas provisionados possuem armazenamento local persistente. Estes são classificados como persistentes.

Juntos, esses dois fatores definem os seguintes tipos de máquina:

- **Ambos persistentes e dedicados**. Exemplos são máquinas de SO de sessão única com uma atribuição estática e armazenamento local persistente que são criadas com Machine Creation Services, estações de trabalho físicas e laptops.
- **Ambos persistentes e compartilhados**. Exemplos são máquinas de SO de múltiplas sessões que são criadas com Machine Creation Services e servidores Citrix Virtual Apps.
- **Ambos provisionados e dedicados**. Exemplos são máquinas de SO de sessão única com uma atribuição estática, mas sem armazenamento persistente, que são criadas com Citrix Provisioning Service (no Citrix Virtual Desktops™).
- **Ambos provisionados e compartilhados**. Exemplos são máquinas de SO de sessão única com uma atribuição aleatória que são criadas com Citrix Provisioning™ Service (no Citrix Virtual Desktops) e servidores Citrix Virtual Apps.

As seguintes configurações de política do Profile Management são diretrizes sugeridas para os diferentes tipos de máquina. Elas funcionam bem na maioria dos casos, mas você pode querer se desviar delas conforme sua implantação exigir.

> **Importante:**
>
> **Excluir perfis armazenados em cache localmente no logoff**, **Streaming de perfil** e **Sempre armazenar em cache** são impostos pelo recurso de configuração automática. Ajuste as outras políticas manualmente.

Máquinas persistentes

POLÍTICA	AMBOS PERSISTENTES E DEDICADOS	AMBOS PERSISTENTES E COMPARTILHADOS
Excluir perfis armazenados em cache localmente no logoff	Desabilitado	Ativado
Streaming de perfil	Desabilitado	Ativado
Sempre armazenar em cache	Ativado (nota 1)	Desativado (nota 2)
Gravação ativa	Desabilitado	Desativado (nota 3)
Processar logons de administradores locais	Ativado	Desativado (nota 4)

Máquinas provisionadas

POLÍTICA	AMBOS PROVISIONADOS E DEDICADOS	AMBOS PROVISIONADOS E COMPARTILHADOS
Excluir perfis armazenados em cache localmente no logoff	Desativado (nota 5)	Ativado
Streaming de perfil	Ativado	Ativado
Sempre armazenar em cache	Desativado (nota 6)	Desabilitado
Gravação ativa	Ativado	Ativado
Processar logons de administradores locais	Ativado	Ativado (nota 7)

1. Como o **Streaming de perfil** está desativado para este tipo de máquina, a configuração **Sempre armazenar em cache** é sempre ignorada.
2. Desative **Sempre armazenar em cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, ativando esta política e

usando-a para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo deste tamanho ou maior é armazenado em cache localmente o mais rápido possível.

3. Desative **Gravação ativa**, exceto para salvar alterações em perfis de usuários que fazem roaming entre servidores Citrix Virtual Apps. Nesse caso, ative esta política.
4. Desative **Processar logons de administradores locais**, exceto para Desktops Compartilhados Hospedados. Nesse caso, ative esta política.
5. Desative **Excluir perfis armazenados em cache localmente no logoff**. Essa configuração retém perfis armazenados em cache localmente. Como as máquinas são redefinidas no logoff, mas são atribuídas a usuários individuais, os logons são mais rápidos se seus perfis estiverem em cache.
6. Desative **Sempre armazenar em cache**. No entanto, você pode garantir que arquivos grandes sejam carregados nos perfis o mais rápido possível após o logon, ativando esta política e usando-a para definir um limite de tamanho de arquivo (em MB). Qualquer arquivo deste tamanho ou maior é armazenado em cache localmente o mais rápido possível.
7. Ative **Processar logons de administradores locais**, exceto para perfis de usuários que fazem roaming entre servidores Citrix Virtual Apps and Desktops. Nesse caso, desative esta política.

Redirecionamento de pasta

O redirecionamento de pasta permite armazenar dados do usuário em compartilhamentos de rede diferentes do local onde os perfis são armazenados. O redirecionamento de pasta reduz o tamanho do perfil e o tempo de carregamento, mas pode afetar a largura de banda da rede. O redirecionamento de pasta não exige que os perfis de usuário do Citrix sejam empregados. Você pode optar por gerenciar perfis de usuário por conta própria e ainda redirecionar pastas.

Configure o redirecionamento de pasta usando políticas Citrix no Studio.

- Certifique-se de que os locais de rede usados para armazenar o conteúdo das pastas redirecionadas estejam disponíveis e tenham as permissões corretas. As propriedades do local são validadas.
- As pastas redirecionadas são configuradas na rede e seu conteúdo é preenchido a partir dos desktops virtuais dos usuários no logon.

Configure o redirecionamento de pasta usando apenas Políticas Citrix ou Objetos de Política de Grupo do Active Directory, não ambos. Configurar o redirecionamento de pasta usando ambos os mecanismos de política pode resultar em comportamento imprevisível.

Redirecionamento avançado de pasta

Em implantações com vários sistemas operacionais (SOs), você pode querer que parte do perfil de um usuário seja compartilhada por cada SO. O restante do perfil não é compartilhado e é usado apenas por um SO. Para garantir uma experiência de usuário consistente entre os SOs, você precisa de uma configuração diferente para cada SO, ou seja, redirecionamento avançado de pasta. Por exemplo, diferentes versões de um aplicativo em execução em dois SOs podem precisar ler ou editar um arquivo compartilhado, então você decide redirecioná-lo para um único local de rede onde ambas as versões possam acessá-lo. Alternativamente, como o conteúdo da pasta **Menu Iniciar** é estruturado de forma diferente em dois SOs, você decide redirecionar apenas uma pasta, não ambas. Essa abordagem separa a pasta **Menu Iniciar** e seu conteúdo em cada SO, garantindo uma experiência consistente para os usuários.

Se sua implantação requer redirecionamento avançado de pastas, você deve entender a estrutura dos dados de perfil de seus usuários e determinar quais partes podem ser compartilhadas entre sistemas operacionais. Comportamentos imprevisíveis podem ocorrer a menos que o redirecionamento de pastas seja usado corretamente.

Para redirecionar pastas em implantações avançadas:

- Use um Grupo de Entrega separado para cada SO.
- Entenda onde seus aplicativos virtuais, incluindo aqueles em desktops virtuais, armazenam dados e configurações do usuário, e entenda como os dados são estruturados.
- Para dados de perfil compartilhados que podem ser movidos com segurança (porque são estruturados de forma idêntica em cada SO), redirecione as pastas que os contêm em cada Grupo de Entrega.
- Para dados de perfil não compartilhados que não podem ser movidos, redirecione a pasta que os contém em apenas um dos Grupos de Desktop, geralmente aquele com o SO mais usado ou aquele onde os dados são mais relevantes. Alternativamente, para dados não compartilhados que não podem ser movidos entre SOs, redirecione as pastas que os contêm em ambos os sistemas para locais de rede separados.

Exemplo de implantação avançada

A implantação possui aplicativos, incluindo versões do Microsoft Outlook e Internet Explorer, sendo executados em desktops Windows 10 e aplicativos, incluindo outras versões do Outlook e Internet Explorer, entregues pelo Windows Server 2019. Você já configurou dois Grupos de Entrega para os dois SOs. Os usuários desejam acessar o mesmo conjunto de **Contatos** e **Favoritos** em ambas as versões dos dois aplicativos.

Importante: As seguintes decisões e conselhos são válidos para os SOs e a implantação descritos. Em sua organização, as pastas que você escolher redirecionar e se decidir compartilhá-las dependem de vários fatores exclusivos da sua implantação específica.

- Usando políticas aplicadas aos Grupos de Entrega, você escolhe as seguintes pastas para redirecionar.

PASTA	REDIRECIONADO NO WINDOWS 10?	REDIRECIONADO NO WINDOWS SERVER 2019?
Meus Documentos	Sim	Sim
Dados do Aplicativo	Não	Não
Contatos	Sim	Sim
Área de Trabalho	Sim	Não
Downloads	Não	Não
Favoritos	Sim	Sim
Links	Sim	Não
Minhas Músicas	Sim	Sim
Minhas Imagens	Sim	Sim
Meus Vídeos	Sim	Sim
Pesquisas	Sim	Não
Jogos Salvos	Não	Não
Menu Iniciar	Sim	Não

- Para as pastas compartilhadas e redirecionadas:
  - Após analisar a estrutura dos dados salvos pelas diferentes versões do Outlook e do Internet Explorer, você decide que é seguro compartilhar as pastas **Contatos** e **Favoritos**.
  - Você sabe que a estrutura das pastas **Meus Documentos**, **Minhas Músicas**, **Minhas Imagens** e **Meus Vídeos** é padrão em todos os sistemas operacionais. Portanto, é seguro armazenar essas pastas no mesmo local de rede para cada Grupo de Entrega.

- Para as pastas não compartilhadas e redirecionadas:
  - Você não redireciona as pastas Área de Trabalho, Links, Pesquisas ou **Menu Iniciar** no Grupo de Entrega do Windows Server porque os dados nessas pastas são organizados de forma diferente nos dois sistemas operacionais. Portanto, não podem ser compartilhados.
  - Para garantir um comportamento previsível desses dados não compartilhados, você os redireciona apenas no Grupo de Entrega do Windows 10. O Windows 10 é usado com mais frequência pelos usuários em seu trabalho diário. Os usuários acessam apenas ocasionalmente os aplicativos entregues pelo Windows Server. Além disso, neste caso, os dados não compartilhados são mais relevantes para um ambiente de área de trabalho do que para um ambiente de aplicativo. Por exemplo, os atalhos da área de trabalho são armazenados na pasta **Área de Trabalho** e podem ser úteis se forem originados de uma máquina Windows 10, mas não de uma máquina Windows Server.
- Para as pastas não redirecionadas:
  - Você não quer sobrecarregar seus servidores com arquivos baixados pelos usuários, então você escolhe não redirecionar a pasta Downloads
  - Dados de aplicativos individuais podem causar problemas de compatibilidade e desempenho, então você decide não redirecionar a pasta Dados de Aplicativos

Para obter mais informações sobre o redirecionamento de pastas, consulte Visão geral do redirecionamento de pastas, arquivos offline e perfis de usuário móveis.

Redirecionamento de pastas e exclusões

No Citrix Profile Management (mas não no Studio), uma melhoria de desempenho permite que você impeça que as pastas sejam processadas usando exclusões. Se você usar esse recurso, não exclua nenhuma pasta redirecionada. Os recursos de redirecionamento de pastas e exclusão funcionam juntos. Garantir que nenhuma pasta redirecionada seja excluída permite que o Profile Management as mova de volta para a estrutura da pasta de perfil e preserve a integridade dos dados se você decidir mais tarde não redirecioná-las. Para obter mais informações sobre exclusões, consulte Incluir e excluir itens.

Registro de VDA

Introdução

> **Observação:**

> Em um ambiente local, os VDAs se registram em um Delivery Controller. Em um ambiente de serviço Citrix Cloud, os VDAs se registram em um Cloud Connector. Em um ambiente híbrido, alguns VDAs se registram em um Delivery Controller enquanto outros se registram em um Cloud Connector.

> Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) com um ou mais Controllers ou Cloud Connectors no site. O VDA encontra um Controller ou Connector verificando uma lista chamada `ListofDDCs`. O `ListOfDDCs` em um VDA contém entradas DNS que apontam esse VDA para Controllers ou Cloud Connectors no site. Para balanceamento de carga, o VDA distribui automaticamente as conexões entre todos os Controllers ou Cloud Connectors na lista.

Por que o registro do VDA é tão importante?

- De uma perspectiva de segurança, o registro é uma operação sensível. Você está estabelecendo uma conexão entre o Controller ou Cloud Connector e o VDA. Para uma operação tão sensível, o comportamento esperado é rejeitar a conexão se tudo não estiver em perfeita ordem. Você está efetivamente estabelecendo dois canais de comunicação separados: VDA para Controller ou Cloud Connector, e Controller ou Cloud Connector para VDA. A conexão usa Kerberos, então problemas de sincronização de tempo e associação de domínio são implacáveis. O Kerberos usa Nomes de Entidade de Serviço (SPNs), então você não pode usar IP\\hostname balanceado por carga.
- Se um VDA não tiver informações precisas e atuais do Controller ou Cloud Connector à medida que você adiciona e remove Controllers (ou Cloud Connectors), o VDA poderá rejeitar inicializações de sessão que são intermediadas por um Controller ou Cloud Connector não listado. Entradas inválidas podem atrasar a inicialização do software do sistema de desktop virtual. Um VDA não aceitará uma conexão de um Controller ou Cloud Connector desconhecido e não confiável.

Além do `ListofDDCs`, o `ListOfSIDs` (IDs de Segurança) indica quais máquinas no `ListofDDCs` são confiáveis. O `ListofSIDs` pode ser usado para diminuir a carga no Active Directory ou para evitar possíveis ameaças de segurança de um servidor DNS comprometido. Para mais informações, consulte ListOfSIDs.

Se um `ListofDDCs` especificar mais de um Controller ou Cloud Connector, o VDA tenta se conectar a eles em ordem aleatória. Em uma implantação local, o `ListofDDCs` também pode

conter grupos de Controller. O VDA tenta se conectar a cada Controller em um grupo antes de passar para outras entradas no `ListofDDCs`.

O Citrix Virtual Apps and Desktops™ testa automaticamente a conectividade com os Controllers ou Cloud Connectors configurados durante a instalação do VDA. Erros são exibidos se um Controller ou Cloud Connector não puder ser alcançado. Se você ignorar um aviso de que um Controller ou Cloud Connector não pode ser contatado (ou quando você não especifica endereços de Controller ou Cloud Connector durante a instalação do VDA), as mensagens o lembrarão.

Métodos para configurar endereços de Controller ou Cloud Connector

O administrador escolhe o método de configuração a ser usado quando o VDA se registra pela primeira vez (o registro inicial). Durante o registro inicial, um cache persistente é criado no VDA. Durante os registros subsequentes, o VDA recupera a lista de Controllers ou Cloud Connectors desse cache local, a menos que uma alteração de configuração seja detectada.

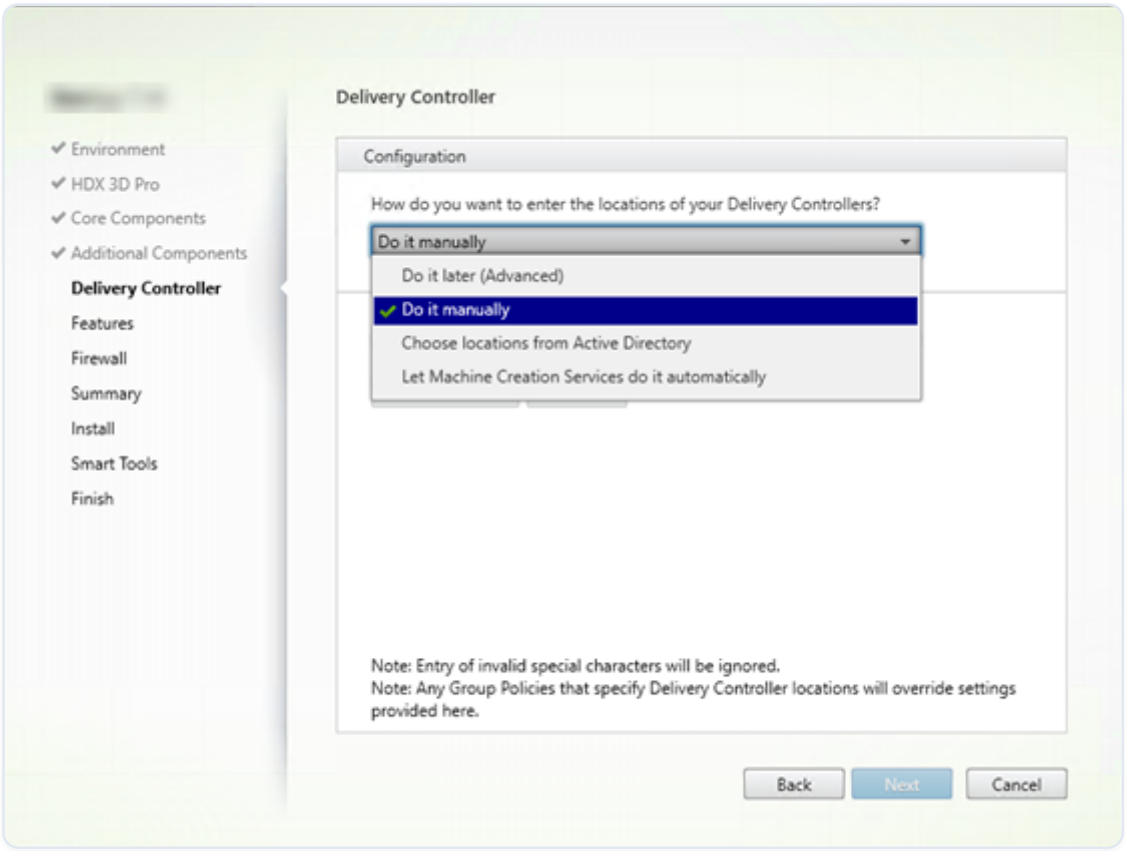
A maneira mais fácil de recuperar essa lista durante os registros subsequentes é usando o recurso de atualização automática. A atualização automática é habilitada por padrão. Para mais informações, consulte Atualização automática.

Existem vários métodos para configurar endereços de Controller ou Cloud Connector em um VDA.

- Baseado em política (LGPO ou GPO)
- Baseado em registro (manual, Preferências de Política de Grupo (GPP), especificado durante a instalação do VDA)
- Baseado em OU do Active Directory (descoberta de OU legada)
- Baseado em MCS (personality.ini)

Você especifica o método de registro inicial ao instalar um VDA. (Se você desativar a atualização automática, o método selecionado durante a instalação do VDA será usado para registros subsequentes.)

O gráfico a seguir mostra a página **Delivery Controller** do assistente de instalação do VDA.



Baseado em política (LGPO\\GPO)

A Citrix® recomenda usar GPO para o registro inicial do VDA. Ele tem a prioridade mais alta. (Embora a atualização automática seja listada como a prioridade mais alta, a atualização automática é usada somente após o registro inicial.) O registro baseado em política oferece as vantagens de centralização do uso da Política de Grupo para configuração.

Para especificar este método, conclua as duas etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer mais tarde (avançado)**. O assistente o lembrará várias vezes para especificar os endereços do Controller, mesmo que você não os esteja especificando durante a instalação do VDA. (O registro do VDA é muito importante.)
- Habilite ou desabilite o registro de VDA baseado em política por meio da política Citrix com a configuração `Virtual Delivery Agent Settings > Controllers`. (Se a segurança for sua principal prioridade, use a configuração `Virtual Delivery Agent Settings > Controller SIDs`.)

Essa configuração é armazenada em `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

Baseado em registro

Para especificar este método, conclua uma das seguintes etapas:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Fazer manualmente**. Em seguida, insira o FQDN de um Controller instalado e clique em **Adicionar**. Se você instalou mais Controllers, adicione seus endereços.
- Para uma instalação de VDA por linha de comando, use a opção /controllers e especifique os FQDNs dos Controllers ou Cloud Connectors instalados.

Essa informação é armazenada no valor de registro `ListOfDDCs` na chave de registro `HKLM\Software\Citrix\VirtualDesktopAgent` ou `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

Você também pode configurar esta chave de registro manualmente ou usar Preferências de Política de Grupo (GPP). Este método pode ser preferível ao método baseado em política (por exemplo, se você quiser processamento condicional de diferentes Controladores ou Cloud Connectors, como: usar XDC-001 para nomes de computador que começam com XDW-001-).

Atualize a chave de registro `ListOfDDCs`, que lista os FQDNs de todos os Controladores ou Cloud Connectors no site. (Esta chave é o equivalente à OU do site do Active Directory.)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

Se o local de registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` contiver as chaves `ListOfDDCs` e `FarmGUID`, `ListOfDDCs` será usado para a descoberta de Controladores ou Cloud Connectors. O `FarmGUID` está presente se uma OU de site foi especificada durante a instalação do VDA. (Isso pode ser usado em implantações legadas.)

Opcionalmente, atualize a chave de registro `ListOfSIDs` (para mais informações, consulte ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

Lembre-se: Se você também habilitar o registro de VDA baseado em política através da política Citrix que substitui as configurações especificadas durante a instalação do VDA, porque é um método de prioridade mais alta.

Baseado em OU do Active Directory (legado)

Este método é suportado principalmente para compatibilidade com versões anteriores e não é recomendado. Se você ainda o estiver usando, a Citrix sugere mudar para outro método.

Para especificar este método, conclua as duas etapas a seguir:

- Na página **Delivery Controller** do assistente de instalação do VDA, selecione **Escolher locais do Active Directory.**
- Use o script `Set-ADControllerDiscovery.ps1` (disponível em cada Controller). Além disso, configure a entrada de registro `FarmGuid` em cada VDA para apontar para a OU correta. Esta configuração pode ser feita usando a Política de Grupo.

Baseado em MCS

Se você usa o MCS para provisionar VMs, o MCS configura a lista de Controladores ou Cloud Connectors. Este recurso funciona com a atualização automática. Ao criar o catálogo, o MCS injeta a lista de Controladores ou Cloud Connectors no arquivo `Personality.ini` durante o provisionamento inicial. A atualização automática mantém a lista atualizada.

Para especificar este método, na página **Delivery Controller** do assistente de instalação do VDA, selecione **Deixar o Machine Creation Services™ fazer isso**.

Revisão e recomendações

Como melhor prática:

- Use o método de registro de Política de Grupo para o registro inicial.
- Use a atualização automática (habilitada por padrão) para manter sua lista de Controladores atualizada.
- Em uma implantação de várias zonas, use a Política de Grupo para a configuração inicial (com pelo menos dois Controladores ou Cloud Connectors). Aponte os VDAs para Controladores ou Cloud Connectors locais (em) sua zona. Use a atualização automática para mantê-los atualizados. A atualização automática otimiza automaticamente o `ListofDDCs` para VDAs em zonas satélites.
- Liste mais de um controlador na chave de registro `ListOfDDCs`, separados por um espaço, para evitar problemas de registro se um Controlador não estiver disponível. Por exemplo:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs
```

```
HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- Certifique-se de que todos os valores listados em `ListofDDCs` mapeiem para um nome de domínio totalmente qualificado válido para evitar atrasos no registro de inicialização.

Atualização automática

A atualização automática (introduzida no XenApp e XenDesktop 7.6) é habilitada por padrão. É o método mais eficiente para manter seus registros de VDA atualizados. Embora não seja usada para o registro inicial, o software de atualização automática baixa e armazena o `ListofDDCs` em um cache persistente no VDA quando o registro inicial ocorre. Este processo é feito para cada VDA. O cache também contém informações de política da máquina, o que garante que as configurações de política sejam mantidas após reinicializações.

A atualização automática é suportada ao usar MCS ou Citrix Provisioning™ para provisionar máquinas, exceto para o cache do lado do servidor do Citrix Provisioning. O cache do lado do servidor não é um cenário comum porque não há armazenamento persistente para o cache de atualização automática.

Para especificar este método:

- Habilite ou desabilite a atualização automática por meio de uma política Citrix contendo a configuração `Virtual Delivery Agent Settings > Enable auto update of Controllers`. Esta configuração é habilitada por padrão.

Como funciona:

- Cada vez que um VDA se registra novamente (por exemplo, após uma reinicialização da máquina), o cache é atualizado. Cada Controlador ou Cloud Connector também verifica o banco de dados do site a cada 90 minutos. Se um Controlador ou Cloud Connector foi adicionado ou removido desde a última verificação, ou se ocorreu uma alteração de política que afeta o registro do VDA, o Controlador ou Cloud Connector envia uma lista atualizada para seus VDAs registrados e o cache é atualizado. O VDA aceita conexões de todos os Controladores ou Cloud Connectors em sua lista mais recentemente armazenada em cache.
- Se um VDA receber uma lista que não inclui o Controlador ou Cloud Connector com o qual está registrado (em outras palavras, esse Controlador ou Cloud Connector foi removido do

site), o VDA se registrará novamente, escolhendo entre os Controladores ou Cloud Connectors no `ListofDDCs`.

Exemplo:

- Uma implantação tem três Controladores: A, B e C. Um VDA se registra com o Controlador B (que foi especificado durante a instalação do VDA).
- Posteriormente, dois Controladores (D e E) são adicionados ao site. Em 90 minutos, os VDAs recebem listas atualizadas e então aceitam conexões dos Controladores A, B, C, D e E. (A carga não é distribuída igualmente para todos os Controladores até que os VDAs sejam reiniciados.)
- Mais tarde ainda, o Controller B é movido para outro site. Em 90 minutos, os VDAs no site original recebem listas atualizadas porque houve uma alteração de Controller desde a última verificação. O VDA que se registrou originalmente com o Controller B (que não está mais na lista) se registra novamente, escolhendo entre os Controllers na lista atual (A, C, D e E).

Em uma implantação multizona, a atualização automática em uma zona satélite armazena em cache automaticamente todos os Controllers locais primeiro. Todos os Controllers na zona primária são armazenados em cache em um grupo de backup. Se nenhum Controller local na zona satélite estiver disponível, o registro é tentado com os Controllers na zona primária.

Conforme mostrado no exemplo a seguir, o arquivo de cache contém nomes de host e uma lista de IDs de Segurança (`ListofSIDs`). O VDA não consulta SIDs e, portanto, reduz a carga do Active Directory.

```
<?xml version="1.0"?>
<ListOfDDCsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
 - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    - <d2p1:ArrayOfstring>
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
      </d2p1:ArrayOfstring>
  </_x003C_GroupsOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
  </_x003C_ListOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
  </_x003C_ListOfSids_x003E_k__BackingField>
  <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
  <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDCsListIfSids>
```

Você pode recuperar o arquivo de cache com uma chamada WMI. No entanto, ele é armazenado em um local que é legível apenas pela conta SYSTEM.

> **Importante:**

> Esta informação é fornecida apenas para fins informativos. NÃO MODIFIQUE ESTE ARQUIVO. Qualquer modificação neste arquivo ou pasta resulta em uma configuração não suportada.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

Se você precisar configurar manualmente o `ListofSIDs` por motivos de segurança (distinto da redução da carga do Active Directory), você não poderá usar o recurso de atualização automática. Para obter detalhes, consulte ListOfSIDs.

Exceção à prioridade de atualização automática

Embora a atualização automática geralmente tenha a maior prioridade entre todos os métodos de registro de VDA e substitua as configurações para outros métodos, há uma exceção. Os elementos `NonAutoListOfDDCs` no cache especificam o método de configuração inicial do VDA. A atualização automática monitora essas informações. Se o método de registro inicial mudar, o processo de registro ignora a atualização automática e usa o método de prioridade configurado de nível mais alto seguinte. Esse processo pode ser útil ao mover um VDA para outro site (por exemplo, durante a recuperação de desastres).

Considerações de configuração

Visualize uma configuração comum de registro de VDA.

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Visualize as etapas de registro do VDA.

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Considere o seguinte ao configurar itens que podem afetar o registro do VDA.

Endereços de Controller ou Cloud Connector

Independentemente do método que você usa para especificar Controllers ou Cloud Connectors, a Citrix recomenda usar um endereço FQDN. Um endereço IP não é considerado uma configuração confiável, porque é mais fácil comprometer um IP do que um registro DNS. Se você preencher o `ListofSIDs` manualmente, poderá usar um IP em um `ListofDDCs`. No entanto, o FQDN ainda é recomendado.

Balanceamento de carga

Conforme observado anteriormente, o VDA distribui automaticamente as conexões entre todos os Controllers ou Cloud Connectors no `ListofDDCs`. A funcionalidade de failover e balanceamento de carga é incorporada ao Citrix Brokering Protocol (CBP). Se você especificar vários Controllers ou Cloud Connectors em sua configuração, o registro fará o failover automaticamente entre eles, se necessário. Com a atualização automática, o failover automático ocorre automaticamente para todos os VDAs.

Por motivos de segurança, você não pode usar um balanceador de carga de rede, como o Citrix ADC. O registro do VDA usa autenticação mútua Kerberos, onde o cliente (VDA) deve provar sua identidade ao serviço (Controller). No entanto, o Controller ou Cloud Connector deve provar sua identidade ao VDA. Isso significa que o VDA e o Controller ou Cloud Connector estão agindo como servidor e cliente ao mesmo tempo. Conforme observado no início deste artigo, existem dois canais de comunicação: VDA para Controller/Cloud Connector e Controller/Cloud Connector para VDA.

Um componente neste processo é chamado Service Principal Name (SPN), que é armazenado como uma propriedade em um objeto de computador do Active Directory. Quando seu VDA se conecta a um Controller ou Cloud Connector, ele deve especificar com quem deseja se comunicar. Este endereço é um SPN. Se você usar um IP balanceado por carga, a autenticação mútua Kerberos reconhece corretamente que o IP não pertence ao Controller ou Cloud Connector esperado.

Para obter mais informações, consulte:

- Introdução ao Kerberos
- Autenticação mútua usando Kerberos

A atualização automática substitui o CNAME

O recurso de atualização automática substitui a função CNAME (alias DNS) das versões do XenApp e XenDesktop anteriores à 7.x. A funcionalidade CNAME é desabilitada a partir do XenApp e XenDesktop 7. Use a atualização automática em vez de CNAME. (Se você precisar usar CNAME, consulte CTX137960. Para que o aliasing de DNS funcione de forma consistente, não use atualização automática e CNAME ao mesmo tempo.)

Grupos de Controller/Cloud Connector

Em certos cenários, você pode querer processar Controllers ou Cloud Connectors em grupos, com um grupo sendo preferencial e o outro grupo usado para failover se todos os Controllers/Cloud

Connectors falharem. Lembre-se de que os Controllers ou Cloud Connectors são selecionados aleatoriamente da lista, então o agrupamento pode ajudar a impor o uso preferencial.

Esses grupos são destinados ao uso dentro de um único site (não em vários sites).

Use parênteses para especificar grupos de Controllers/Cloud Connectors. Por exemplo, com quatro Controllers (dois primários e dois de backup), um agrupamento pode ser:

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

Neste exemplo, os Controllers do primeiro grupo (001 e 002) são processados primeiro. Se ambos falharem, os Controllers do segundo grupo (003 e 004) são processados.

Para XenDesktop 7.0 ou superior, há uma etapa extra que você precisa realizar para usar o recurso **Registration Groups**. Você precisa **Proibir** a política **Enable Auto Update of Controller** no Studio.

ListOfSIDs

A lista de Controllers que um VDA pode contatar para registro é o `ListofDDCs`. Um VDA também deve saber em quais Controllers confiar, pois os VDAs não confiam automaticamente nos Controllers em `ListofDDCs`. Os `ListofSIDs` (IDs de Segurança) identificam os Controllers confiáveis. Os VDAs tentam se registrar apenas com Controllers confiáveis.

Na maioria dos ambientes, o `ListofSIDs` é gerado automaticamente a partir do `ListofDDCs`. Você pode usar um rastreamento CDF para ler o `ListofSIDs`.

Geralmente, não há necessidade de modificar manualmente o `ListofSIDs`. Existem várias exceções. As duas primeiras exceções não são mais válidas porque tecnologias mais recentes estão disponíveis.

- **Funções separadas para Controllers:** Antes da introdução das zonas no XenApp e XenDesktop 7.7, o `ListofSIDs` era configurado manualmente quando apenas um subconjunto de Controllers era usado para registro. Por exemplo, se você estivesse usando XDC-001 e XDC-002 como XML brokers, e XDC-003 e XDC-004 para registro de VDA, você especificava todos os Controllers em `ListofSIDs`, e XDC-003 e XDC-004 em `ListofDDCs`. Esta não é uma configuração típica ou recomendada. Não a use em ambientes mais recentes. Em vez disso, use zonas.
- **Reduzindo a carga do Active Directory:** Antes da introdução do recurso de atualização automática no XenApp e XenDesktop 7.6, o `ListofSIDs` era usado para reduzir a carga nos controladores de domínio. Ao pré-popular o `ListofSIDs`, a resolução de nomes DNS para

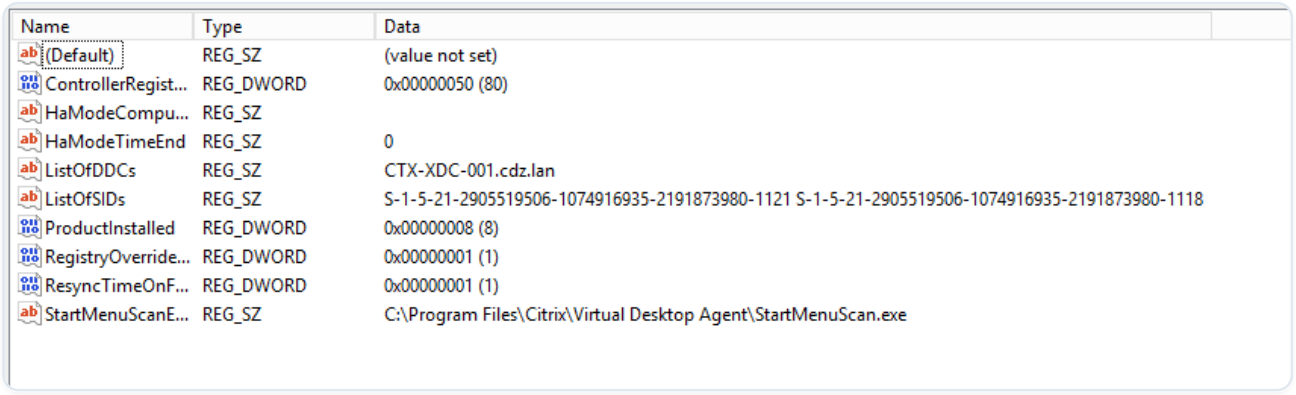
SIDs pode ser ignorada. No entanto, o recurso de atualização automática elimina a necessidade desse trabalho, pois esse cache persistente contém SIDs. A Citrix recomenda manter o recurso de atualização automática ativado.

- **Segurança:** Em alguns ambientes altamente seguros, os SIDs de Controllers confiáveis eram configurados manualmente para evitar possíveis ameaças de segurança de um servidor DNS comprometido. No entanto, se você fizer isso, também deverá desativar o recurso de atualização automática. Caso contrário, a configuração de um cache persistente será usada.

Portanto, a menos que você tenha um motivo específico, não modifique o `ListofSIDs`.

Se você precisar modificar o `ListofSIDs`, crie uma chave de registro chamada `ListOfSIDs (REG_SZ)` em `HKLM\Software\Citrix\VirtualDesktopAgent`. O valor é uma lista de SIDs confiáveis, separados por espaços se houver mais de um.

No exemplo a seguir, um Controller é usado para registro de VDA (`ListofDDCs`), mas dois Controllers são usados para intermediação (List OfSIDs).



Pesquisa de Controller durante o registro de VDA

Quando um VDA tenta se registrar, o Broker Agent primeiro executa uma pesquisa DNS no domínio local para garantir que o Controller especificado possa ser alcançado.

Se essa pesquisa inicial não encontrar o Controller, o Broker Agent pode iniciar uma consulta de fallback de cima para baixo no AD. Essa consulta pesquisa todos os domínios e se repete com frequência. Se o endereço do Controller for inválido (por exemplo, o administrador inseriu um FQDN incorreto ao instalar o VDA), a atividade dessa consulta pode potencialmente levar a uma condição de negação de serviço distribuída (DDoS) no controlador de domínio.

A seguinte chave de registro controla se o Broker Agent usa a consulta de fallback de cima para baixo quando não consegue localizar um Controller durante a pesquisa inicial.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- Nome: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valor: `0` (padrão) ou qualquer valor diferente de zero

Quando definido como `0`, a pesquisa de fallback é ativada. Se a pesquisa inicial pelo Controller falhar, a pesquisa de fallback de cima para baixo é iniciada. Este é o comportamento padrão. No entanto, se definido como qualquer valor diferente de zero, a pesquisa de fallback é desativada. Se a pesquisa inicial pelo Controller falhar, o Broker Agent para de procurar.

Sequenciamento de vinculação LDAP durante o registro do VDA usando um controlador de domínio somente leitura

Quando um VDA se registra em um controlador de domínio somente leitura (RODC), o Broker Agent deve selecionar qual vinculação ou vinculações do Light Directory Access Protocol (LDAP) ignorar. Para fazer essa seleção, o Broker Agent requer uma chave de registro adequada.

Se uma chave de registro não for fornecida, ou o campo da chave de registro estiver vazio, o registro do VDA com o RODC leva mais tempo porque é necessário passar pela sequência de vinculação LDAP original.

Para modificar a sequência de vinculação LDAP, a chave de registro `ListofIgnoredBindings` foi adicionada a `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. O uso de `ListofIgnoredBindings` permite modificar a sequência de vinculação LDAP conforme necessário e, assim, acelerar o registro do VDA com um RODC.

- Nome: `ListofIgnoredBindings`
- Tipo: `REG_SZ`
- Valores: `DefaultPath`, `DomainPath`, `PDCPath`

O valor é uma lista de opções de caminho de vinculação, cada uma separada por uma vírgula. A chave de registro ignora valores que não reconhece como válidos.

Solucionar problemas de registro do VDA

Conforme observado anteriormente, um VDA deve ser registrado em um Delivery Controller ou Cloud Connector para ser considerado ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos que, de outra forma, estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador

pode solucionar. O Studio fornece informações de solução de problemas no assistente de criação de catálogo e depois que você cria um Grupo de Entrega.

- **Identificando problemas durante a criação do catálogo de máquinas:** No assistente de criação de catálogo, depois de adicionar máquinas existentes, a lista de nomes de contas de computador indica se cada máquina é adequada para ser adicionada ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre essa máquina.

  Se a mensagem identificar uma máquina problemática, você pode remover essa máquina (usando o botão **Remover**) ou adicionar a máquina. Por exemplo, se uma mensagem indicar que as informações sobre uma máquina não foram obtidas (talvez porque ela nunca tenha sido registrada), você pode optar por adicionar a máquina de qualquer maneira.

  O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso de recursos introduzidos em novas versões do produto pode exigir um novo VDA. Definir um nível funcional torna todos os recursos introduzidos nessa versão (e posteriores, se o nível funcional não mudar) disponíveis para as máquinas no catálogo. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não poderão se registrar.
- **Identificando problemas após a criação de Grupos de Entrega:** Depois de criar um Grupo de Entrega, o Studio exibe detalhes sobre as máquinas associadas a esse grupo.

  O painel de detalhes de um Grupo de Entrega indica o número de máquinas que devem ser registradas, mas não estão. Em outras palavras, pode haver uma ou mais máquinas ligadas e não em modo de manutenção, mas que não estão atualmente registradas em um Controller. Ao visualizar uma máquina "não registrada, mas que deveria estar", revise a guia **Solucionar problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

Mais informações sobre a solução de problemas de registro do VDA

- Para obter mais informações sobre níveis funcionais, consulte Versões de VDA e níveis funcionais.
- Para obter mais informações sobre a solução de problemas de registro de VDA, consulte CTX136668.
- Você também pode usar as verificações de integridade do Citrix Scout para solucionar problemas de registro de VDA e inicialização de sessão. Para obter detalhes, consulte Sobre as verificações de integridade.

IP virtual e loopback virtual

Importante:

- O Windows 10 Enterprise multi-session não oferece suporte à Virtualização de IP da Área de Trabalho Remota (IP Virtual) e não oferecemos suporte à Virtualização de IP da Área de Trabalho Remota ou loopback virtual no Windows 10 Enterprise multi-session.
- A Virtualização de IP da Área de Trabalho Remota (IP Virtual) não é suportada em máquinas hospedadas na nuvem. Para obter mais informações, consulte a documentação Microsoft.

Os recursos de Virtualização de IP da Área de Trabalho Remota e loopback virtual são suportados em máquinas Windows Server 2016, Windows Server 2019 e Windows Server 2022. Esses recursos não se aplicam a máquinas com sistema operacional Windows desktop.

O recurso de endereço de Virtualização de IP da Área de Trabalho Remota da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. Com o recurso de loopback virtual da Citrix, você pode configurar aplicativos que dependem de comunicações com localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo de localhost (127.*).

Certos aplicativos, como CRM e Integração de Telefonia Computadorizada (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros propósitos que exigem um endereço IP exclusivo ou endereço de loopback. Outros aplicativos podem se vincular a uma porta estática, de modo que as tentativas de iniciar instâncias adicionais de um aplicativo em um ambiente multiusuário falham porque a porta está em uso. Para que esses aplicativos funcionem corretamente em um ambiente Citrix Virtual Apps™, é necessário um endereço IP exclusivo para cada dispositivo.

A Virtualização de IP da Área de Trabalho Remota e o loopback virtual são recursos independentes um do outro. Você pode usar um ou ambos.

Sinopse da ação do administrador:

- Para usar a Virtualização de IP da Área de Trabalho Remota da Microsoft, habilite e configure-a no servidor Windows. (As configurações de política do Citrix® não são necessárias.)

- Para usar o loopback virtual da Citrix, configure duas configurações em uma política da Citrix.

Virtualização de IP da Área de Trabalho Remota (IP Virtual)

Quando a Virtualização de IP da Área de Trabalho Remota é habilitada e configurada no servidor Windows, cada aplicativo configurado em execução em uma sessão parece ter um endereço exclusivo. Os usuários acessam esses aplicativos em um servidor Citrix Virtual Apps da mesma forma que acessam qualquer outro aplicativo publicado. Um processo requer Virtualização de IP da Área de Trabalho Remota em qualquer um dos seguintes casos:

- O processo usa um número de porta TCP codificado
- O processo usa soquetes do Windows e requer um endereço IP exclusivo ou um número de porta TCP especificado

Para determinar se um aplicativo precisa usar endereços de Virtualização de IP da Área de Trabalho Remota:

1. Obtenha a ferramenta **TCPView** da Microsoft. Esta ferramenta lista todos os aplicativos que vinculam endereços IP e portas específicos. Para obter mais informações sobre o TCPView, consulte a documentação Microsoft.
2. Desative o recurso **Resolver Endereços IP** para que você veja os endereços em vez dos nomes de host.
3. Inicie o aplicativo e use o **TCPView** para ver quais endereços IP e portas o aplicativo abre e quais nomes de processo estão abrindo essas portas.
4. Configure quaisquer processos que abram o endereço IP do servidor, 0.0.0.0 ou 127.0.0.1.
5. Para garantir que um aplicativo não abra o mesmo endereço IP em uma porta diferente, inicie outra instância do aplicativo.

Como funciona a virtualização de IP do Microsoft Remote Desktop (RD)

- O endereçamento IP virtual deve ser habilitado no servidor Microsoft.

  Por exemplo, em um ambiente Windows Server 2016, no Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões do Host da Sessão RD** para habilitar o recurso de Virtualização de IP RD e configurar as definições para atribuir dinamicamente endereços IP usando o servidor Dynamic Host Configuration Protocol (DHCP) por sessão ou por programa. Para obter mais informações sobre como configurar a Virtualização de IP da Área de Trabalho Remota, consulte a documentação Microsoft.

- Após habilitar o recurso, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente do servidor DHCP.
- O recurso **Virtualização de IP RD** atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilharão um endereço IP por sessão.
- Depois que um endereço é atribuído a uma sessão, a sessão usa o endereço virtual em vez do endereço IP principal do sistema sempre que as seguintes chamadas são feitas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Ao usar o recurso de virtualização de IP da Microsoft na configuração de hospedagem de sessão da Área de Trabalho Remota, os aplicativos são vinculados a endereços IP específicos inserindo um componente de “filtro” entre o aplicativo e as chamadas de função Winsock. O aplicativo então vê apenas o endereço IP correto a ser usado. Qualquer tentativa do aplicativo de escutar comunicações TCP ou UDP é vinculada automaticamente ao seu endereço IP virtual alocado (ou endereço de loopback). Quaisquer conexões de origem abertas pelo aplicativo se originam do endereço IP vinculado ao aplicativo.

Em funções que retornam um endereço (como `GetAddrInfo()`, que uma política do Windows controla), se o endereço IP do host local for solicitado, a Virtualização de IP da Área de Trabalho Remota examina o endereço IP retornado e o altera para o endereço de Virtualização de IP da Área de Trabalho Remota da sessão. Aplicativos que tentam obter o endereço IP do servidor local por meio de tais funções de nome veem apenas o endereço de Virtualização de IP da Área de Trabalho Remota exclusivo atribuído a essa sessão. Este endereço IP é frequentemente usado em chamadas de soquete subsequentes, como bind ou connect. Para obter mais informações sobre as políticas do Windows, consulte Virtualização de IP RDS no Windows Server.

Frequentemente, um aplicativo solicita vincular-se a uma porta para escutar no endereço 0.0.0.0. Quando um aplicativo faz isso e usa uma porta estática, você não pode iniciar mais de uma instância do aplicativo. O recurso de endereço de Virtualização de IP da Área de Trabalho Remota também procura por 0.0.0.0 nesses tipos de chamada. Ele altera a chamada para escutar no endereço de Virtualização de IP da Área de Trabalho Remota específico, o que permite que mais de um aplicativo escute na mesma porta no mesmo computador, pois todos estão escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço de Virtualização de IP da Área de Trabalho Remota estiver habilitado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentarem se vincular a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas serão vinculadas a VIPAddress1:9000 e VIPAddress2:9000 e não haverá conflito.

Loopback virtual

Habilitar as configurações da **política de loopback de Virtualização de IP da Área de Trabalho Remota da Citrix** permite que cada sessão tenha seu próprio endereço de loopback para comunicação. Quando um aplicativo usa o endereço localhost (padrão = 127.0.0.1) em uma chamada Winsock, o recurso de loopback virtual simplesmente substitui 127.0.0.1 por 127.X.X.X, onde X.X.X é uma representação do ID da sessão + 1. Por exemplo, um ID de sessão de 7 é 127.0.0.8. No caso improvável de o ID da sessão exceder o quarto octeto (mais de 255), o endereço passa para o próximo octeto (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em qualquer um dos seguintes casos:

- O processo usa o endereço de loopback (localhost) do soquete do Windows (127.0.0.1)
- O processo usa um número de porta TCP codificado

Use as configurações da política de loopback virtual para aplicativos que usam um endereço de loopback para comunicação entre processos. Nenhuma configuração adicional é necessária. O loopback virtual não tem dependência de IP Virtual, então você não precisa configurar o servidor Microsoft.

- Suporte a loopback de IP virtual. Quando ativada, esta configuração de política permite que cada sessão tenha seu próprio endereço de loopback virtual. Esta configuração está desativada por padrão. O recurso se aplica apenas a aplicativos especificados com a configuração de política da lista de programas de loopback virtual de IP virtual.
- Lista de programas de loopback virtual de IP virtual. Esta configuração de política especifica os aplicativos que usam o recurso de loopback de IP virtual. Esta configuração se aplica apenas quando a configuração de política de suporte a loopback de IP virtual está ativada.
- Exclusão de porta de loopback de IP virtual. Quando um aplicativo chama o endereço de loopback nas portas especificadas nesta configuração, o loopback virtual não altera a chamada para o endereço de loopback específico da sessão.

Recurso relacionado

Você pode usar as seguintes configurações de registro para garantir que o loopback virtual tenha preferência sobre o IP virtual. Esse recurso é chamado de loopback preferencial. No entanto, prossiga com cautela:

- Use o loopback preferencial somente se o IP Virtual e o loopback virtual estiverem habilitados. Caso contrário, você poderá ter resultados inesperados.

- A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Execute regedit nos servidores onde os aplicativos residem.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- Nome: PreferLoopback, Tipo: REG_DWORD, Dados: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dados: \<lista de processos\>

Zonas

> **Observação:**
>
> Você pode gerenciar sua implantação do Citrix Virtual Apps and Desktops™ usando dois consoles de gerenciamento: Web Studio (baseado na web) e Citrix Studio (baseado no Windows). Este artigo aborda apenas o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Implantações que abrangem locais amplamente dispersos conectados por uma WAN podem enfrentar desafios devido à latência e confiabilidade da rede. Existem duas opções que mitigam esses desafios:

- Implante vários sites, cada um com seu próprio banco de dados de site do SQL Server.

  Esta opção é recomendada para grandes implantações corporativas. Vários sites são gerenciados separadamente, e cada um requer seu próprio banco de dados de site do SQL Server. Cada site é uma implantação separada do Citrix Virtual Apps™.

- Configure várias zonas dentro de um único site.

  A configuração de zonas pode ajudar os usuários em regiões remotas a se conectarem a recursos sem necessariamente forçar suas conexões a atravessar grandes segmentos da WAN. O uso de zonas permite o gerenciamento eficaz do site a partir de um único console do Web Studio, Citrix Director e do banco de dados do site. Isso economiza os custos de implantação, pessoal, licenciamento e operação de mais sites contendo bancos de dados separados em locais remotos.

As zonas podem ser úteis em implantações de todos os tamanhos. Você pode usar zonas para manter aplicativos e desktops mais próximos dos usuários finais, o que melhora o desempenho. Uma zona pode ter um ou mais Controllers instalados localmente para redundância e resiliência, mas isso não é obrigatório.

O número de Controllers configurados no site pode afetar o desempenho de algumas operações, como adicionar novos Controllers ao próprio site. Para evitar isso, recomendamos que você limite o número de zonas em seu site Citrix Virtual Apps ou Citrix Virtual Desktops™ a no máximo 50.

Quando a latência da rede de suas zonas for superior a 250 ms RTT, recomendamos que você implante vários sites em vez de zonas.

Ao longo deste artigo, o termo local refere-se à zona em discussão. Por exemplo, "Um VDA se registra em um Controller local" significa que um VDA se registra em um Controller na zona onde o VDA está localizado.

As zonas nesta versão são semelhantes, mas não idênticas às zonas no XenApp versão 6.5 e anteriores. Por exemplo, nesta implementação de zonas, não há coletores de dados. Todos os Controllers no site se comunicam com um banco de dados do site na zona primária. Além disso, o failover e as zonas preferenciais funcionam de forma diferente nesta versão.

Tipos de zona

Um site sempre tem uma zona primária. Ele também pode, opcionalmente, ter uma ou mais zonas satélite. As zonas satélite podem ser usadas para recuperação de desastres, data centers geograficamente distantes, filiais, uma nuvem ou uma zona de disponibilidade em uma nuvem.

Zona primária:

A zona primária tem o nome padrão "Primary". Esta zona contém o banco de dados do site do SQL Server (e servidores SQL de alta disponibilidade, se usados), Web Studio, Director, Citrix StoreFront™, Citrix License Server e Citrix Gateway. Sempre mantenha o banco de dados do site na zona primária.

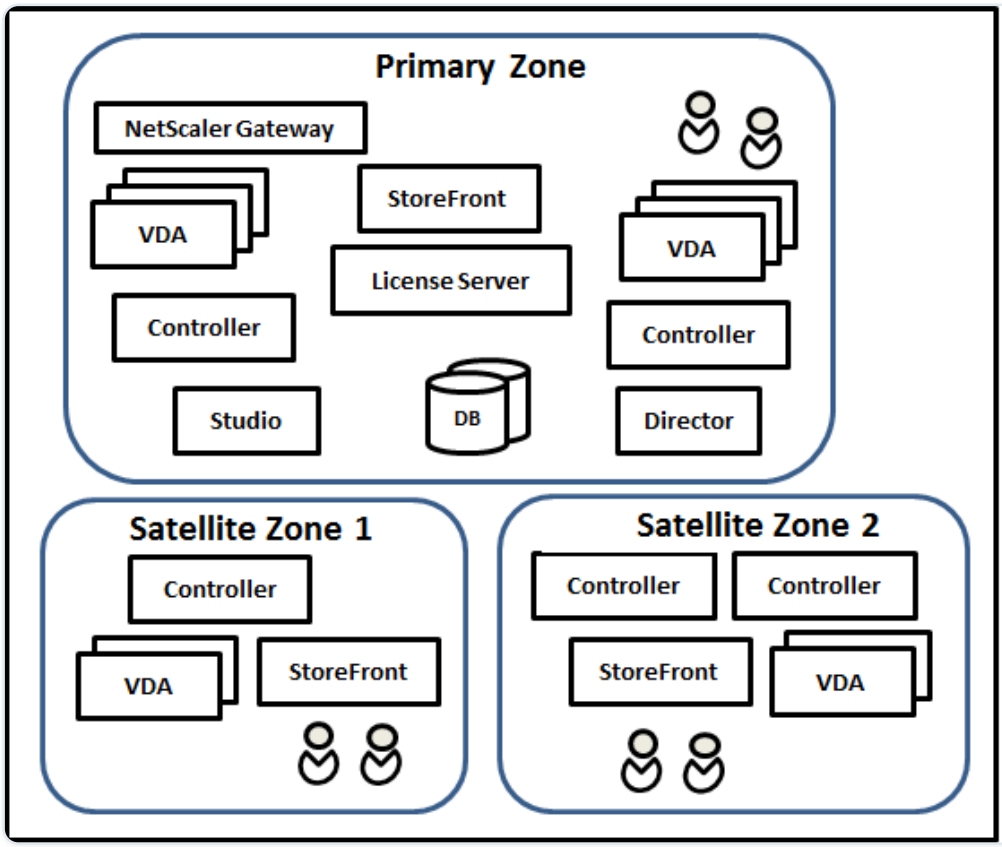
A zona primária deve ter pelo menos dois Controllers para redundância. A zona primária pode ter VDAs com aplicativos que estão fortemente acoplados ao banco de dados e à infraestrutura.

Zona satélite:

Uma zona satélite contém um ou mais VDAs, Controllers, servidores StoreFront e servidores Citrix Gateway. Em operações normais, os Controllers em uma zona satélite se comunicam diretamente com o banco de dados na zona primária.

Uma zona satélite, particularmente uma grande, também pode conter um hipervisor que é usado para provisionar e armazenar máquinas para essa zona. Ao configurar uma zona satélite, você pode associar um hipervisor ou outra conexão de serviço a ela. (Certifique-se de que todos os catálogos que usam essa conexão estejam na mesma zona.)

Um site pode ter zonas satélite com diferentes configurações, com base nas suas necessidades e ambiente exclusivos. A figura a seguir ilustra uma zona primária e exemplos de zonas satélite.



Na ilustração:

- **Zona primária:** Contém dois Controllers, Web Studio, Director, StoreFront, License Server e o banco de dados do site (além de implantações de SQL Server de alta disponibilidade). A zona primária também contém vários VDAs e um Citrix Gateway.
- **Zona satélite 1: VDAs com Controller:** A zona satélite 1 contém um Controller, VDAs e um servidor StoreFront. Os VDAs nesta zona satélite se registram no Controller local. O Controller local se comunica com o banco de dados do site e o servidor de licenças na zona primária.

  Se a WAN falhar, o recurso Local Host Cache permite que o Controller na zona satélite continue a intermediar conexões para VDAs nessa zona. Tal implantação pode ser eficaz em

um escritório onde os trabalhadores usam um site StoreFront local e o Controller local para acessar seus recursos locais.

- **Zona satélite 2: VDAs com Controllers redundantes:** A zona satélite 2 contém dois Controllers, VDAs e um servidor StoreFront. Este é o tipo de zona mais resiliente, oferecendo proteção contra uma falha simultânea da WAN e de um dos Controllers locais.

Onde os VDAs se registram e onde os Controllers fazem failover

Em um site contendo zonas primárias e satélite, com VDAs na versão mínima 7.7:

- Um VDA na zona primária se registra em um Controller na zona primária. Um VDA na zona primária nunca tenta se registrar em um Controller em uma zona satélite.
- Um VDA em uma zona satélite se registra em um Controller local, se possível. (Este é considerado o Controller preferencial.) Se nenhum Controller local estiver disponível (por exemplo, porque não podem aceitar mais registros de VDA ou falharam), o VDA tentará se registrar em um Controller na zona primária. Neste caso, o VDA permanece registrado na zona primária, mesmo que um Controller em uma zona satélite se torne disponível novamente. Um VDA em uma zona satélite nunca tenta se registrar em um Controller em outra zona satélite.
- Quando a atualização automática está habilitada para a descoberta de Controllers pelo VDA, e você especifica uma lista de endereços de Controller durante a instalação do VDA, um Controller é selecionado aleatoriamente dessa lista para o registro inicial (independentemente da zona em que o Controller reside). Após a reinicialização da máquina com esse VDA, o VDA começará a preferir registrar-se com um Controller em sua zona local.
- Se um Controller em uma zona satélite falhar, ele fará failover para outro Controller local, se possível. Se nenhum Controller local estiver disponível, ele fará failover para um Controller na zona primária.
- Se você mover um Controller para dentro ou para fora de uma zona, e a atualização automática estiver habilitada, os VDAs em ambas as zonas receberão listas atualizadas indicando quais Controllers são locais e quais estão na zona primária, para que saibam com quem podem se registrar e de quem podem aceitar conexões.
- Se você mover um catálogo para outra zona, os VDAs nesse catálogo se registrarão novamente com os Controllers na zona para onde você moveu o catálogo. (Ao mover um catálogo para outra zona, certifique-se de que esta zona e a zona com a conexão de host associada estejam bem conectadas. Se houver largura de banda limitada ou alta latência, mova a conexão de host para a mesma zona que contém o catálogo de máquinas associado.)

Se todos os Controllers na zona primária falharem:

- O Web Studio não consegue se conectar ao site.
- Conexões com VDAs na zona primária não podem ser estabelecidas.
- O desempenho do site degrada até que os Controllers na zona primária se tornem disponíveis.

Para sites contendo versões de VDA anteriores a 7.7:

- Um VDA em uma zona satélite aceita solicitações de Controllers em sua zona local e na zona primária. (VDAs na versão mínima 7.7 podem aceitar solicitações de Controller de outras zonas satélites.)
- Um VDA em uma zona satélite se registra com um Controller na zona primária ou na zona local aleatoriamente. (VDAs na versão mínima 7.7 preferem a zona local.)

Preferência de zona

Para usar o recurso de preferência de zona, você deve estar usando no mínimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

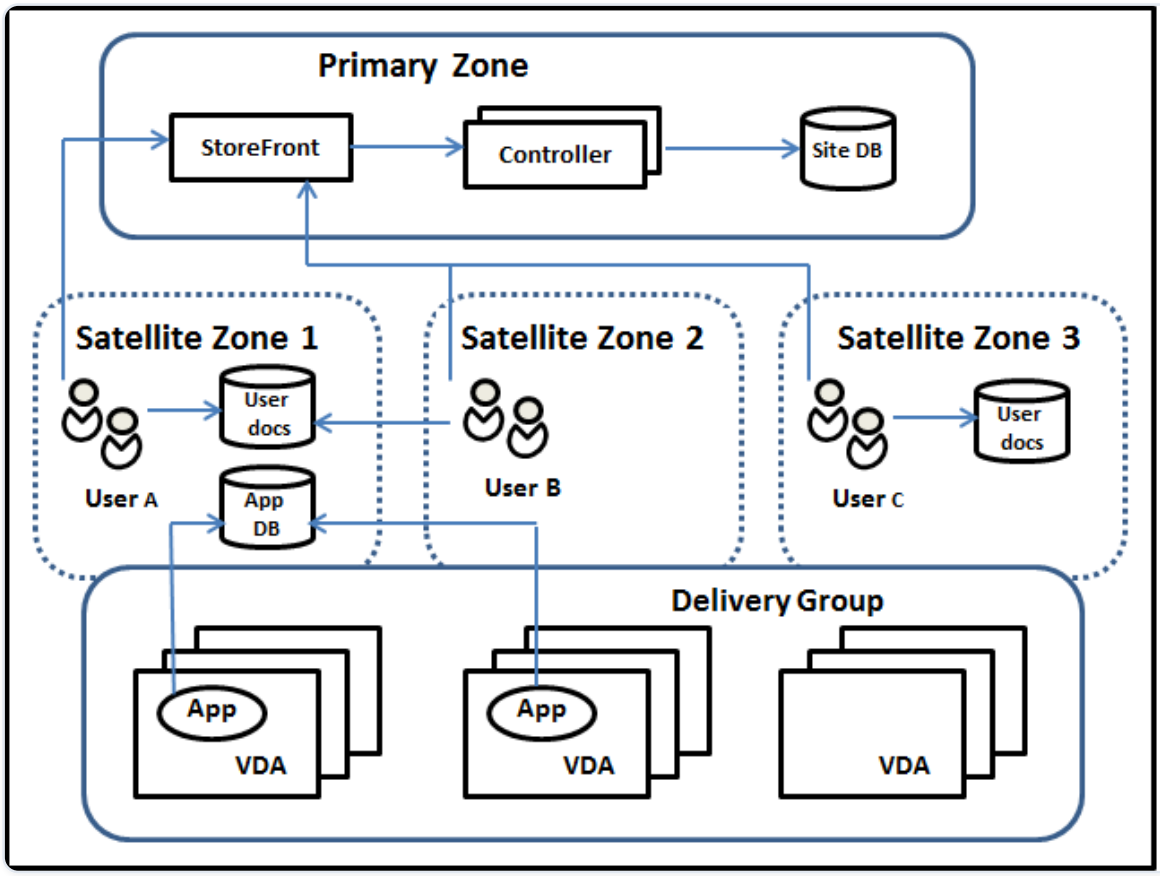
Em um site multi-zona, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou desktop.

Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma zona específica, com base em:

- Onde os dados do aplicativo são armazenados. Isso é chamado de home do aplicativo.
- O local dos dados home do usuário, como um perfil ou compartilhamento home. Isso é chamado de home do usuário.
- A localização atual do usuário (onde o aplicativo Citrix Workspace™ está sendo executado). Isso é referido como a localização do usuário.

O gráfico a seguir mostra um exemplo de configuração multizona.



Neste exemplo, os VDAs estão espalhados por três zonas satélite, mas todos estão no mesmo Grupo de Entrega. Portanto, o broker pode ter uma escolha de qual VDA usar para uma solicitação de inicialização do usuário. Este exemplo indica que existem vários locais onde os usuários podem estar executando seus endpoints do aplicativo Citrix Workspace:

- O Usuário A está usando um dispositivo com o aplicativo Citrix Workspace na zona satélite 1.
- O Usuário B está usando um dispositivo na zona satélite 2.
- Os documentos de um usuário podem ser armazenados em vários locais.
    - Os Usuários A e B usam um compartilhamento baseado na zona satélite 1.
    - O Usuário C usa um compartilhamento da zona satélite C.
    - Um dos aplicativos publicados usa um banco de dados localizado na zona satélite 1.

Você associa um usuário ou aplicativo a uma zona configurando uma zona inicial para o usuário ou aplicativo. O broker no Delivery Controller™ então usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se houver recursos disponíveis. Você pode:

- Configure a zona home para um usuário adicionando um usuário a uma zona.
- Configure a zona inicial para um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona inicial por vez. (Uma exceção para usuários pode ocorrer quando várias associações de zona ocorrem devido à associação a grupos de usuários; consulte a seção "Outras considerações". No entanto, mesmo neste caso, o broker usa apenas uma zona inicial.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o broker seleciona apenas uma zona preferencial para um lançamento. A ordem de prioridade padrão para selecionar a zona preferencial é zona inicial do aplicativo \> zona inicial do usuário \> localização do usuário. Você pode restringir a sequência; consulte Personalizando a preferência de zona. Quando um usuário inicia um aplicativo:

- Se essa aplicação tiver uma associação de zona configurada (uma zona inicial da aplicação), então a zona preferencial é a zona inicial para essa aplicação.
- Se o aplicativo não tiver uma associação de zona configurada, mas o usuário tiver uma associação de zona configurada (uma zona inicial do usuário), então a zona preferencial é a zona inicial para esse usuário.
- Se nem o aplicativo nem o usuário tiverem uma associação de zona configurada, então a zona preferencial é a zona onde o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, uma seleção aleatória de VDA e zona é usada. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver zona preferencial, o balanceamento de carga é aplicado a todos os VDAs no Grupo de Entrega.

Personalizando a preferência de zona

Ao configurar (ou remover) uma zona inicial para um usuário ou um aplicativo, você também pode restringir ainda mais como a preferência de zona é usada.

- **Uso obrigatório da zona inicial do usuário:** Em um Grupo de Entrega, você pode especificar que as sessões sejam iniciadas na zona inicial do usuário (se configurada), sem failover para outra zona se a zona inicial não tiver recursos disponíveis. Essa restrição é útil quando você precisa evitar o risco de copiar perfis grandes ou arquivos de dados entre zonas. Em outras palavras, você preferiria negar o lançamento de uma sessão a lançar a sessão em uma zona diferente.
- **Uso obrigatório da zona inicial do aplicativo:** Da mesma forma, ao configurar uma zona inicial para um aplicativo, você pode indicar que o aplicativo seja iniciado apenas nessa zona, sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona inicial do aplicativo.

- **Nenhuma zona inicial de aplicativo e ignorar a zona inicial de usuário configurada:** Se você não especificar uma zona inicial para um aplicativo, também poderá indicar que nenhuma zona de usuário configurada seja considerada ao iniciar esse aplicativo. Por exemplo, você pode preferir que os usuários executem um aplicativo em um VDA próximo ao seu dispositivo, usando a preferência de zona de localização do usuário, mesmo que alguns usuários possam ter uma zona inicial diferente.

Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia uma aplicação ou desktop, o broker prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário que está iniciando um aplicativo ou desktop já tiver uma sessão adequada para o recurso que está sendo iniciado (por exemplo, que possa usar o compartilhamento de sessão para um aplicativo, ou uma sessão que já esteja executando o recurso que está sendo iniciado), mas essa sessão estiver sendo executada em um VDA em uma zona diferente da zona preferencial para o usuário/aplicativo, então o sistema poderá criar uma nova sessão. Isso satisfaz o lançamento na zona correta (se tiver capacidade disponível), antes de reconectar a uma sessão em uma zona menos preferencial para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não pode mais ser alcançada, a reconexão é permitida para sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem de desejabilidade para as sessões satisfazerem um lançamento é:

1. Reconectar a uma sessão existente na zona preferencial.
2. Reconectar a uma sessão desconectada existente em uma zona diferente da zona preferencial.
3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar a uma sessão conectada existente em uma zona diferente da zona preferencial.
5. Iniciar uma nova sessão em uma zona diferente da zona preferencial.

Outras considerações sobre a preferência de zona

- Se você configurar uma zona inicial para um grupo de usuários (como um grupo de segurança), os usuários desse grupo (por meio de associação direta ou indireta) serão associados à zona especificada. No entanto, um usuário pode ser membro de vários grupos de segurança e, portanto, pode ter uma zona inicial diferente configurada por meio de outra associação de grupo. Nesses casos, a determinação da zona inicial desse usuário pode ser ambígua.

Se um usuário tiver uma zona inicial configurada que não foi adquirida por meio de associação a grupo, essa zona será usada para preferência de zona. Quaisquer associações de zona adquiridas por meio de associação a grupo são ignoradas.

Se o usuário tiver várias associações de zona diferentes adquiridas exclusivamente por meio da associação a grupos, o broker escolherá aleatoriamente entre as zonas. Uma vez que o broker faça essa escolha, essa zona será usada para lançamentos de sessão subsequentes, até que a associação a grupos do usuário mude.

- A preferência de zona de localização do usuário requer a detecção do aplicativo Citrix Workspace no dispositivo de endpoint pelo Citrix Gateway através do qual esse dispositivo está se conectando. O Citrix Gateway deve ser configurado para associar intervalos de endereços IP a zonas específicas, e a identidade da zona descoberta deve ser passada através do StoreFront para o Controller.

Para obter mais informações sobre a preferência de zona, consulte Detalhes internos da preferência de zona.

Considerações, requisitos e melhores práticas

- Você pode colocar os seguintes itens em uma zona: Controllers, catálogos de máquinas, conexões de host, usuários e aplicativos. Se um catálogo usar uma conexão de host, certifique-se de que o catálogo e a conexão estejam na mesma zona. (No entanto, com uma conexão de baixa latência e alta largura de banda disponível, eles podem estar em zonas diferentes.)
- Quando você coloca itens em uma zona satélite, isso afeta como o site interage com eles e com outros objetos relacionados a eles.
    - Quando os Controllers são colocados em uma zona satélite, presume-se que essas máquinas tenham boa conectividade (local) com hipervisores e VDAs na mesma zona. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária para lidar com esses hipervisores e máquinas VDA.
    - Quando uma conexão de hipervisor é colocada em uma zona satélite, presume-se que todos os hipervisores gerenciados por meio dessa conexão de hipervisor também residam nessa zona satélite. Os Controllers nessa zona satélite são então usados em preferência aos Controllers na zona primária ao se comunicar com essa conexão de hipervisor.
    - Quando um catálogo de máquinas é colocado em uma zona satélite, presume-se que todas as máquinas VDA nesse catálogo estejam na zona satélite. Os Controllers locais são usados em preferência aos Controllers na zona primária ao tentar se registrar no site,

depois que o mecanismo de atualização automática da lista de Controllers for ativado após o primeiro registro de cada VDA.

- As instâncias do Citrix Gateway também podem ser associadas a zonas. Isso é feito como parte da configuração de Roteamento HDX™ Otimizado do StoreFront, e não, como para os outros elementos descritos aqui, como parte da configuração do site. Quando um Citrix Gateway é associado a uma zona, ele é preferencialmente usado quando conexões HDX para máquinas VDA nessa zona são utilizadas.

- Ao criar um site de produção e, em seguida, criar o primeiro catálogo e Grupo de Entrega, todos os itens estão na zona primária – você não pode criar zonas satélite até concluir essa configuração inicial. (Se você criar um site vazio, a zona primária conterá inicialmente apenas um Controller. Você pode criar zonas satélite antes ou depois de criar um catálogo e um Grupo de Entrega.)
- Ao criar a primeira zona satélite contendo um ou mais itens, todos os outros itens em seu site permanecem na zona primária.
- A zona primária é nomeada 'Primary' por padrão; você pode alterar esse nome. Embora o Web Studio indique qual zona é a zona primária, é uma boa prática usar um nome facilmente identificável para a zona primária. Você pode reatribuir a zona primária (ou seja, tornar outra zona a zona primária), mas ela deve sempre conter o banco de dados do site e quaisquer servidores de alta disponibilidade.
- Sempre mantenha o banco de dados do site na zona primária.
- Depois de criar uma zona, você pode mover itens de uma zona para outra. Essa flexibilidade permite que você separe itens que funcionam melhor em proximidade. Por exemplo, mover um catálogo para uma zona diferente da conexão (host) que cria as máquinas no catálogo pode afetar o desempenho. Considere os possíveis efeitos não intencionais antes de mover itens entre zonas. Mantenha um catálogo e a conexão de host que ele usa na mesma zona, ou em zonas que estejam bem conectadas (por exemplo, via uma rede de baixa latência e alta largura de banda).
- Para um desempenho ideal, instale o Web Studio e o Director apenas na zona primária. Você pode acessar o Web Studio e o Director de uma zona satélite (por exemplo, uma zona satélite contendo Controllers para usar como failover se a zona primária se tornar inacessível) porque eles são aplicativos web.
- Idealmente, o Citrix Gateway em uma zona satélite é usado para conexões de usuário que chegam a essa zona de outras zonas ou locais externos, embora você possa usá-lo para conexões dentro da zona.

- Lembre-se: Para usar o recurso de preferência de zona, você deve estar usando no mínimo StoreFront 3.7 e Citrix Gateway 11.0-65.x.

Limites de qualidade da conexão

Os Controllers na zona satélite realizam interações SQL diretamente com o banco de dados do site. Isso impõe alguns limites à qualidade do link entre a zona satélite e a zona primária que contém o banco de dados do site. Os limites específicos são relativos ao número de VDAs e sessões de usuário nesses VDAs que são implantados na zona satélite. Assim, zonas satélite com apenas alguns VDAs e sessões podem funcionar com uma conexão de qualidade inferior ao banco de dados do que zonas satélite com um grande número de VDAs e sessões.

Para obter mais informações, consulte Melhorias na Latência e na Consulta de Bloqueio SQL.

O impacto da latência no desempenho do brokering

Embora as zonas permitam que os usuários estejam em links de maior latência, desde que haja um broker local, a latência adicional impacta inevitavelmente a experiência do usuário final. Para a maioria do trabalho que os usuários realizam, eles experimentam lentidão causada por viagens de ida e volta entre os Controllers na zona satélite e o banco de dados do site.

Para o lançamento de aplicativos, ocorrem atrasos extras enquanto o processo de brokering de sessão identifica VDAs adequados para enviar solicitações de lançamento de sessão.

Criar e gerenciar zonas

Um Administrador Completo pode realizar todas as tarefas de criação e gerenciamento de zonas. No entanto, você também pode criar uma função personalizada que permite criar, editar ou excluir uma zona. Mover itens entre zonas não requer permissões relacionadas à zona (exceto permissão de leitura da zona); no entanto, você deve ter permissão de edição para os itens que está movendo. Por exemplo, para mover um catálogo de uma zona para outra, você deve ter permissão de edição para esse catálogo. Para obter mais informações, consulte Administração delegada.

Se você usa Citrix Provisioning™: O console do Citrix Provisioning não reconhece zonas, por isso recomendamos usar o Web Studio para criar catálogos para zonas satélite. Crie o catálogo no Web Studio, especificando a zona satélite correta. Em seguida, use o console do Citrix Provisioning para provisionar máquinas nesse catálogo. (Se você criar o catálogo usando o assistente do Citrix Provisioning, o catálogo será colocado na zona primária. Você deve usar o Web Studio para movê-lo para a zona satélite posteriormente.)

Criar uma zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione **Criar Zona** na barra de ações.
4. Insira um nome para a zona e uma descrição (opcional). O nome deve ser exclusivo dentro do site.
5. Selecione os itens a serem colocados na nova zona. Você pode filtrar ou pesquisar a lista de itens dos quais pode selecionar. Você também pode criar uma zona vazia; simplesmente não selecione nenhum item.
6. Clique em **Salvar**.

Como alternativa a este método, você pode selecionar um ou mais itens no Web Studio e, em seguida, selecionar **Criar Zona** na barra de ações.

Alterar o nome ou a descrição de uma zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel central e, em seguida, selecione **Editar Zona** na barra de ações.
4. Altere o nome da zona, a descrição ou ambos. Se você alterar o nome da zona primária, certifique-se de que a zona permaneça facilmente identificável como a zona primária.
5. Clique em **Salvar** ou **Aplicar**.

Mover itens de uma zona para outra zona

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel do meio e, em seguida, selecione um ou mais itens.
4. Arraste os itens para a zona de destino ou selecione **Mover Itens** na barra de ações e, em seguida, especifique para qual zona movê-los.

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 usa uma conexão de host com um hipervisor ou outro serviço, coloque o catálogo e a conexão na mesma zona. Caso contrário, o desempenho pode ser afetado. Se você mover um, mova o outro também.

Excluir uma zona

Uma zona deve estar vazia antes de poder ser excluída. Você não pode excluir a zona primária.

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo.
3. Selecione uma zona no painel central.
4. Selecione **Excluir Zona** na barra de ações. Se a zona não estiver vazia (contiver itens), será solicitado que você escolha a zona para onde esses itens serão movidos.
5. Confirme a exclusão.

Adicionar uma zona inicial para um usuário

Configurar uma zona inicial para um usuário também é conhecido como *adicionar um usuário a uma zona*.

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo e, em seguida, selecione uma zona no painel central.
3. Selecione **Adicionar Usuários à Zona** na barra de ações.
4. Na caixa de diálogo **Adicionar Usuários à Zona**, clique em **Adicionar** e, em seguida, selecione os usuários e grupos de usuários a serem adicionados à zona. Se você especificar usuários que já possuem uma zona inicial, uma mensagem oferece duas opções: **Sim** = adicionar apenas os usuários especificados que não possuem uma zona inicial; **Não** = retornar à caixa de diálogo de seleção de usuário.
5. Clique em **OK**.

Para usuários com uma zona inicial configurada, você pode exigir que as sessões sejam iniciadas apenas a partir de sua zona inicial:

1. Crie ou edite um grupo de entrega.
2. Na página **Usuários**, marque a caixa de seleção **As sessões devem ser iniciadas na zona inicial de um usuário, se configurado**.

Todas as sessões iniciadas por um usuário nesse grupo de entrega devem ser iniciadas a partir de máquinas na zona inicial desse usuário. Se um usuário no grupo de entrega não tiver uma zona inicial configurada, essa configuração não terá efeito.

Remover uma zona inicial para um usuário

Este procedimento também é conhecido como remover um usuário de uma zona.

1. Faça login no Web Studio.
2. Selecione **Zonas** no painel esquerdo e, em seguida, selecione uma zona no painel central.
3. Selecione **Remover Usuários da Zona** na barra de ações.
4. Na caixa de diálogo **Adicionar Usuários à Zona**, clique em **Remover** e, em seguida, selecione os usuários e grupos a serem removidos da zona. Esta ação remove os usuários apenas da zona; esses usuários permanecem nos grupos de entrega e grupos de aplicativos aos quais pertencem.
5. Confirme a remoção quando solicitado.

Gerenciar zonas iniciais para aplicativos

Configurar uma zona inicial para um aplicativo também é conhecido como adicionar um aplicativo a uma zona. Por padrão, em um ambiente multizona, um aplicativo não tem uma zona inicial.

A zona inicial de um aplicativo é especificada nas propriedades do aplicativo. Você pode configurar as propriedades do aplicativo ao adicionar o aplicativo a um grupo ou posteriormente.

- Ao criar um Grupo de Entrega, criar um Grupo de Aplicativos ou adicionar aplicativos a grupos existentes, selecione **Propriedades** na página **Aplicativos** do assistente.
- Para alterar as propriedades de um aplicativo depois que ele é adicionado, selecione **Aplicativos** no painel esquerdo. Selecione um aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo** na barra de ações.

Na página **Zonas** das propriedades/configurações do aplicativo:

- Se você quiser que o aplicativo tenha uma zona inicial:
  - Selecione o botão de opção **Usar a zona selecionada para decidir** e, em seguida, selecione a zona.
  - Se você quiser que o aplicativo seja iniciado apenas da zona selecionada (e não de qualquer outra zona), selecione a caixa de seleção abaixo da seleção de zona.
- Se você não quiser que o aplicativo tenha uma zona inicial:

- Selecione o botão de opção **Não configurar uma zona inicial**.
- Se você não quiser que o broker considere quaisquer zonas de usuário configuradas ao iniciar este aplicativo, marque a caixa de seleção abaixo do botão de opção. Neste caso, nem as zonas iniciais do aplicativo nem as do usuário são usadas para determinar onde iniciar este aplicativo.

Outras ações que incluem a especificação de zonas

Depois de criar pelo menos uma zona satélite, você pode especificar uma zona ao adicionar uma conexão de host ou criar um catálogo.

Normalmente, a zona primária é a padrão. Ao usar o Machine Creation Services™ para criar um catálogo, a zona configurada para a conexão do host é selecionada automaticamente.

Se o site não contiver zonas satélite, a zona primária é assumida e a caixa de seleção de zona não aparece.

Monitor

Administradores e pessoal de suporte podem monitorar Sites do Citrix Virtual Apps and Desktops™ usando uma variedade de recursos e ferramentas. Usando essas ferramentas, você pode monitorar:

- Sessões de usuário e uso da sessão
- Desempenho de logon
- Conexões e máquinas, incluindo falhas
- Avaliação de carga
- Tendências históricas
- Infraestrutura

Citrix Director

O Director é uma ferramenta web em tempo real que você pode usar para monitorar e solucionar problemas, e para realizar tarefas de suporte para usuários finais.

Para obter detalhes, consulte os artigos do Director.

Registro de Configuração

O Registro de Configuração permite que os administradores acompanhem as alterações administrativas em um Site. O Registro de Configuração pode ajudar os administradores a diagnosticar e solucionar problemas após a realização de alterações de configuração, auxiliar no gerenciamento de mudanças e rastrear configurações, e relatar a atividade de administração.

Você pode visualizar e gerar relatórios sobre informações registradas no Studio. Você também pode visualizar itens registrados no Director com a Visualização de Tendências para fornecer notificações de alterações de configuração. Este recurso é útil para administradores que não têm acesso ao Studio.

A Visualização de Tendências fornece dados históricos de alterações de configuração ao longo de um período de tempo para que os administradores possam avaliar quais alterações foram feitas

no Site, quando foram feitas e quem as fez para encontrar a causa de um problema. Esta visualização classifica as informações de configuração em três categorias:

- Falhas de Conexão
- Máquinas de sessão única com falha
- Máquinas multissessão com falha

Para obter detalhes sobre como habilitar e configurar o Registro de Configuração, consulte Registro de Configuração. Os artigos do Director descrevem como visualizar as informações registradas a partir dessa ferramenta.

Logs de eventos

Os serviços no Citrix Virtual Apps and Desktops registram os eventos que ocorrem. Os logs de eventos são usados para monitorar e solucionar problemas de operações.

Para obter detalhes, consulte Logs de eventos. Artigos de recursos individuais também podem conter informações de eventos.

Registro de configuração

O registro de configuração é um recurso que captura alterações de configuração do site e atividades administrativas para o banco de dados. O recurso é habilitado por padrão. Você pode usar o conteúdo registrado para:

- Diagnosticar e solucionar problemas depois que as alterações de configuração são feitas. O log fornece um rastro de navegação.
- Auxiliar o gerenciamento de mudanças e rastrear configurações.
- Relatar a atividade de administração.

Você define as preferências de registro de configuração, exibe logs de configuração e gera relatórios HTML e CSV do Citrix Studio. Você pode filtrar as exibições do log de configuração por intervalos de datas e resultados de pesquisa de texto completo. O registro obrigatório, quando habilitado, impede que alterações de configuração sejam feitas, a menos que possam ser registradas. Com a permissão apropriada, você pode excluir entradas do log de configuração. Você não pode usar o recurso de registro de configuração para editar o conteúdo do log.

O registro de configuração usa um SDK do PowerShell e o Serviço de Registro de Configuração. O Serviço de Registro de Configuração é executado em cada Controller no site. Se um Controller falhar, o serviço em outro Controller lida automaticamente com as solicitações de registro.

Por padrão, o recurso de registro de configuração é habilitado e usa o banco de dados que é criado quando você cria o site (o banco de dados de configuração do site). Você pode especificar um local diferente para o banco de dados. O Banco de Dados de registro de configuração suporta os mesmos recursos de alta disponibilidade que o Banco de Dados de configuração do site.

O acesso ao registro de configuração é controlado por meio de administração delegada, com as permissões Editar Preferências de Registro e Visualizar Logs de Configuração.

Os logs de configuração são localizados quando são criados. Por exemplo, um log criado em inglês é lido em inglês, independentemente do local do leitor.

O que é registrado

Alterações de configuração e atividades administrativas iniciadas no Studio, Director e scripts do PowerShell são registradas. Exemplos de alterações de configuração registradas incluem trabalhar com (criar, editar, excluir, atribuir):

- Catálogos de máquinas
- Grupos de entrega (incluindo a alteração das configurações de gerenciamento de energia)
- Funções e escopos de administrador
- Recursos e conexões de host
- Políticas Citrix via Studio

Exemplos de alterações administrativas registradas incluem:

- Gerenciamento de energia de uma máquina virtual ou de um desktop de usuário
- Studio ou Director enviando uma mensagem para um usuário

As seguintes operações não são registradas:

- Operações autônomas, como o gerenciamento de pool de inicialização de máquinas virtuais.
- Ações de política implementadas através do Console de Gerenciamento de Política de Grupo (GPMC); use ferramentas da Microsoft para visualizar os logs dessas ações.
- Alterações feitas através do registro, acesso direto ao banco de dados ou de fontes diferentes de Studio, Director ou PowerShell.
- Quando a implantação é inicializada, o registro de configuração fica disponível quando a primeira instância do Serviço de Registro de Configuração se registra no Serviço de Configuração. Portanto, os estágios iniciais da configuração não são registrados (por exemplo,

quando o esquema do banco de dados é obtido e aplicado, quando um hipervisor é inicializado).

Gerenciar o registro de configuração

Por padrão, o registro de configuração usa o banco de dados criado ao criar um site (também conhecido como banco de dados de configuração do site). A Citrix recomenda que você use um local separado para o banco de dados de registro de configuração (e o banco de dados de monitoramento) pelos seguintes motivos:

- A estratégia de backup para o banco de dados de registro de configuração provavelmente será diferente da estratégia de backup para o banco de dados de configuração do site.
- O volume de dados coletados para o registro de configuração (e o Serviço de Monitoramento) pode afetar negativamente o espaço disponível para o banco de dados de configuração do site.
- Isso divide o ponto único de falha para os três bancos de dados.

As edições do produto que não suportam o registro de configuração não possuem um nó de Registro no Studio.

Habilitar e desabilitar o registro de configuração e o registro obrigatório

Por padrão, o registro de configuração está ativado e o registro obrigatório está desativado.

1. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
2. Selecione **Preferências** na barra de ações. A caixa de diálogo de registro de configuração contém informações do banco de dados e indica se o registro de configuração e o registro obrigatório estão ativados ou desativados.
3. Selecione a ação desejada:

   Para ativar o registro de configuração, selecione **Ativar**. Esta é a configuração padrão. Se não for possível gravar no banco de dados, as informações de registro serão descartadas, mas a operação continuará.

   Para desativar o registro de configuração, selecione **Desativar**. Se o registro estava ativado anteriormente, os logs existentes permanecem legíveis com o SDK do PowerShell.

   Para ativar o registro obrigatório, selecione **Impedir alterações na configuração do site quando o banco de dados não estiver disponível**. Nenhuma alteração de configuração ou atividade administrativa que normalmente é registrada é permitida, a menos que possa ser

gravada no banco de dados de registro de configuração. Você pode ativar o registro obrigatório somente quando o registro de configuração estiver ativado (quando **Ativar** estiver selecionado). Se o Serviço de Registro de Configuração falhar e a alta disponibilidade não estiver em uso, o registro obrigatório será assumido. Nesses casos, as operações que normalmente seriam registradas não são executadas.

Para desativar o registro obrigatório, selecione **Permitir alterações na configuração do site quando o banco de dados não estiver disponível**. Alterações de configuração e atividades administrativas são permitidas, mesmo que o banco de dados de registro de configuração não possa ser acessado. Esta é a configuração padrão.

Alterar o local do banco de dados de registro de configuração

Não é possível alterar o local do banco de dados quando o registro obrigatório está ativado, porque a alteração de local inclui um breve intervalo de desconexão que não pode ser registrado.

1. Crie um servidor de banco de dados, usando uma versão compatível do SQL Server.
2. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
3. Selecione **Preferências** na barra de ações.
4. Na caixa de diálogo Preferências de Registro, selecione **Alterar banco de dados de registro**.
5. Na caixa de diálogo Alterar Banco de Dados de Registro, especifique o local do servidor que contém o novo servidor de banco de dados. Consulte Formatos de endereço de banco de dados para formatos válidos.
6. Para permitir que o Studio crie o banco de dados, clique em **OK**. Quando solicitado, clique em **OK**, e ele será criado automaticamente. O Studio tenta acessar o banco de dados usando as credenciais do usuário atual do Studio. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. O Studio então carrega o esquema do banco de dados para o mesmo. (As credenciais são retidas apenas durante a criação do banco de dados.)
7. Para criar o banco de dados manualmente, clique em **Gerar script de banco de dados**. O script gerado inclui instruções para criar o banco de dados manualmente. Certifique-se de que o banco de dados esteja vazio e que pelo menos um usuário tenha permissão para acessar e alterar o banco de dados antes de carregar o esquema.

Os dados de log de configuração no banco de dados anterior não são importados para o novo banco de dados. Os logs não podem ser agregados de ambos os bancos de dados ao recuperar logs. A primeira entrada de log no novo banco de dados de log de configuração indica que uma alteração no banco de dados ocorreu, mas não identifica o banco de dados anterior.

Exibir conteúdo do log de configuração

Ao iniciar alterações de configuração e atividades administrativas, as operações de alto nível criadas pelo Studio e Director são listadas no painel superior central do Studio. Uma operação de alto nível resulta em uma ou mais chamadas de serviço e SDK, que são operações de baixo nível. Ao selecionar uma operação de alto nível no painel superior, o painel inferior exibe as operações de baixo nível.

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 terá um registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Ao exibir logs com base em intervalos de tempo, logs incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se todos os logs dos últimos cinco dias forem solicitados e um log existir com um horário de início nos últimos cinco dias, mas não tiver um horário de término, ele será incluído.

Ao usar um script que chama cmdlets do PowerShell, se você criar uma operação de baixo nível sem especificar uma operação de alto nível pai, o log de configuração criará uma operação de alto nível substituta.

Para exibir o conteúdo do log de configuração, selecione **Registro** no painel de navegação do Studio. Por padrão, o painel central lista o conteúdo do log cronologicamente (entradas mais recentes primeiro), separado por data. Você pode:

- Classificar a exibição pelo cabeçalho da coluna.
- Filtrar a exibição especificando um intervalo de dias ou inserindo texto na caixa **Pesquisar**. Para retornar à exibição padrão após usar a pesquisa, limpe o texto na caixa **Pesquisar**.
- Escolha quais colunas aparecem na exibição selecionando o ícone **Colunas a Exibir** no canto superior direito da tabela. Por exemplo, para visualizar o endereço IP que o administrador usa para acessar o Web Studio, clique no ícone e adicione a coluna **IP do Cliente**.

Gerar relatórios

Você pode gerar relatórios CSV e HTML contendo dados de log de configuração.

- O relatório CSV contém todos os dados de log de um intervalo de tempo especificado. Os dados hierárquicos no banco de dados são nivelados em uma única tabela CSV. Nenhum aspecto dos dados tem precedência no arquivo. Nenhuma formatação é usada e nenhuma legibilidade humana é assumida. O arquivo (nomeado MyReport) contém os dados em um formato universalmente consumível. Arquivos CSV são frequentemente usados para arquivar

dados ou como fonte de dados para uma ferramenta de relatório ou manipulação de dados, como o Microsoft Excel.

- O relatório HTML fornece uma forma legível por humanos dos dados de log para um intervalo de tempo especificado. Ele oferece uma visualização estruturada e navegável para revisar as alterações. Um relatório HTML é composto por dois arquivos, chamados Resumo e Detalhes. O Resumo lista as operações de alto nível: quando cada operação ocorreu, por quem e o resultado. Clicar em um link **Detalhes** ao lado de cada operação leva você às operações de baixo nível no arquivo Detalhes, que fornece informações adicionais.

Para gerar um relatório de log de configuração, selecione **Logging** no painel de navegação do Studio e, em seguida, selecione **Create custom report** na barra de ações.

- Selecione o intervalo de datas para o relatório.
- Selecione o formato do relatório: CSV, HTML ou ambos.
- Navegue até o local onde você deseja salvar o relatório.

Excluir conteúdo do log de configuração

Para excluir o log de configuração, você deve ter certas permissões de administração delegada e de banco de dados do SQL Server.

- **Administração delegada:** Você deve ter uma função de administração delegada que permita a leitura da configuração da implantação. A função de administrador completo tem essa permissão. Uma função personalizada deve ter Somente leitura ou Gerenciar selecionado na categoria Outras permissões.

  Para criar um backup dos dados de log de configuração antes de excluí-los, a função personalizada também deve ter Somente leitura ou Gerenciar selecionado na categoria Permissões de log.
- **Banco de dados SQL Server:** Você deve ter um login de servidor SQL com permissão para excluir registros do banco de dados. Existem duas maneiras de fazer isso:
  - Use um login de banco de dados do SQL Server com uma função de servidor sysadmin, que permite realizar qualquer atividade no servidor de banco de dados. Alternativamente, as funções de servidor `serveradmin` ou `setupadmin` permitem que você execute operações de exclusão.
  - Se sua implantação exigir mais segurança, use um login de banco de dados não sysadmin mapeado para um usuário de banco de dados que tenha permissão para excluir registros do banco de dados.

a. No SQL Server Management Studio, crie um login do SQL Server com uma função de servidor diferente de 'sysadmin'.
b. Mapeie o login para um usuário no banco de dados. O SQL Server cria automaticamente um usuário no banco de dados com o mesmo nome do login.
c. Em Associação de função de banco de dados, especifique pelo menos um dos membros da função para o usuário do banco de dados: `ConfigurationLoggingSchema_ROLE` ou `dbowner`.

Para obter mais informações, consulte a documentação do SQL Server Management Studio.

Para excluir os logs de configuração:

1. Faça login no Web Studio e selecione **Registro** no painel esquerdo.
2. Selecione **Excluir logs** na barra de ações.
3. Você será perguntado se deseja criar um backup dos logs antes que eles sejam excluídos. Se você optar por criar um backup, navegue até o local onde o arquivo de backup será salvo. O backup é criado como um arquivo CSV.

Depois que os logs de configuração são limpos, a exclusão do log é a primeira atividade registrada no log vazio. Essa entrada fornece detalhes sobre quem excluiu os logs e quando.

Exibir logs de API e PowerShell

Para monitorar as solicitações de API feitas durante sua sessão atual, clique na guia **APIs**. Os logs de API são limpos depois que você sai do Web Studio.

Para visualizar os comandos do PowerShell correspondentes às ações da interface do usuário que você realizou durante o dia, clique na guia **PowerShell**.

Associar metadados a logs de configuração

Você pode anexar metadados aos logs de configuração associando um par `name-value` chamado `MetadataMap` aos registros de log.

> **Observação:**
>
> - Você só pode anexar metadados a objetos de operação de alto nível.

- Os metadados são associados aos registros existentes no momento da execução.

Definir os metadados

Execute o comando PowerShell `Set-LogHighLevelOperationMetadata` para associar um registro de log ao `MetadataMap`. `Set-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**: ID da operação de alto nível.
- **InputObject**: As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id` onde um objeto de operação de alto nível ou uma lista de objetos é passado para o comando PowerShell.
- **Name**: Nome da propriedade dos metadados a serem adicionados. A propriedade deve ser única para a operação de alto nível especificada. A propriedade não pode conter nenhum dos seguintes caracteres ()\/;:#.*?=<>|'".
- **Value**: Valor para a propriedade.
- **Map**: Dicionário de pares (nome, valor) para as propriedades. Esta é uma alternativa para definir os metadados usando os parâmetros `-Name` e `-Value`.

Por exemplo, para anexar os metadados a todos os registros de log de alto nível com Id 40, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

Para anexar os metadados ao registro de alto nível com o usuário `abc@example.com`, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

Recuperar usando os metadados

Execute os seguintes comandos PowerShell para usar os metadados associados para recuperar os registros de log:

- Pesquisar por chave e valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Pesquisar por valor qualquer chave:

```
Get-LogHighLevelOperation -Metadata "*:Value"
```

- Pesquisar por chave e qualquer valor:

```
Get-LogHighLevelOperation -Metadata "Key:*"
```

Remover os metadados

Execute o comando PowerShell `Remove-LogHighLevelOperationMetadata` para remover os metadados associados. `Remove-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**: ID da operação de alto nível.
- **InputObject**: As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id`` onde um objeto de operação de alto nível ou uma lista de objetos é passado para o comando PowerShell.
- **Nome**: Nome da propriedade dos metadados a serem removidos. Defina como $null para remover todos os metadados do objeto especificado.
- **Mapa**: Dicionário de pares (nome, valor) para as propriedades. Pode ser uma hashtable (criada com @{"name1" = "val1"; "name2" = "val2"}) ou um dicionário de strings (criado com new-object "System.Collections.Generic.Dictionary"). As propriedades cujos nomes correspondem às chaves no mapa são removidas.

Logs de eventos

Os artigos a seguir listam e descrevem eventos que podem ser registrados pelos serviços no Citrix Virtual Apps and Desktops.

Esta informação não é abrangente. Os leitores devem verificar artigos de recursos individuais para obter informações adicionais sobre eventos.

- Eventos do Citrix Broker Service
- Eventos do Citrix FMA Service SDK
- Eventos do Citrix Configuration Service
- Eventos do Citrix Delegated Administration Service

Director

O Director é um console de monitoramento e solução de problemas para Citrix Virtual Apps and Desktops.

Arquitetura do Director(/en-us/citrix-virtual-apps-desktops/2407/media/director-architecture.png)

O Director pode acessar:

- Dados em tempo real do Broker Agent usando um console unificado integrado com Analytics, Performance Manager e Network Inspector. As seguintes análises são fornecidas pelo Citrix ADM para identificar gargalos devido à rede em seu ambiente Citrix Virtual Apps™ ou Desktops:
  - Gerenciamento de desempenho para garantia de saúde e capacidade
  - Tendências históricas e análise de rede
- Dados históricos armazenados no banco de dados Monitor para acessar o banco de dados Configuration Logging.
- Dados ICA® do Citrix Gateway usando o Citrix ADM.
  - Obtenha visibilidade da experiência do usuário final para aplicativos virtuais, desktops e usuários para Citrix Virtual Apps ou Desktops.
  - Correlacione dados de rede com dados de aplicativos e métricas em tempo real para uma solução de problemas eficaz.
  - Integrar com a ferramenta de monitoramento Citrix Virtual Desktop 7 Director.

O Director usa um painel de solução de problemas que fornece monitoramento de saúde em tempo real e histórico do Site do Citrix Virtual Apps ou Desktops. Esse recurso permite que você veja falhas em tempo real, fornecendo uma ideia melhor do que os usuários finais estão experimentando.

Para obter mais informações sobre a compatibilidade dos recursos do Director com o Delivery Controller (DC), VDA e quaisquer outros componentes dependentes, consulte Matriz de compatibilidade de recursos.

Observação:

Com a divulgação das vulnerabilidades de canal lateral de execução especulativa Meltdown e Spectre, a Citrix recomenda que você instale patches de mitigação relevantes. Esses patches podem impactar o desempenho do SQL Server. Para obter mais informações, consulte o artigo de suporte da Microsoft, Proteja o SQL Server contra ataques às vulnerabilidades de canal lateral Spectre e Meltdown. A Citrix recomenda que você teste a escala e planeje suas cargas de trabalho antes de implementar os patches em seus ambientes de produção.

O Director é instalado por padrão como um site no Delivery Controller. Para pré-requisitos e outros detalhes, consulte a documentação de Requisitos do sistema para esta versão. Para informações específicas sobre a instalação e configuração do Director, consulte Instalar e configurar o Director.

Fazer logon no Director

O site do Director está em https ou `http://<Server FQDN>/Director`.

Se um dos Sites em uma implantação multi-site estiver inativo, o logon demorará um pouco mais enquanto tenta se conectar ao Site que está inativo.

Usar o Director com autenticação de cartão inteligente PIV

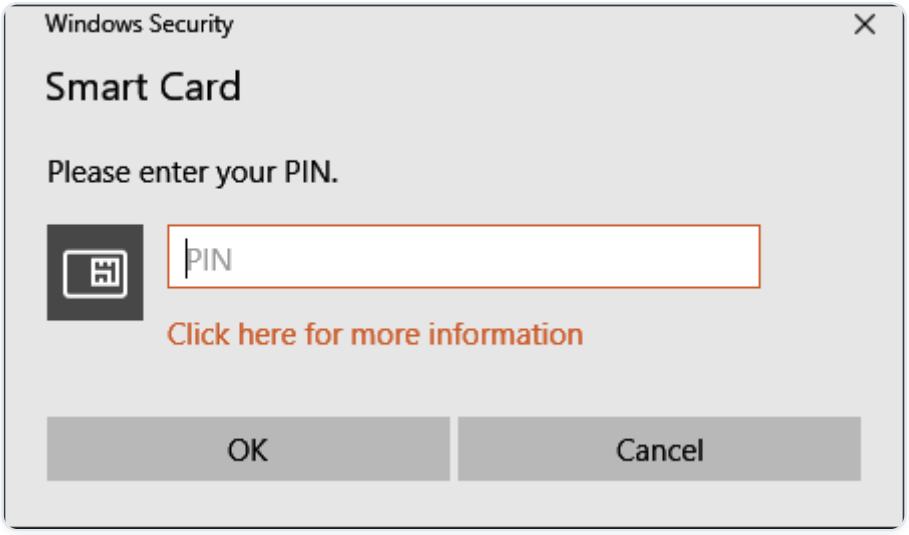
O Director agora oferece suporte à autenticação de cartão inteligente baseada em Verificação de Identidade Pessoal (PIV) para fazer logon. Este recurso é útil para organizações e agências governamentais que usam autenticação baseada em cartão inteligente para controle de acesso. A autenticação de cartão inteligente requer configuração específica no servidor Director e no Active Directory. As etapas de configuração são detalhadas em Configurar a autenticação de cartão inteligente PIV.

Observação:

A autenticação de cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

> Após realizar a configuração necessária, você pode fazer logon no Director usando um cartão inteligente:

1. Insira seu cartão inteligente no leitor de cartão inteligente.
2. Abra um navegador e vá para a URL do Director, `https://<directorfqdn>/Director`.
3. Selecione um certificado de usuário válido na lista exibida.
4. Insira seu token de cartão inteligente.



5. Após a autenticação, você pode acessar o Director sem digitar credenciais adicionais na página de logon do Director.

Usar o Director com Autenticação Integrada do Windows

Com a Autenticação Integrada do Windows (IWA), os usuários ingressados no domínio obtêm acesso direto ao Director sem precisar redigitar suas credenciais na página de logon do Director. Os pré-requisitos para trabalhar com a Autenticação Integrada do Windows e o Director são:

- Habilite a Autenticação Integrada do Windows no site do IIS que hospeda o Director. Ao instalar o Director, as Autenticações Anônima e de Formulários são habilitadas. Para oferecer suporte à Autenticação Integrada do Windows e ao Director, desative a Autenticação Anônima e ative a Autenticação do Windows. A Autenticação de Formulários deve permanecer definida como Habilitada para a autenticação de usuários não pertencentes ao domínio.

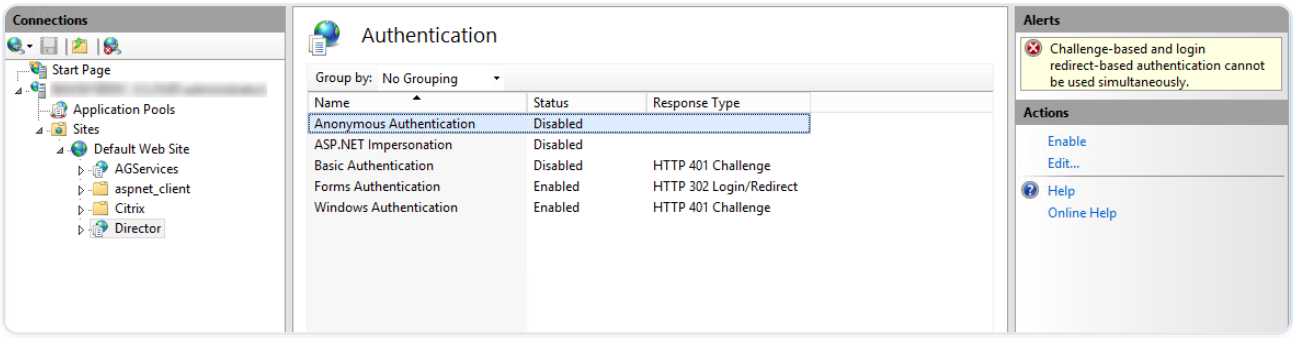
  a. Inicie o gerenciador do IIS.

  b. Vá para **Sites** \> **Default Web Site** \> **Director**.

  c. Selecione **Autenticação**.

  d. Clique com o botão direito em **Autenticação Anônima** e selecione **Desabilitar**.

e. Clique com o botão direito em **Autenticação do Windows** e selecione **Habilitar**.



- Configure a permissão de delegação do Active Directory para a máquina do Director. A configuração é necessária apenas se o Director e o Delivery Controller™ estiverem instalados em máquinas separadas.

  a. Na máquina do Active Directory, abra o Console de Gerenciamento do Active Directory.

  b. No Console de Gerenciamento do Active Directory, navegar até **Domain Name** \> **Computers.** Selecione a máquina do Director.

  c. Clique com o botão direito e selecione **Propriedades**.

  d. Em Propriedades, selecione a guia **Delegação**.

  e. Selecione a opção, **Confiar neste computador para delegação a qualquer serviço (somente Kerberos)**.

- O navegador usado para acessar o Director deve suportar a Autenticação Integrada do Windows. Etapas de configuração adicionais podem ser necessárias no Firefox e no Chrome. Para obter mais informações, consulte a documentação do navegador.
- O Serviço de Monitoramento deve estar executando o Microsoft .NET Framework 4.5.1 ou uma versão posterior compatível listada nos Requisitos do Sistema para o Director. Para obter mais informações, consulte Requisitos do Sistema.

Quando um usuário faz logoff do Director ou se a sessão expira, a página de logon é exibida. Na página de logon, o usuário pode definir o tipo de autenticação para **Logon automático** ou **Credenciais do usuário**.

Visualizações da interface

O Director oferece diferentes visualizações da interface adaptadas a administradores específicos. As permissões do produto determinam o que é exibido e os comandos disponíveis.

Por exemplo, os administradores de help desk veem uma interface adaptada às tarefas de help desk. O Director permite que os administradores de help desk pesquisem o usuário que relata um problema e exibam a atividade associada a esse usuário. Por exemplo, o status dos aplicativos e processos do usuário. Eles podem resolver problemas rapidamente executando ações como encerrar um aplicativo ou processo que não responde, sombrear operações na máquina do usuário, reiniciar a máquina ou redefinir o perfil do usuário.

Em contraste, os administradores completos veem e gerenciam todo o Site e podem executar comandos para vários usuários e máquinas. O Painel fornece uma visão geral dos principais aspectos de uma implantação, como o status das sessões, logons de usuários e a infraestrutura do Site. As informações são atualizadas a cada minuto. Se ocorrerem problemas, os detalhes sobre o número e o tipo de falhas que ocorreram aparecerão automaticamente.

Para obter mais informações sobre as várias funções e suas permissões no Director, consulte Administração Delegada e Director

Coleta de dados de uso pelo Pendo

O Serviço Director começa a usar o Pendo para coletar dados de uso após a instalação do Director. Estatísticas sobre o uso das páginas de Tendências e análises de chamadas da API OData são coletadas. A coleta de análises está em conformidade com a Política de Privacidade da Citrix. A coleta de dados é habilitada por padrão quando você instala o Director.

Para desativar a coleta de dados do Pendo, edite a chave do registro na máquina onde o Director está instalado. Se a chave do registro não existir, crie-a e defina-a para o valor desejado. Atualize a instância do Director após alterar o valor da chave do registro.

Cuidado: O uso incorreto do Editor do Registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

Local: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGoogleAnalytics

> **Observação:**

> Anteriormente, o Serviço Director usava o Google Analytics para coletar os dados. A mesma chave do registro agora é usada para o Pendo.

> Valor: 0 = ativado (padrão), 1 = desativado

Você pode usar o seguinte cmdlet do PowerShell para desabilitar a coleta de dados pelo Pendo:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

Guia de novos recursos

O Director possui um guia no produto que usa Pendo para fornecer informações sobre os novos recursos lançados na versão atual do Director. A visão geral rápida, juntamente com mensagens apropriadas no produto, ajuda você a entender as novidades do produto.

Para desativar este recurso, edite a chave do registro, conforme descrito abaixo, na máquina onde o Director está instalado. Se a chave do registro não existir, crie-a e defina-a para o valor desejado. Atualize a instância do Director após alterar o valor da chave do registro.

> **Cuidado:**

> O uso incorreto do Editor do Registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

> Local: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nome: DisableGuidedHelp

Valor: 0 = ativado (padrão), 1 = desativado

Você pode usar o seguinte cmdlet do PowerShell para desabilitar o guia no produto:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

Artigos de referência

- Reduzir o MTTR do Citrix Director
- Citrix Director - Gerenciar e configurar alertas e notificações com PowerShell
- Documentação do desenvolvedor do Citrix Virtual Apps and Desktops

Novidades em produtos relacionados

- Citrix DaaS
- StoreFront
- Acesso Privado Seguro
- Citrix Enterprise Browser
- Citrix Workspace
- Provisionamento

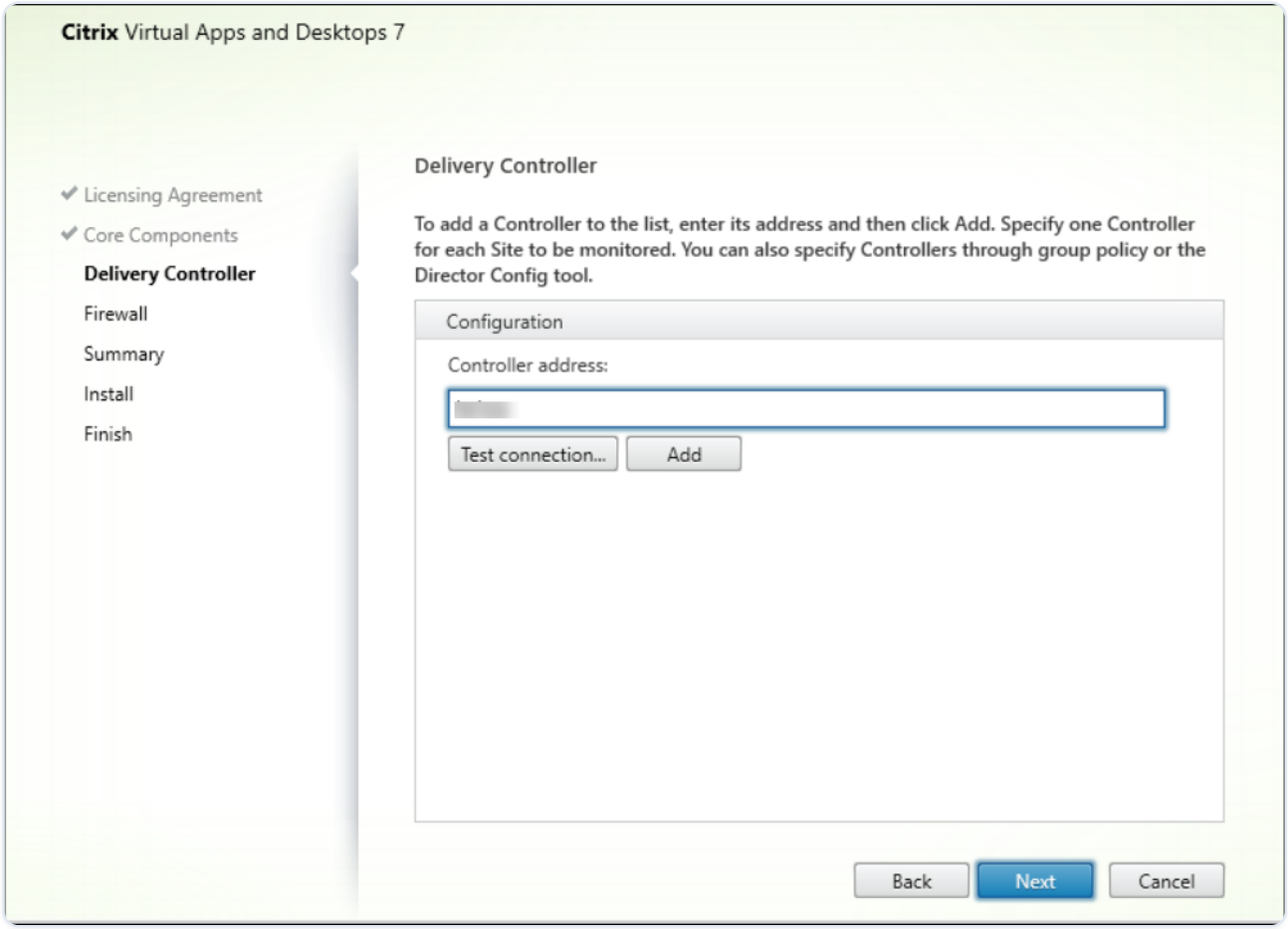
Instalar e configurar

Instalar o Director

Instale o Director usando o Instalador ISO completo do produto para Citrix Virtual Apps and Desktops, que verifica os pré-requisitos, instala quaisquer componentes ausentes, configura o site do Director e executa a configuração básica. Para pré-requisitos e outros detalhes, consulte a documentação de Requisitos do sistema para esta versão. Esta versão do Director não é compatível com implantações do Virtual Apps anteriores à 6.5 ou implantações do Virtual Desktops anteriores à 7. A configuração padrão fornecida pelo instalador ISO lida com implantações típicas. Se o Director não foi incluído durante a instalação, use o instalador ISO para adicionar o Director. Para adicionar quaisquer componentes adicionais, execute novamente o instalador ISO e selecione os componentes a serem instalados. Para obter informações sobre

como usar o instalador ISO, consulte Instalar componentes principais na documentação de instalação. A Citrix recomenda que você instale usando apenas o instalador ISO completo do produto, e não o arquivo .MSI.

Quando o Director é instalado no Controller, ele é configurado automaticamente com localhost como endereço do servidor, e o Director se comunica com o Controller local por padrão. Para instalar o Director em um servidor dedicado que esteja remoto de um Controller, você será solicitado a inserir o FQDN ou o endereço IP de um Controller.



Observação:

Clique em **Adicionar** para adicionar o Controller a ser monitorado.

O Director se comunica com o Controller especificado por padrão. Especifique apenas um endereço de Controller para cada site que você monitora. O Director descobre automaticamente todos os outros Controllers no mesmo site e recorre a esses outros Controllers se o Controller especificado falhar.

Observação:

O Director não faz balanceamento de carga entre os Controllers.

Para proteger as comunicações entre o navegador e o servidor Web, a Citrix® recomenda que você implemente TLS no site do IIS que hospeda o Director. Consulte a documentação do Microsoft IIS para obter instruções. A configuração do Director não é necessária para habilitar o TLS.

Implantar e configurar o Director

Quando o Director é usado em um ambiente que contém mais de um site, certifique-se de sincronizar os relógios do sistema em todos os servidores onde os Controllers, o Director e outros componentes principais estão instalados. Caso contrário, os sites podem não ser exibidos corretamente no Director.

Importante:

Para proteger a segurança de nomes de usuário e senhas enviados em texto simples pela rede, permita conexões do Director usando apenas HTTPS, e não HTTP. Certas ferramentas são capazes de ler nomes de usuário e senhas em texto simples em pacotes de rede HTTP (não criptografados), o que pode criar um risco potencial de segurança para os usuários.

Configurar permissões

Para fazer logon no Director, os administradores com permissões para o Director devem ser usuários de domínio do Active Directory e devem ter os seguintes direitos:

- Direitos de leitura em todas as florestas do Active Directory a serem pesquisadas (consulte Configuração avançada).
- Funções de Administrador Delegado configuradas (consulte administração delegada e Director).
- Para sombrear usuários, os administradores devem ser configurados usando uma política de grupo da Microsoft para Assistência Remota do Windows. Além disso:
    - Ao instalar VDAs, certifique-se de que o recurso Assistência Remota do Windows esteja habilitado em todos os dispositivos de usuário (selecionado por padrão).

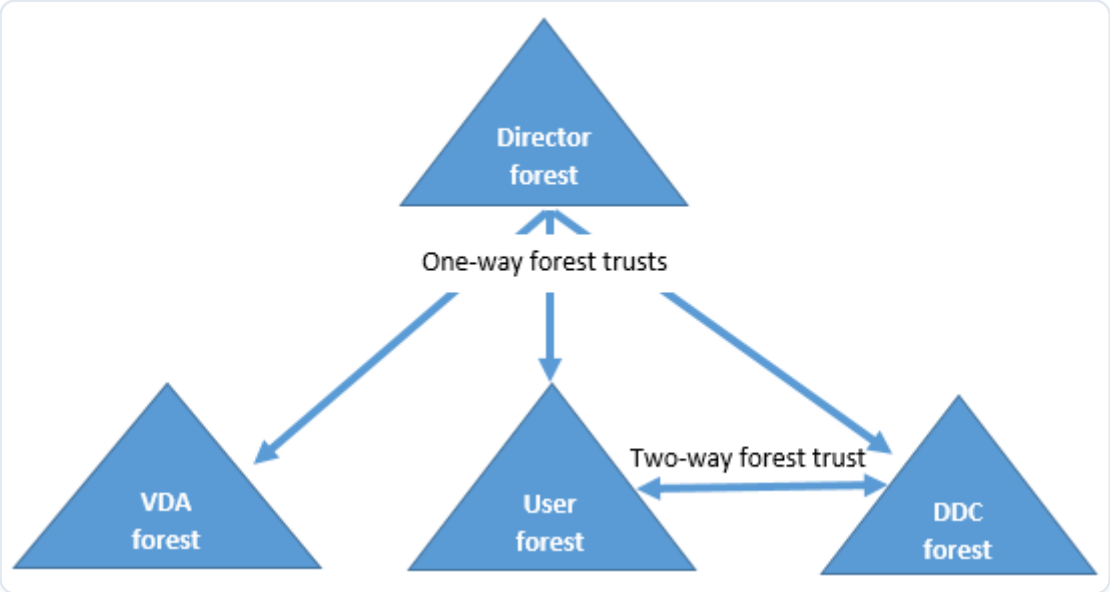
- Ao instalar o Director em um servidor, certifique-se de que a Assistência Remota do Windows esteja instalada (selecionada por padrão). No entanto, ela é desabilitada no servidor por padrão. O recurso não precisa ser habilitado para que o Director forneça assistência aos usuários finais. A Citrix recomenda deixar o recurso desabilitado para melhorar a segurança no servidor.
- Para permitir que os administradores iniciem a Assistência Remota do Windows, conceda a eles as permissões necessárias usando as configurações apropriadas da Política de Grupo da Microsoft para Assistência Remota. Para obter informações, consulte CTX127388: Como habilitar a Assistência Remota para o Desktop Director.

Configuração avançada

O Director pode suportar ambientes de múltiplas florestas abrangendo uma configuração de floresta onde usuários, Delivery Controllers (DCs), VDAs e Directors estão localizados em florestas diferentes. Isso requer uma configuração adequada de relações de confiança entre as florestas e configurações.

Configuração recomendada em um ambiente de múltiplas florestas

A configuração recomendada exige a criação de relações de confiança de floresta de saída e de entrada entre as florestas com autenticação em todo o domínio.



A relação de confiança do Director permite solucionar problemas em sessões de usuário, VDAs e Delivery Controllers localizados em florestas diferentes.

A configuração avançada necessária para o Director suportar múltiplas florestas é controlada por meio de configurações definidas no Gerenciador de Serviços de Informações da Internet (IIS).

> **Importante:**

> Ao alterar uma configuração no IIS, o serviço Director é reiniciado automaticamente e desconecta os usuários.

> Para configurar as configurações avançadas usando o IIS:

1. Abra o console do Gerenciador de Serviços de Informações da Internet (IIS).
2. Vá para o site do Director em site Padrão.
3. Clique duas vezes em **Application Settings**.
4. Clique duas vezes em uma configuração para editá-la.
5. Clique em **Adicionar** para adicionar uma nova configuração.

O Director usa o Active Directory para pesquisar usuários e para procurar mais informações de usuário e máquina. Por padrão, o Director pesquisa o domínio ou a floresta em que:

- A conta do administrador é um membro.
- O servidor web do Director é um membro (se diferente).

O Director tenta realizar pesquisas no nível da floresta usando o catálogo global do Active Directory. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

A pesquisa ou consulta de dados de outro domínio ou floresta do Active Directory exige que você defina explicitamente os domínios ou florestas a serem pesquisados. Configure a seguinte configuração de Aplicativos para o site do Director no Gerenciador do IIS:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Os atributos de valor user e server representam os domínios do usuário do Director (o administrador) e do servidor do Director, respectivamente.

Para habilitar pesquisas de um domínio ou floresta extra, adicione o nome do domínio à lista, conforme mostrado neste exemplo:

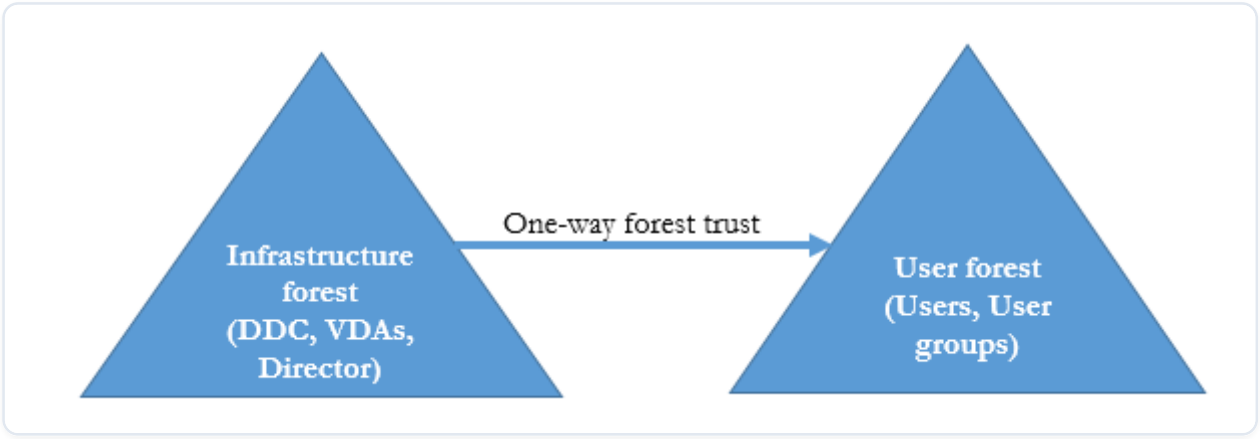
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

Para cada domínio na lista, o Director tenta realizar pesquisas no nível da floresta. Se você não tiver permissões para pesquisar no nível da floresta, apenas o domínio será pesquisado.

Configuração de grupo local de domínio

A maioria dos Provedores de Serviços Citrix (CSPs) tem configurações de ambiente semelhantes, consistindo em VDAs, DCs e Director na floresta de Infraestrutura. Os registros de usuários ou grupos de usuários pertencem à floresta do Cliente. Existe uma confiança de saída unidirecional da floresta de Infraestrutura para a floresta do Cliente.

Os administradores de CSP geralmente criam um grupo local de domínio na floresta de Infraestrutura e adicionam os usuários ou grupos de usuários da floresta do Cliente a este grupo local de domínio.



O Director pode suportar uma configuração multifloresta como esta e monitorar as sessões de usuários configurados usando grupos locais de domínio.

1. Adicione as seguintes configurações de Aplicativos ao site do Director no Gerenciador do IIS:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> são nomes das florestas nas quais o grupo local de domínio existe.

2. Atribua o grupo local de domínio a grupos de entrega no Web Studio.
3. Reinicie o IIS e faça login no Director novamente para que as alterações entrem em vigor. Agora, o Director pode monitorar e exibir as sessões desses usuários.

Adicionar sites ao Director

Se o Director já estiver instalado, configure-o para funcionar com vários sites. Para configurar, use o Console do Gerenciador do IIS em cada servidor do Director para atualizar a lista de endereços de servidor nas configurações do aplicativo.

Adicione um endereço de um Controller de cada site à seguinte configuração:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController e SiteBController são os endereços de Delivery Controllers de dois sites diferentes.

Desabilitar a visibilidade de aplicativos em execução no Gerenciador de Atividades

Por padrão, o Gerenciador de Atividades no Director exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Essas informações são visualizadas por todos os administradores que têm acesso ao recurso Gerenciador de Atividades no Director. Para funções de Administrador Delegado, isso inclui Administrador Completo, Administrador de grupo de entrega e Administrador de Help Desk.

Para proteger a privacidade dos usuários e dos aplicativos que eles estão executando, você pode desabilitar a guia **Aplicativos** para listar os aplicativos em execução.

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não garante que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

1. No VDA, modifique a chave do registro em `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`. Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, portanto, não são exibidas no Gerenciador de Atividades.
2. No servidor com o Director instalado, modifique a configuração que controla a visibilidade dos aplicativos em execução. Por padrão, o valor é "true", o que permite a visibilidade dos aplicativos em execução na guia Aplicativos. Altere o valor para "false", o que desabilita a

visibilidade. Esta opção afeta apenas o Gerenciador de Atividades no Director, não o VDA. Modifique o valor da seguinte configuração: UI.TaskManager.EnableApplications = false

Importante:

Para desabilitar a visualização de aplicativos em execução, faça ambas as alterações para garantir que os dados não sejam exibidos no Gerenciador de Atividades.

Configurar autenticação de cartão inteligente PIV

Este artigo lista a configuração necessária no Servidor Director e no Active Directory para habilitar o recurso de autenticação de cartão inteligente.

Observação:

A autenticação de cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

Configuração do servidor Director

Execute as seguintes etapas de configuração no servidor Director:

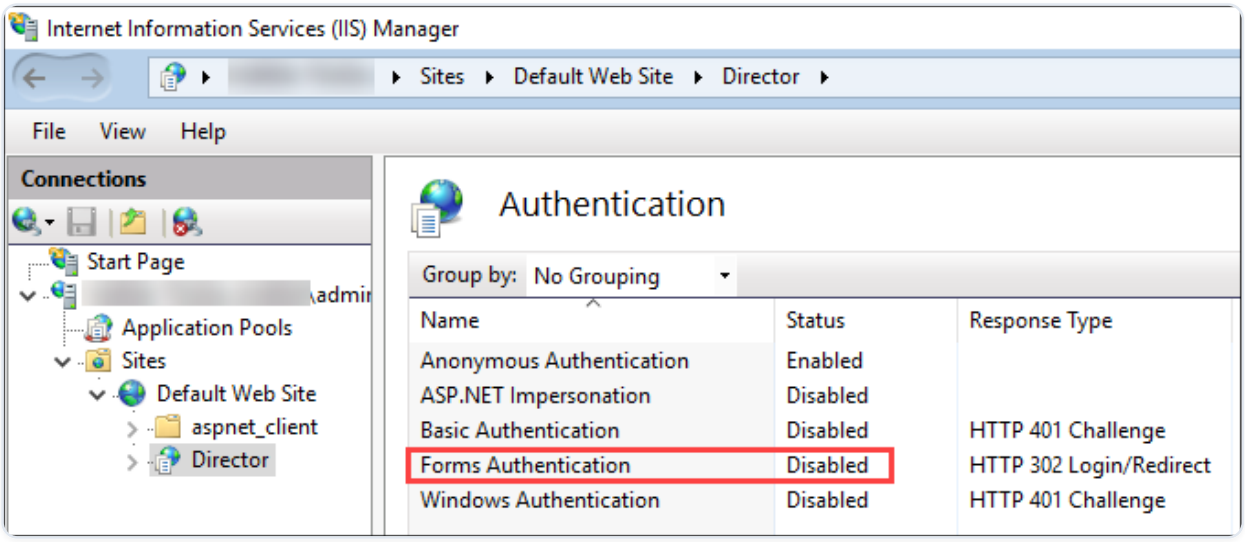
1. Instale e habilite a Autenticação de Mapeamento de Certificado de Cliente. Siga as instruções de **Autenticação de mapeamento de certificado de cliente usando o Active Directory** no documento da Microsoft, Autenticação de Mapeamento de Certificado de Cliente.
2. Desabilite a Autenticação de Formulários no site do Director.

   Inicie o Gerenciador do IIS.

   Vá para **Sites** \> **Default Web Site** \> **Director**.

   Selecione **Autenticação**.

   Clique com o botão direito em **Autenticação de Formulários** e selecione **Desabilitar.**



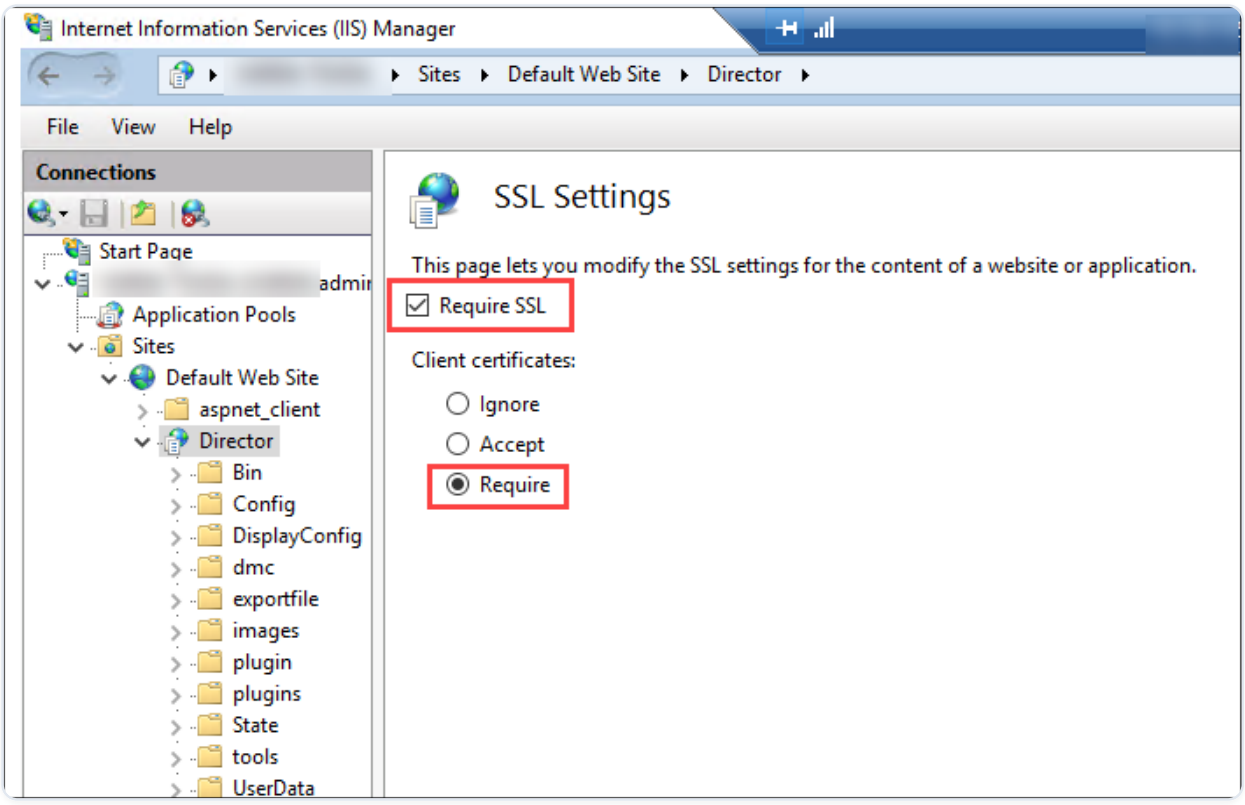
3. Configure a URL do Director para o protocolo https mais seguro (em vez de HTTP) para autenticação de certificado de cliente.

   a. Inicie o Gerenciador do IIS.

   b. Vá para **Sites** \> **Default Web Site** \> **Director**.

   c. Selecione **Configurações SSL.**

   d. Selecione **Exigir SSL** e **Certificados de cliente** \> **Exigir.**



4. Atualize web.config. Abra o arquivo web.config (disponível em `c:\inetpub\wwwroot\Director`) usando um editor de texto.

Sob o elemento pai `<system.webServer>`, adicione o seguinte trecho como o primeiro elemento filho:

```
&lt;defaultDocument&gt;

   &lt;files&gt;

       &lt;add value="LogOn.aspx"/&gt;

   &lt;/files&gt;

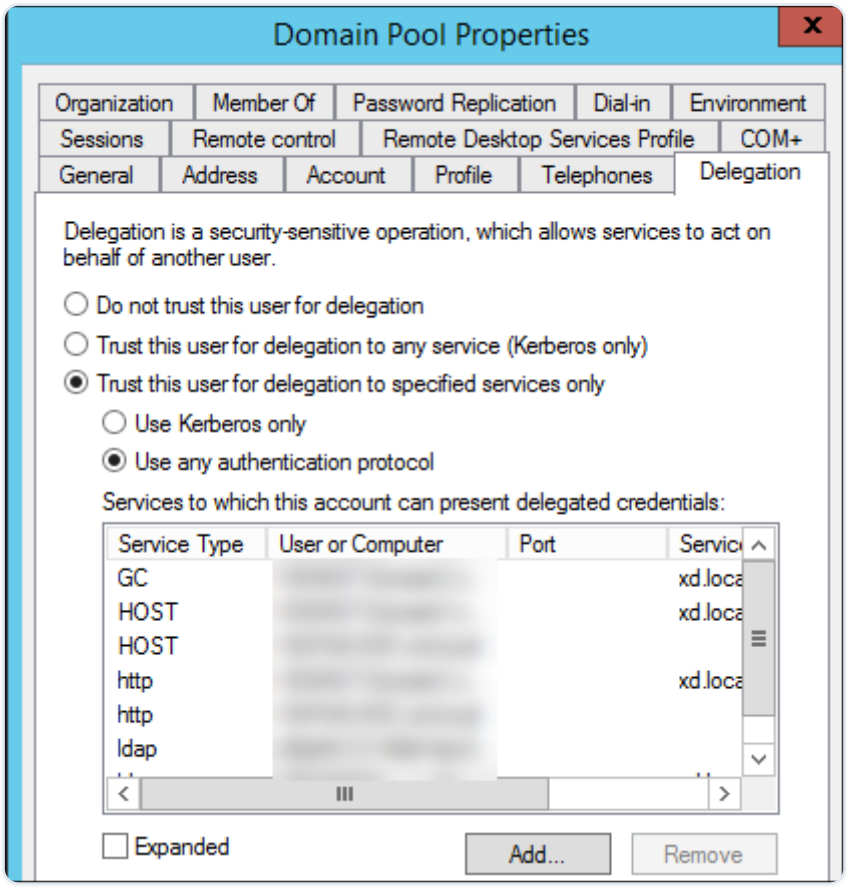
&lt;/defaultDocument&gt;
```

Configuração do Active Directory

Por padrão, o aplicativo Director é executado com a propriedade de identidade do **Application Pool**. A autenticação por cartão inteligente requer delegação para a qual a identidade do aplicativo Director deve ter privilégios de Trusted Computing Base (TCB) no host do serviço.

A Citrix recomenda que você crie uma conta de serviço separada para a identidade do Application Pool. Crie a conta de serviço e atribua privilégios TCB conforme as instruções no artigo da Microsoft MSDN, Protocol Transition with Constrained Delegation Technical Supplement.

Atribua a conta de serviço recém-criada ao pool de aplicativos do Director. A figura a seguir mostra a caixa de diálogo de propriedades de uma conta de serviço de exemplo, Domain Pool.

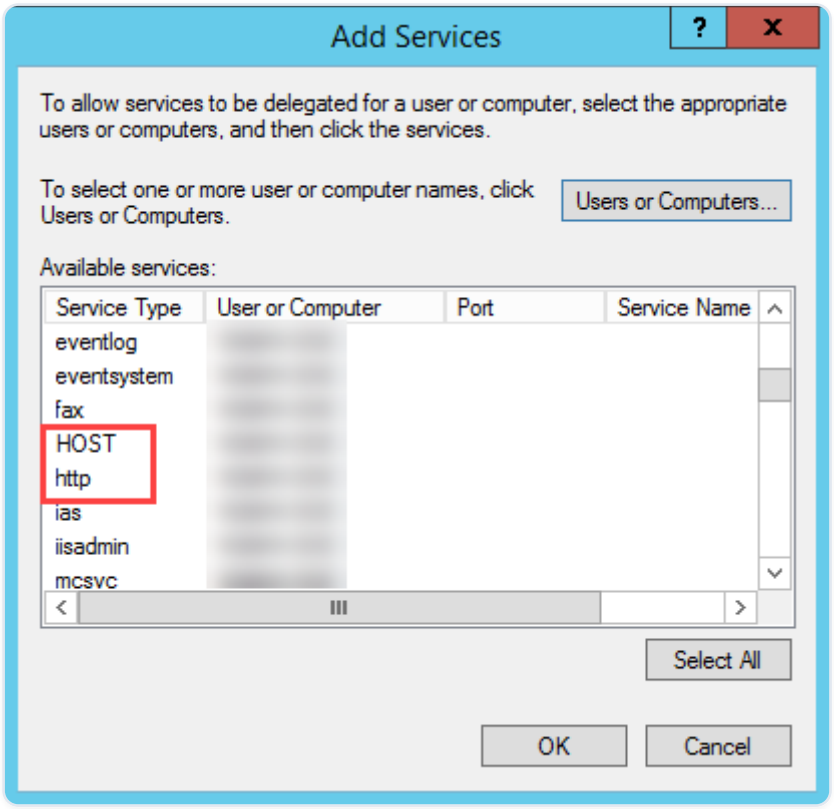


Configure os seguintes serviços para esta conta:

- Delivery Controller™: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

Para configurar,

1. Na caixa de diálogo de propriedades da conta de usuário, clique em **Adicionar.**
2. Na caixa de diálogo **Adicionar Serviços**, clique em Usuários ou Computadores.
3. Selecione o nome do host do Delivery Controller.
4. Na lista **Serviços disponíveis**, selecione HOST e **Tipo de Serviço** HTTP.



Da mesma forma, adicione Tipos de Serviço para os hosts do **Director** e do **Active Directory**.

Criar registros de Nome Principal de Serviço

Você deve criar uma conta de serviço para cada servidor Director e IPs Virtuais (VIP) com balanceamento de carga usados para acessar um pool de servidores Director. Você deve criar registros de nome principal de serviço (SPN) para configurar uma delegação para a conta de serviço recém-criada.

- Use o seguinte comando para criar um registro SPN para um servidor Director:

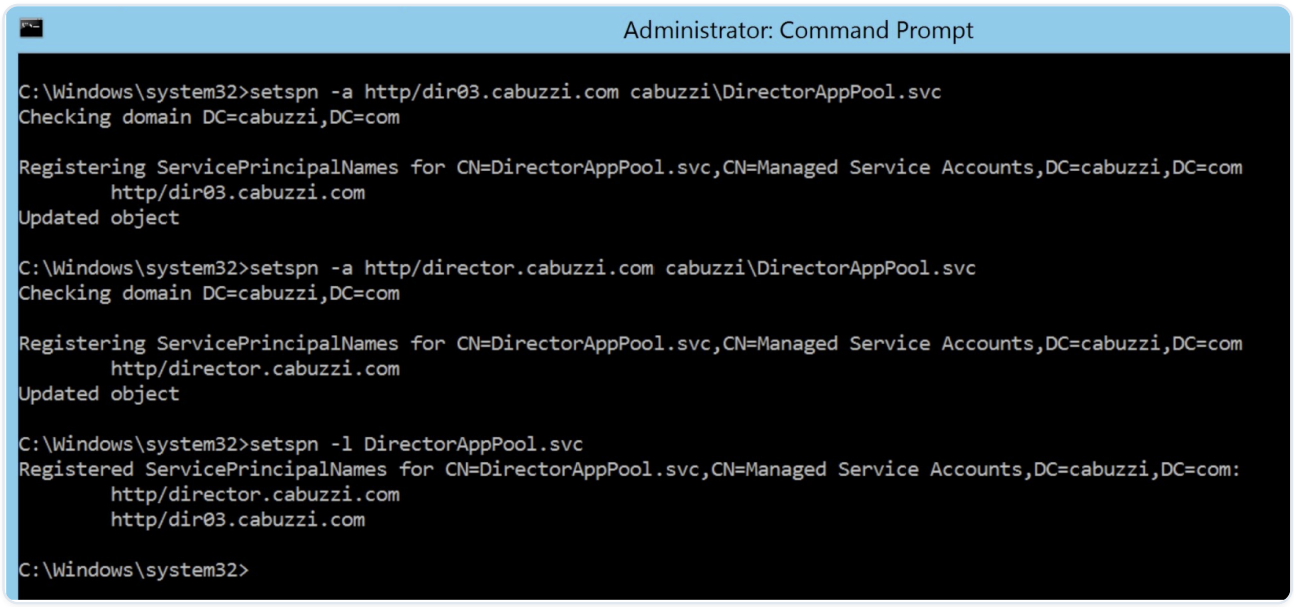
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- Use o seguinte comando para criar um registro SPN para um VIP com balanceamento de carga:

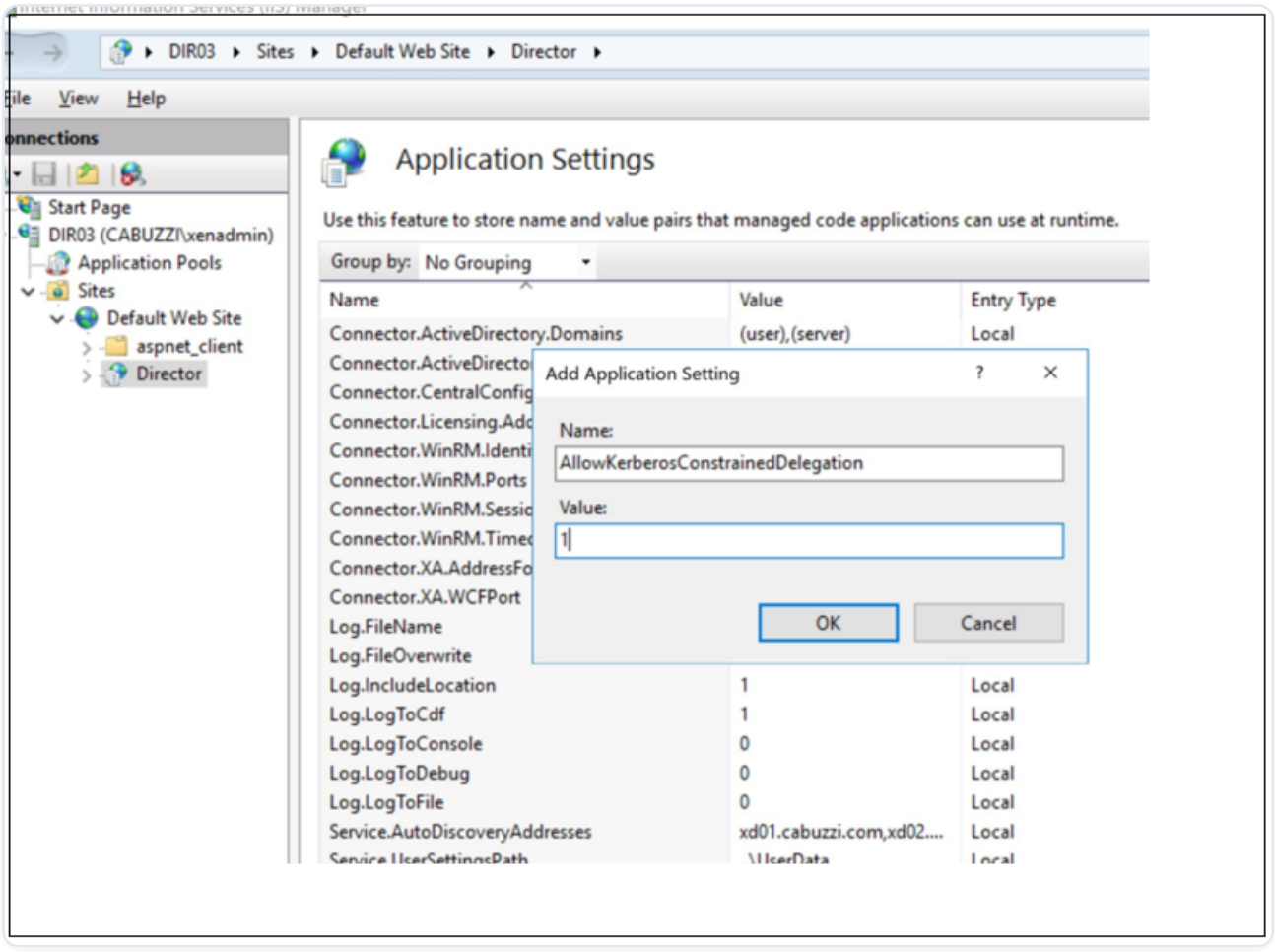
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- Use o seguinte comando para visualizar ou testar os SPNs criados:

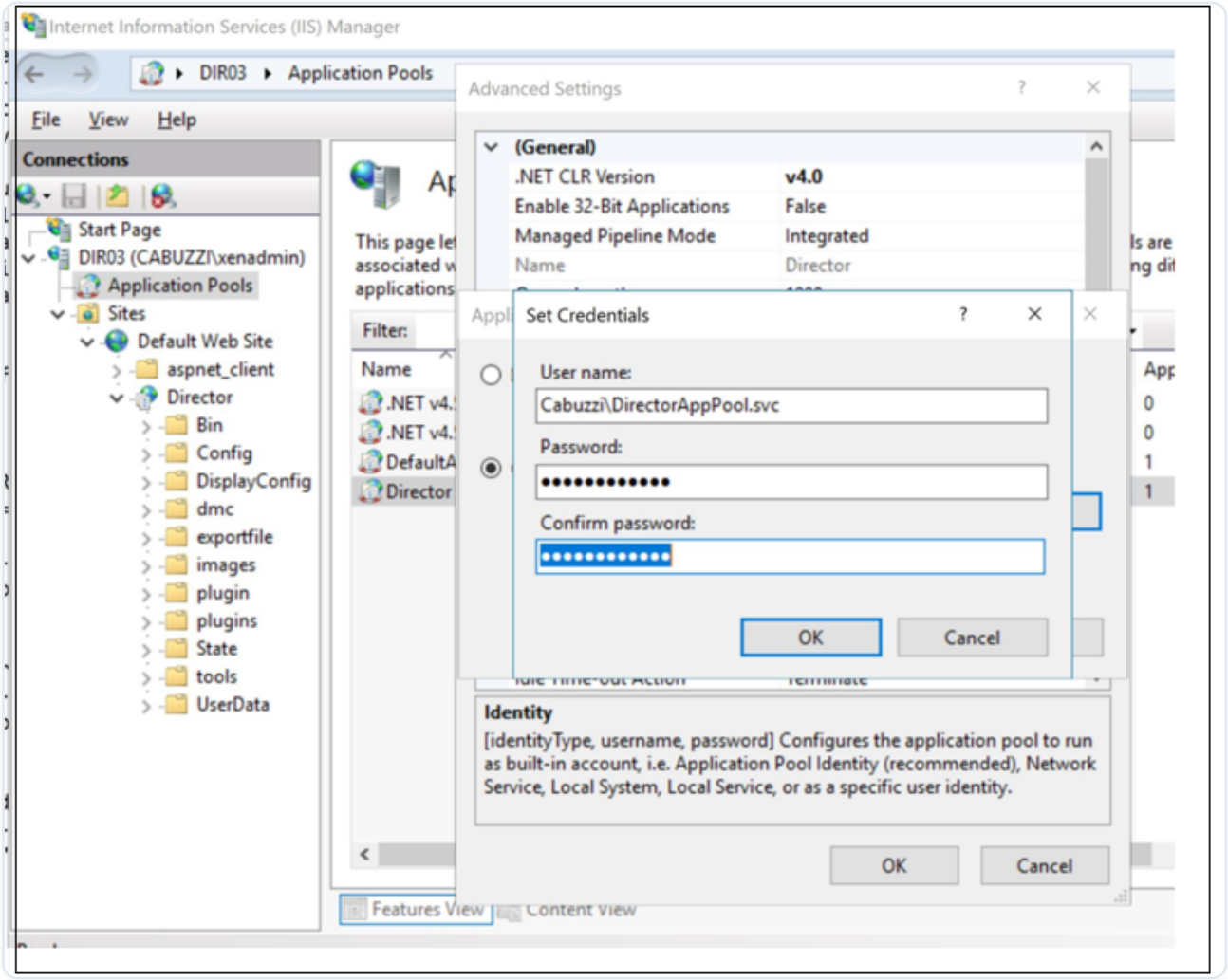
```
setspn –l <DirectorAppPoolServiceAcct>
```



- Selecione o diretório virtual do Director no painel esquerdo e clique duas vezes em **Application Settings**. Dentro da janela Application Settings, clique em **Adicionar** e certifique-se de que **AllowKerberosConstrainedDelegation** esteja definido como 1.



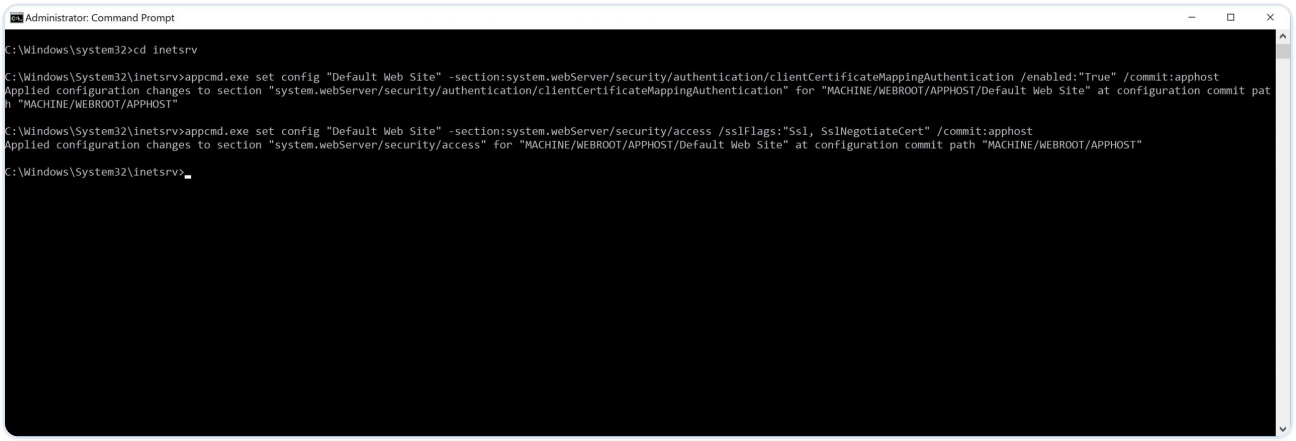
- Selecione **Application Pools** no painel esquerdo, clique com o botão direito do mouse no pool de aplicativos do Director e selecione **Advanced Settings**.
- Selecione **Identity**, clique nas reticências (“…”) para inserir as credenciais de domínio\logon e senha da conta de serviço. Feche o console do IIS.



- Em um prompt de comando elevado, altere o diretório para C:\Windows\System32\inetsrv e insira os seguintes comandos:

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Configuração do navegador Firefox

Para usar o navegador Firefox, instale o driver PIV disponível em OpenSC 0.17.0. Para obter instruções de instalação e configuração, consulte Installing OpenSC PKCS#11 Module in Firefox, Step by Step. Para obter informações sobre o uso do recurso de autenticação de cartão inteligente no Director, consulte a seção Use Director with PIV based smart card authentication no artigo do Director.

Configurar análise de rede

> **Nota:** A disponibilidade deste recurso depende da licença da sua organização e das suas permissões de administrador.

> O Director se integra ao Citrix ADM para fornecer análise de rede e gerenciamento de desempenho:

- A análise de rede usa relatórios HDX™ Insight do Citrix ADM para fornecer uma visão contextual da rede para aplicativos e desktops. Com esse recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação.
- O gerenciamento de desempenho oferece retenção histórica e relatórios de tendências. Com a retenção histórica de dados em comparação com a avaliação em tempo real, você pode criar relatórios de tendências, incluindo tendências de capacidade e integridade.

Depois de habilitar esse recurso no Director, os relatórios do HDX Insight fornecem ao Director informações adicionais:

- A guia Rede na página Tendências mostra os efeitos de latência e largura de banda para aplicativos, desktops e usuários em toda a sua implantação.
- A página Detalhes do Usuário mostra informações de latência e largura de banda específicas para uma sessão de usuário em particular.

Limitações:

- Na exibição Tendências, os dados de logon de conexão HDX não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.

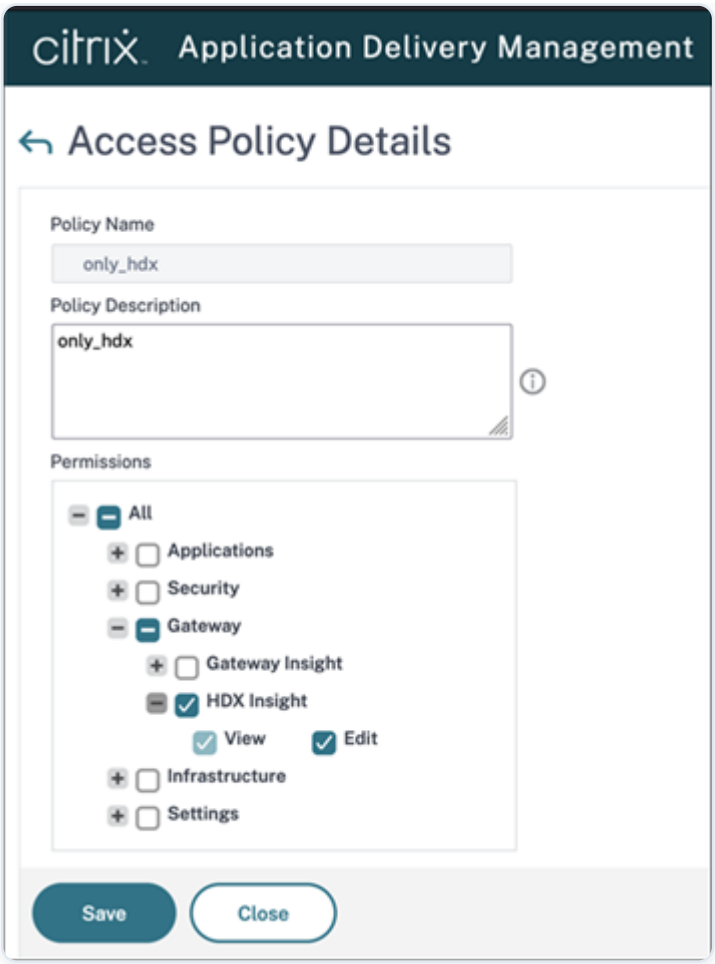
Para habilitar a análise de rede, você deve instalar e configurar o Citrix ADM no Director. O Director requer o Citrix ADM Versão 11.1 Build 49.16 ou posterior. O MAS é um dispositivo virtual que é executado no XenServer. Usando a análise de rede, o Director se comunica e coleta as informações relacionadas à sua implantação.

Para obter mais informações, consulte a documentação do Citrix ADM.

> **Observação:**
>
> O Citrix NetScaler Insight Center atingiu sua data de Fim de Manutenção em 15 May 2018. Consulte a Matriz de Produtos Citrix. Integre o Director ao Citrix ADM para análise de rede. Para migrar seu NetScaler Insight Center para o Citrix ADM, consulte Migrar do NetScaler Insight Center para o Citrix ADM.

1. No servidor onde o Director está instalado, localize a ferramenta de linha de comando DirectorConfig em `C:\inetpub\wwwroot\Director\tools` e execute-a com o parâmetro /configNetScaler a partir de um prompt de comando.
2. Quando solicitado, insira o nome da máquina Citrix ADM (FQDN ou endereço IP), o nome de usuário, a senha, o tipo de conexão HTTPS (preferencial em relação ao HTTP) e escolha a integração do Citrix ADM.
3. Para verificar as alterações, faça logoff e faça login novamente.

> **Observação:**
>
> Por motivos de segurança, recomenda-se criar uma função personalizada para a integração do ADM com o Director com permissão suficiente para acessar apenas o HDX Insight.



Para obter mais informações, consulte Configurar políticas de acesso.

Administração delegada e Director

A administração delegada usa três conceitos: administradores, funções e escopos. As permissões são baseadas na função de um administrador e no escopo dessa função. Por exemplo, um administrador pode receber uma função de administrador de Help Desk onde o escopo envolve a responsabilidade por usuários finais em apenas um site.

Para obter informações sobre como criar administradores delegados, consulte o artigo principal sobre administração delegada.

As permissões administrativas determinam a interface do Director apresentada aos administradores e as tarefas que eles podem executar. As permissões determinam:

- As exibições que o administrador pode acessar, coletivamente referidas como uma exibição.
- Os desktops, máquinas e sessões que o administrador pode visualizar e interagir.
- Os comandos que o administrador pode executar, como sombrear a sessão de um usuário ou habilitar o modo de manutenção.

As funções e permissões integradas também determinam como os administradores usam o Director:

FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO DIRECTOR
Administrador Completo	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o modo de manutenção e exportar dados de tendências.
Administrador de grupo de entrega	Acesso total a todas as visualizações e pode executar todos os comandos, incluindo o espelhamento da sessão de um usuário, gerenciamento de energia e gerenciamento de sessão, habilitação do modo de manutenção e exportação de dados de tendências.
Administrador Somente Leitura	Pode acessar todas as visualizações e ver todos os objetos em escopos especificados e informações globais. Pode baixar relatórios de canais HDX™ e exportar dados de Tendências usando a opção Exportar na visualização Tendências. Não pode executar nenhum outro comando ou alterar nada nas visualizações.
Administrador de Help Desk	Pode acessar apenas as visualizações de Help Desk e Detalhes do Usuário e pode visualizar apenas os objetos que o administrador está delegado a gerenciar. Pode espelhar a sessão de um usuário e executar comandos para esse usuário. Pode executar operações de modo de manutenção. Pode usar opções de controle de energia para Máquinas de SO de sessão única. Não pode acessar as visualizações de Painel, Tendências, Alertas ou Filtros. Não pode usar opções de controle de energia para máquinas de SO de múltiplas sessões.
Administrador de catálogo de máquinas	Pode acessar apenas a página Detalhes da Máquina (pesquisa baseada em máquina).

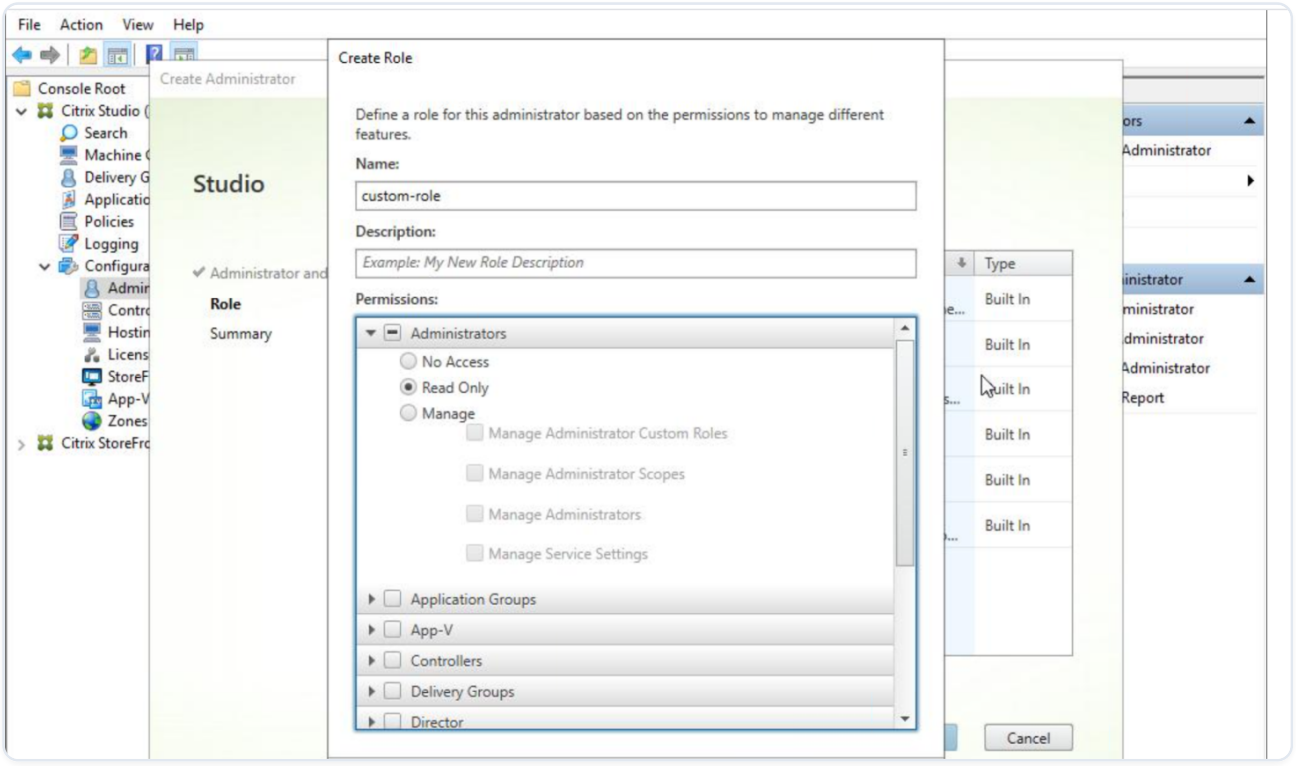
FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO DIRECTOR
Administrador de Host	Sem acesso. Este administrador não é suportado para o Director e não pode visualizar dados.

Configurar funções personalizadas para administradores do Director

No Studio, você também pode configurar funções personalizadas específicas do Director para corresponder mais de perto aos requisitos da sua organização e delegar permissões de forma mais flexível. Por exemplo, você pode restringir a função de administrador de Help Desk integrada para que este administrador não possa encerrar sessões.

Se você criar uma função personalizada com permissões do Director, também deverá conceder a essa função outras permissões genéricas:

- Permissão do Delivery Controller™ para fazer logon no Director - pelo menos acesso somente leitura no nó Administrador
- Permissões para grupos de entrega para visualizar os dados relacionados a esses grupos de entrega no Director - pelo menos acesso somente leitura

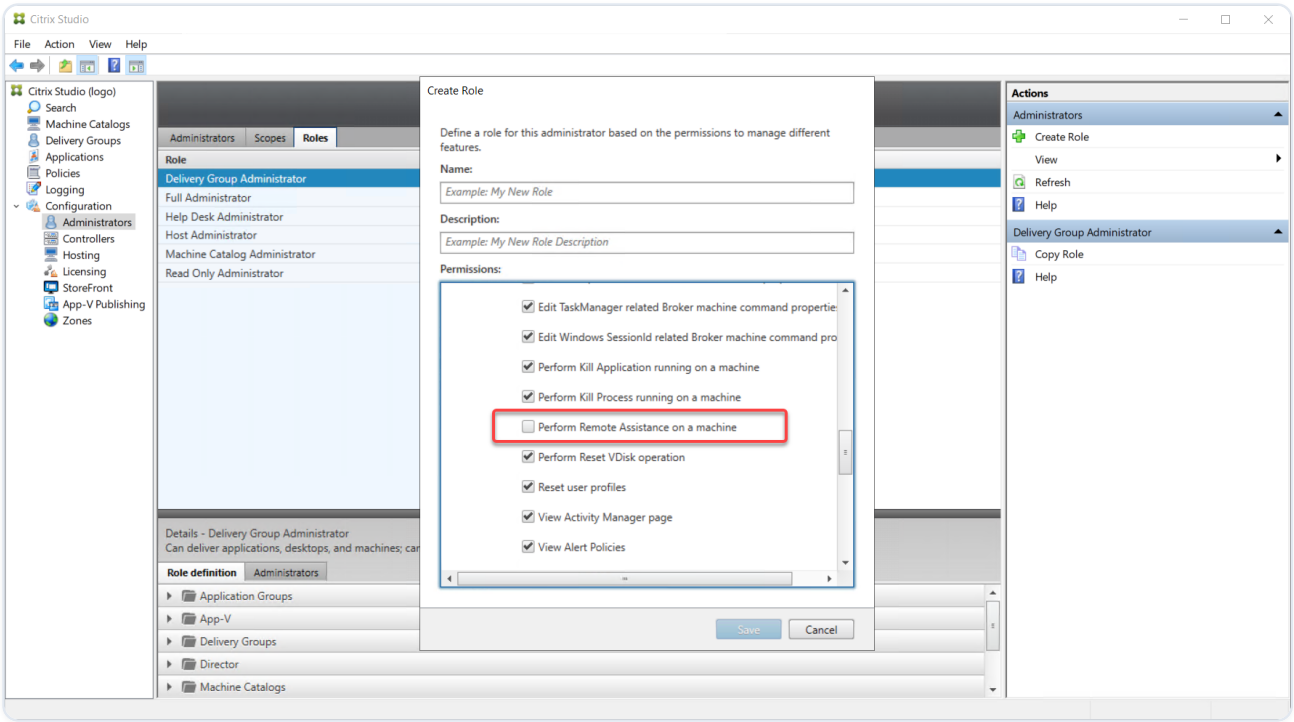


Alternativamente, você pode criar uma função personalizada copiando uma função existente e incluir permissões extras para diferentes visualizações. Por exemplo, você pode copiar a função de Help Desk e incluir permissões para visualizar as páginas de Painel ou Filtros.

Selecione as permissões do Director para a função personalizada, que incluem:

- Executar Encerrar Aplicativo em execução em uma máquina
- Executar Encerrar Processo em execução em uma máquina
- Executar Assistência Remota em uma máquina
- Redefinir perfis de usuário
- Visualizar página de Detalhes do Cliente
- Visualizar página do Painel
- Visualizar página de Filtros
- Visualizar página de Detalhes da Máquina
- Visualizar página de Tendências
- Visualizar página de Detalhes do Usuário

Neste exemplo, o Sombreamento (Executar Assistência Remota em uma máquina) está desativado.



Uma permissão pode ter dependências de outras permissões para se tornar aplicável na interface do usuário. Por exemplo, selecionar a permissão **Executar Encerrar Aplicativo em execução em uma máquina** habilita a funcionalidade **Encerrar Aplicativo** apenas nos painéis para os quais a função tem permissão. Você pode selecionar as seguintes permissões de painel:

- Visualizar página de Filtros
- Página de Detalhes do Usuário

- Página de Detalhes da Máquina
- Página de Detalhes do Cliente

Além disso, da lista de permissões para outros componentes, considere estas permissões de grupos de entrega:

- Ativar/desativar o modo de manutenção de uma máquina usando a associação ao grupo de entrega.
- Executar operações de energia em máquinas Windows Desktop usando a associação ao grupo de entrega.
- Executar gerenciamento de sessão em máquinas usando a associação ao grupo de entrega.

Implantação segura do Director

Este artigo destaca áreas que podem ter um impacto na segurança do sistema ao implantar e configurar o Director.

Configurar o Microsoft Internet Information Services (IIS)

Você pode configurar o Director com uma configuração restrita do IIS.

Limites de reciclagem do Pool de Aplicativos

Você pode definir os seguintes limites de reciclagem do Pool de Aplicativos:

- Limite de Memória Virtual: 4.294.967.295
- Limite de Memória Privada: O tamanho da memória física do servidor StoreFront™
- Limite de Solicitações: 4.000.000.000

Extensões de nome de arquivo

Você pode desabilitar extensões de nome de arquivo não listadas.

O Director requer estas extensões de nome de arquivo na Filtragem de Solicitações:

- .aspx
- .css
- .HTML
- .js
- Extensão .png
- Extensão .svc

- Extensão .gif
- Extensão .json
- Extensão .woff
- .woff2
- Extensão .ttf

O Director requer os seguintes verbos HTTP na Filtragem de Solicitações. Você pode desautorizar verbos não listados.

- GET
- POST
- HEAD

O Director não requer:

- filtros ISAPI
- extensões ISAPI
- Programas CGI
- Programas FastCGI

Importante:

- O Director requer Confiança Total. Não defina o nível de confiança global do .NET como Alto ou inferior.
- O Director mantém um pool de aplicativos separado. Para modificar as configurações do Director, selecione o site do Director e modifique.

Configurar direitos de usuário

Quando o Director é instalado, seus pools de aplicativos recebem o seguinte:

- Direito de logon **Fazer logon como um serviço**
- Privilégios **Ajustar cotas de memória para um processo**, **Gerar auditorias de segurança** e **Substituir um token de nível de processo**

Os direitos e privilégios mencionados são comportamentos normais de instalação quando os pools de aplicativos são criados.

Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Director e são desativados automaticamente.

Comunicações do Director

Em um ambiente de produção, use os protocolos de segurança de protocolo de Internet (IPsec) ou HTTPS para proteger os dados que trafegam entre o Director e seus servidores.

O IPsec é um conjunto de extensões padrão para o Protocolo de Internet que fornece comunicações autenticadas e criptografadas com integridade de dados e proteção contra repetição. Como o IPsec é um conjunto de protocolos de camada de rede, protocolos de nível superior podem usá-lo sem modificação. O HTTPS usa os protocolos Transport Layer Security (TLS) para fornecer criptografia de dados forte.

> **Observação:**
>
> - A Citrix® recomenda fortemente que você restrinja o acesso ao console do Director dentro da rede intranet.
> - A Citrix recomenda fortemente que você não habilite conexões não seguras ao Director em um ambiente de produção.
> - Comunicações seguras do Director exigem configuração para cada conexão separadamente.
> - O protocolo SSL não é recomendado. Use o protocolo TLS mais seguro em vez disso.
> - Proteja suas comunicações com o Citrix ADC usando TLS, não IPsec.

> Para proteger as comunicações entre o Director e os servidores Citrix Virtual Apps and Desktops (para monitoramento e relatórios), consulte Segurança de Acesso a Dados.

Para proteger as comunicações entre o Director e o Citrix ADC (para Citrix Insight), consulte Configurar análise de rede.

Para proteger as comunicações entre o Director e o servidor de licenças, consulte Proteger o Console de Administração de Licenças.

Separação de segurança do Director

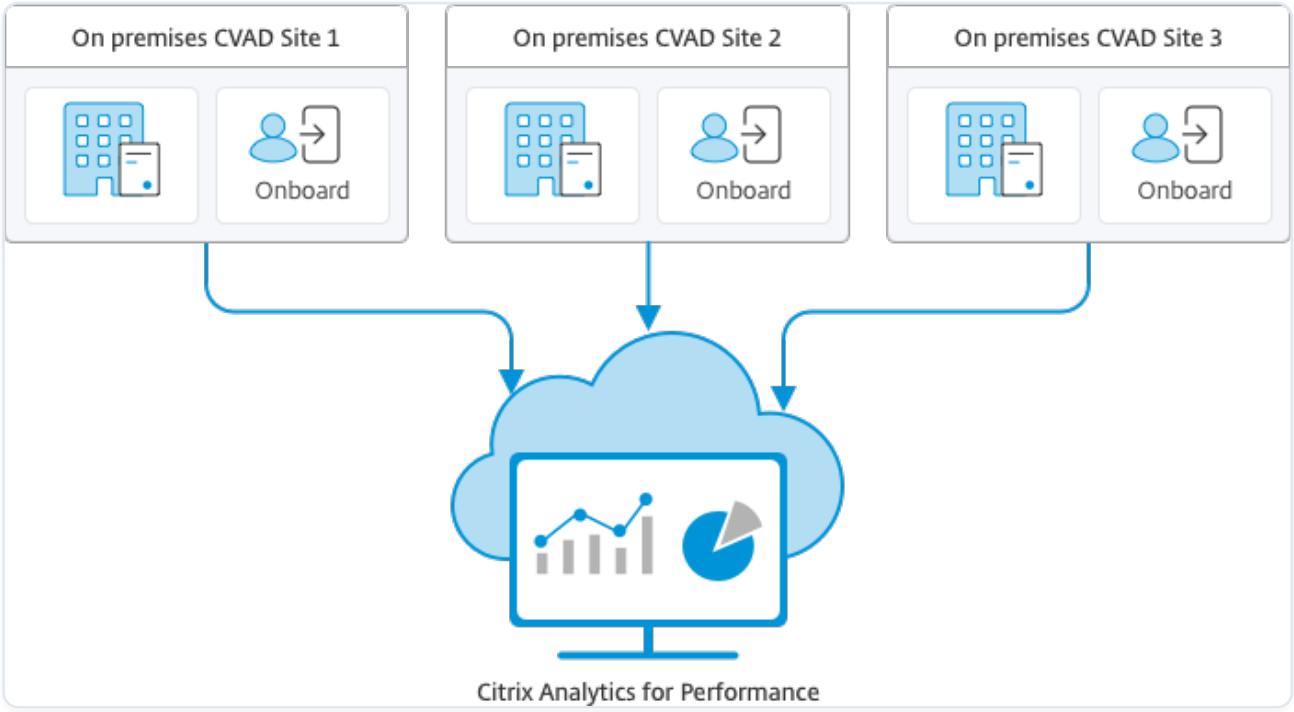
Você pode implantar quaisquer aplicativos web no mesmo domínio web (nome de domínio e porta) que o Director. No entanto, quaisquer riscos de segurança nesses aplicativos web podem potencialmente reduzir a segurança da sua implantação do Director. Onde um maior grau de separação de segurança é necessário, a Citrix recomenda que você implante o Director em um domínio web separado.

Configurando sites locais com Citrix Analytics for Performance™

O Citrix Analytics for Performance (Performance Analytics) é a solução abrangente de monitoramento de desempenho do Citrix Analytics Cloud Service. O Performance Analytics fornece insights e análises avançados baseados em métricas de desempenho. O Performance Analytics ajuda você a monitorar e visualizar as métricas de uso e desempenho de um ou mais sites do Citrix Virtual Apps and Desktops™ em sua organização.

Para obter mais informações sobre o Performance Analytics, consulte o artigo do Performance Analytics.

Você pode enviar dados de desempenho do seu site para o Citrix Analytics for Performance no Citrix Cloud™ para aproveitar seus recursos avançados de análise de desempenho. Para visualizar e usar o Performance Analytics, você deve primeiro configurar seus sites locais com o Citrix Analytics for Performance na guia **Analytics** no **Director**.



O Performance Analytics acessa os dados de forma segura e nenhum dado é transferido do Citrix Cloud para o ambiente local.

Pré-requisitos

Para configurar o Citrix Analytics for Performance a partir do Director, nenhum novo componente precisa ser instalado. Certifique-se de que os seguintes requisitos sejam atendidos:

- Seu Delivery Controller e Director estão na versão 1912 CU2 ou posterior. Para obter mais informações, consulte Matriz de compatibilidade de recursos.

Observação:

- A configuração do seu site local com o Citrix Analytics for Performance a partir do Director pode falhar se o Delivery Controller estiver executando uma versão do Microsoft .NET Framework anterior à 4.8. Como solução alternativa, atualize o .NET Framework em seu Delivery Controller para a versão 4.8. LCM-9255.
- Ao configurar seu site local executando o Citrix Virtual Apps and Desktops versão 2012 com o Citrix Analytics for Performance a partir do Director, a configuração pode falhar após algumas horas ou após uma reinicialização do Serviço de Monitoramento Citrix no Delivery Controller. A guia Analytics exibe um status Não Conectado neste caso. Como solução alternativa, crie uma pasta Encryption no registro do Delivery Controller, Local: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor, Nome da Pasta: Encryption. Certifique-se de que a conta CitrixMonitor tenha Acesso de Controle Total na pasta Encryption. Reinicie o Serviço de Monitoramento Citrix.DIR-14324.

- O acesso à guia **Analytics** para realizar esta configuração está disponível apenas para administradores completos.
- Para que o Performance Analytics acesse as métricas de desempenho, o acesso à internet de saída está disponível em todos os Delivery Controllers e nas máquinas nas quais o Director está instalado. Especificamente, garanta a acessibilidade aos seguintes URLs:
  - Registro de Chave Citrix: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Caso os Delivery Controllers e as máquinas do Director estejam em uma intranet e o acesso à internet de saída seja feito por meio de um servidor proxy, certifique-se do seguinte:
- O servidor proxy deve permitir a lista de URLs anterior.

- Adicione a seguinte configuração nos arquivos web.config do Director e citrix.monitor.exe.config. Certifique-se de adicionar esta configuração dentro das tags **configuration**:

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - O web.config do Director está localizado em `C:\inetpub\wwwroot\Director\web.config` na máquina onde o Director está instalado.
  - O citrix.monitor.exe.config está localizado em `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` na máquina onde o Delivery Controller está instalado.

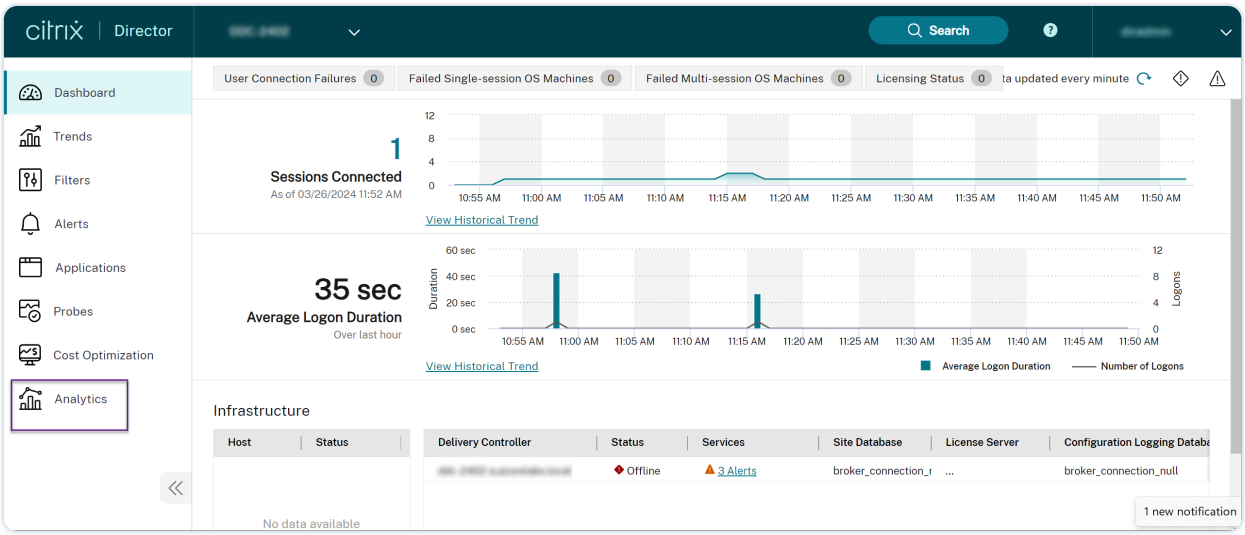
  Essa configuração é fornecida pela Microsoft no IIS. Para obter mais informações, consulte `https://docs.microsoft.com/pt-br/dotnet/framework/network-programming/proxy-configuration`. O campo **defaultproxy** no arquivo de configuração controla o acesso de saída do Director e do Monitor Service. A configuração e a comunicação com o Performance Analytics exigem que o campo **defaultproxy** seja definido como **true**. É possível que as políticas em vigor definam esse campo como false. Nesse caso, você deve definir manualmente o campo como true. Faça um backup dos arquivos de configuração antes de fazer as alterações. Reinicie o serviço de Monitoramento no Delivery Controller™ para que as alterações sejam aplicadas.

- Você tem um direito ativo do Citrix Cloud para o Citrix Analytics for Performance.
- Sua conta do Citrix Cloud é uma conta de Administrador com direitos à Experiência de Registro de Produto. Para obter mais informações sobre permissões de administrador, consulte Modificar Permissões de Administrador.

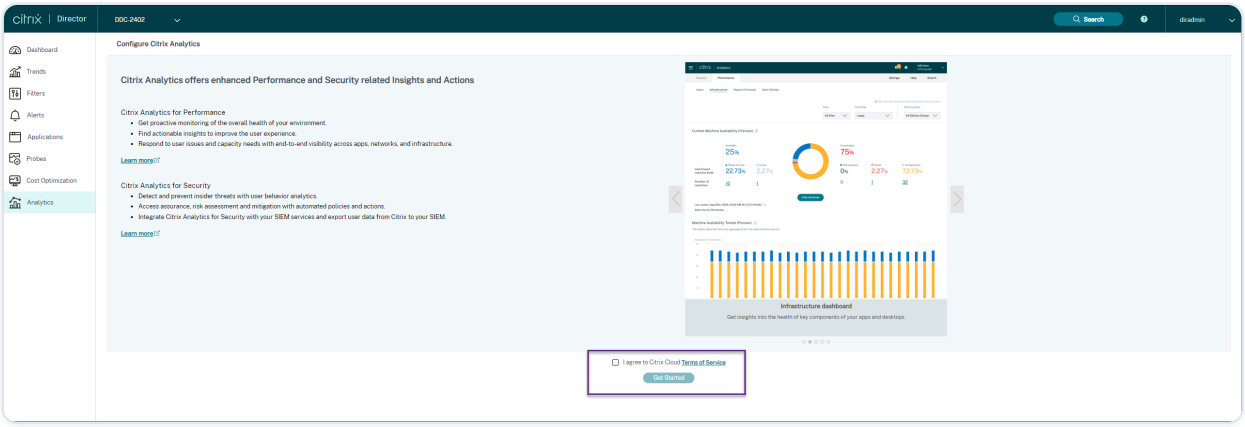
Etapas de configuração

Depois de verificar os pré-requisitos, faça o seguinte:

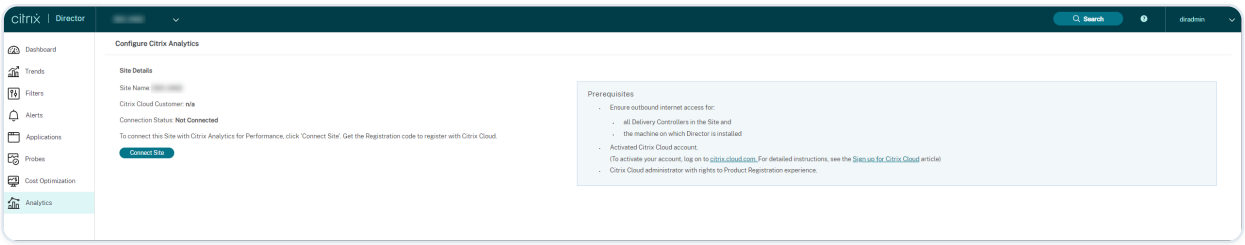
1. Faça login no Director como administrador completo e selecione o site que você deseja configurar com o Performance Analytics. A página do Painel do Director é exibida.



2. Clique na guia **Analytics**. A página **Configurar Citrix Analytics** é exibida.

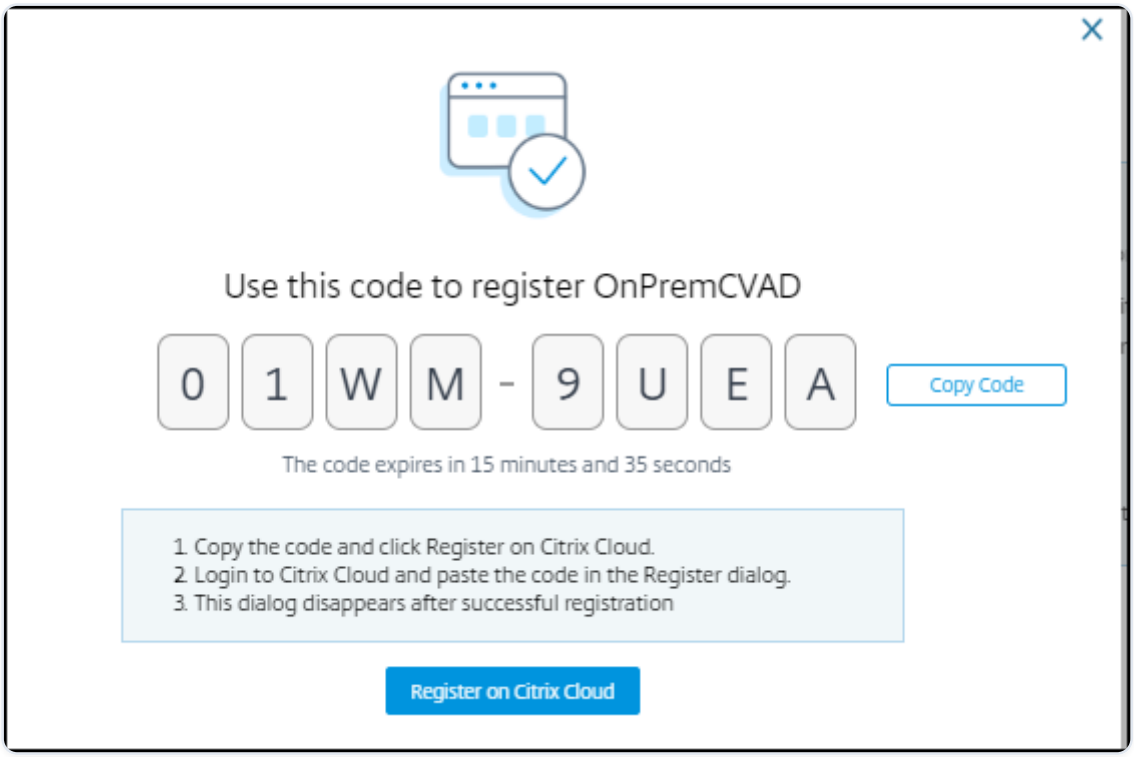


3. Revise as etapas, selecione os termos de serviço e clique em **Começar**. A página **Detalhes do Site** é exibida.

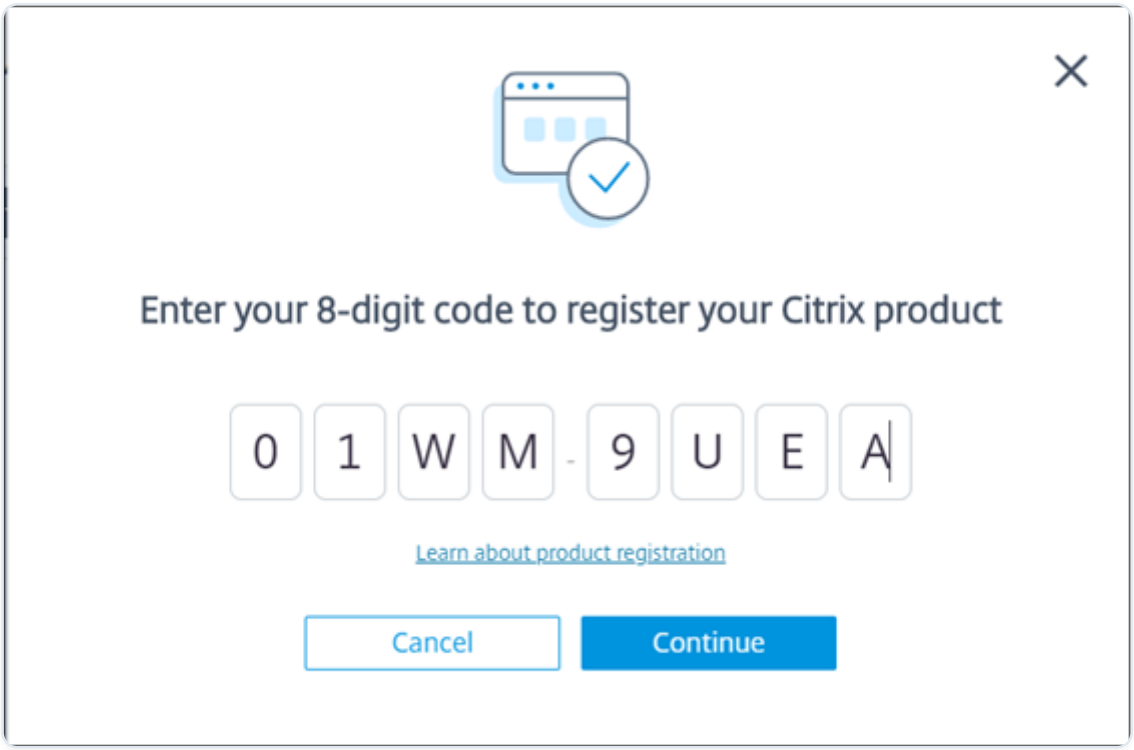


4. Revise os pré-requisitos e certifique-se de que sejam atendidos. Revise os detalhes do site.
5. Clique em **Conectar Site** para iniciar o processo de configuração.

   Um código de registro exclusivo de 8 dígitos é gerado para ser usado para registrar este site no Citrix Cloud.

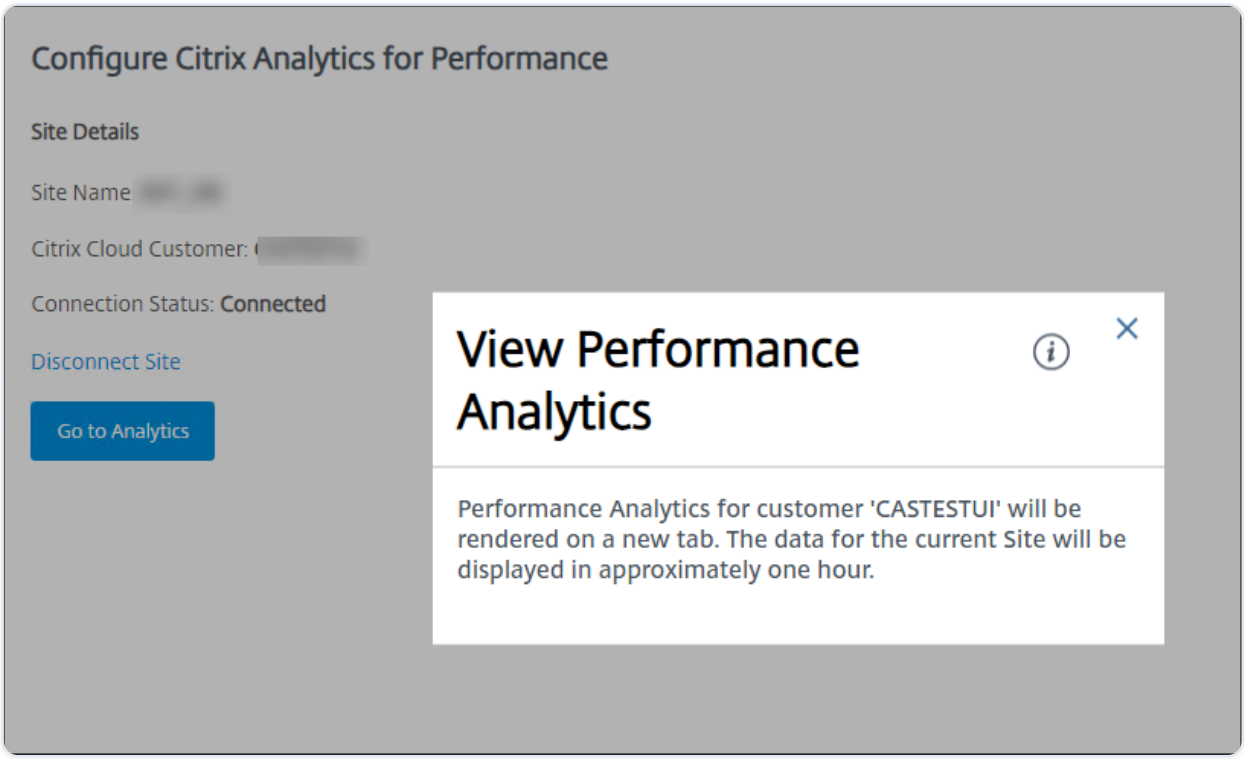


6. Clique em **Copiar Código** para copiar o código e, em seguida, clique em **Registrar no Citrix Cloud**. Você será redirecionado para o URL de registro no Citrix Cloud.
7. Faça login com suas credenciais do Citrix Cloud e selecione seu cliente.
8. Cole o código de registro copiado na página Registros de Produto no Citrix Cloud. Clique em **Continuar** para registrar. Revise os detalhes do registro e clique em **Registrar**.

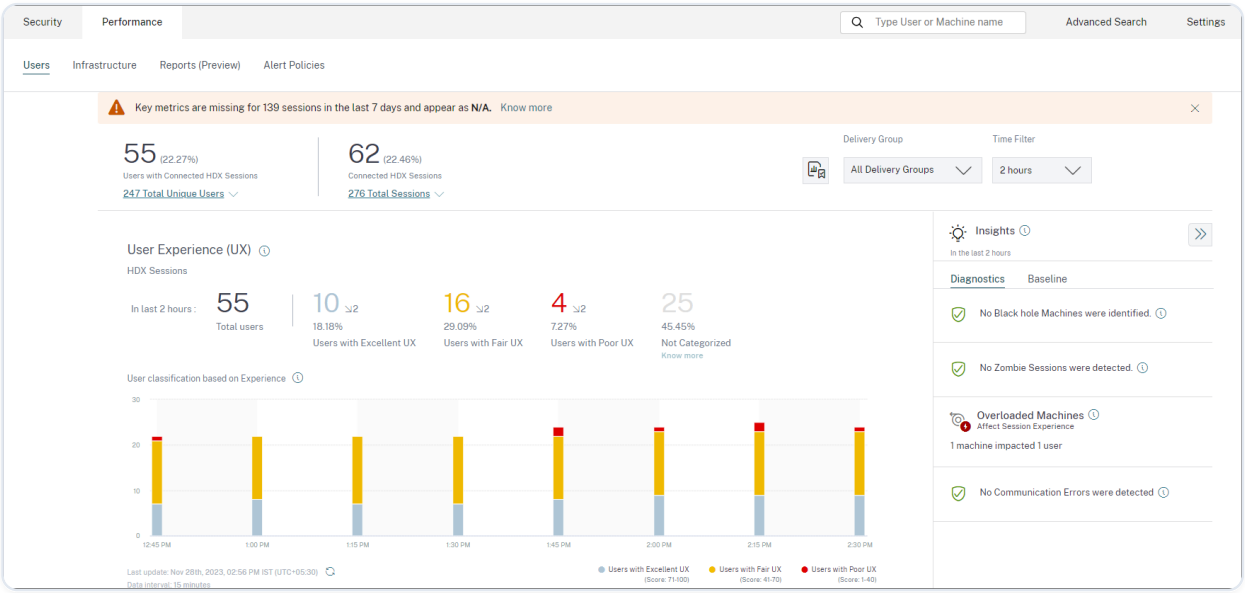


Seu site local se registra no Citrix Cloud.

9. No **Director**, clique em **Ir para Análise** na guia **Análise**.



O Performance Analytics é aberto em uma nova guia no seu navegador.



Se sua sessão do Citrix Cloud tiver expirado, você poderá ser redirecionado para a página de logon da conta Citrix.com ou My Citrix.

10. Para registrar vários sites no Performance Analytics, repita as etapas de configuração anteriores para cada site a partir do Director. As métricas de todos os sites configurados são exibidas no painel do Performance Analytics.

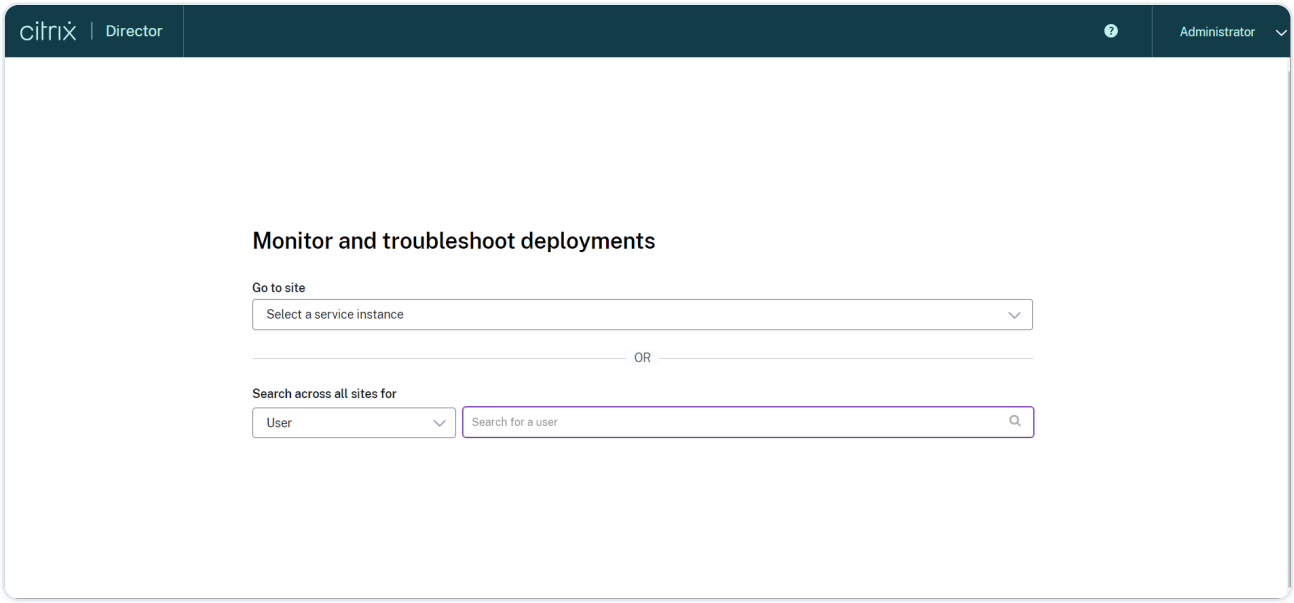
    Caso você tenha mais de uma instância do Director em execução por site, configure a partir de qualquer instância do Director. Todas as outras instâncias do Director conectadas ao site são atualizadas na próxima atualização após o processo de configuração.

11. Para desconectar seu site do Citrix Cloud, clique em **Desconectar Site**. Esta opção exclui a configuração existente.

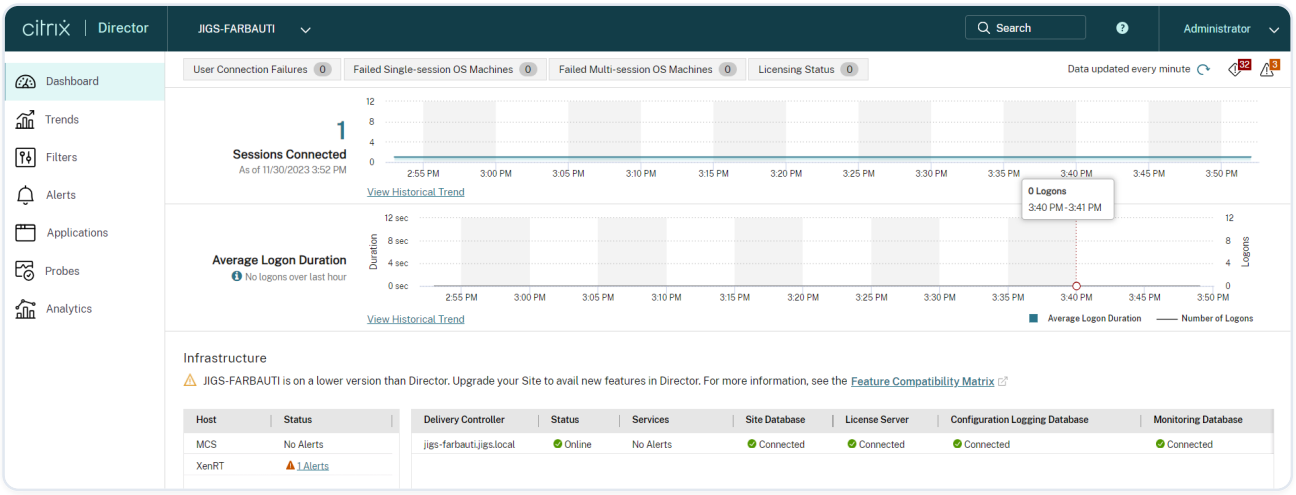
> **Notas:**
>
> Na primeira vez que você configura um site, os eventos do site podem levar algum tempo (aproximadamente uma hora) para serem processados; causando um atraso na exibição das métricas no painel do Performance Analytics. Depois disso, os eventos são atualizados em intervalos regulares.
>
> Após a desconexão, a transmissão de dados da conta antiga continua por algum tempo até que os eventos da nova conta sejam transmitidos. Por aproximadamente uma hora após a interrupção da transmissão de dados, as análises relacionadas à conta antiga permanecem exibidas no Painel do Performance Analytics.
>
> Após a expiração do direito ao serviço Citrix Analytics, leva até um dia para parar de enviar as métricas do site para o Performance Analytics.

Análise do Site

Usando o Director, você pode monitorar a integridade de suas implantações. Você pode solucionar problemas de desempenho pesquisando por um usuário, endpoint ou máquina em todos os sites integrados.



Com permissão total de administrador, ao abrir o Director, o Painel fornece um local centralizado para monitorar a integridade e o uso de um site.



Se não houver falhas atualmente e nenhuma falha tiver ocorrido nos últimos 60 minutos, os painéis permanecem recolhidos. Quando há falhas, o painel de falha específico aparece automaticamente.

> **Observação:**
>
> Dependendo da licença da sua organização e dos seus privilégios de Administrador, algumas opções ou recursos podem não estar disponíveis.

Painéis no Painel do Director

Falhas de Conexão do Usuário

Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para visualizar métricas para esse tipo de falha. Na tabela adjacente, esse número é detalhado por grupos de entrega. As falhas de conexão incluem falhas causadas pelo atingimento dos limites do aplicativo. Para obter mais informações sobre limites de aplicativos, consulte Aplicativos.

Máquinas OS de sessão única com falha ou Máquinas OS de várias sessões com falha

Total de falhas nos últimos 60 minutos detalhadas por grupos de entrega. Falhas detalhadas por tipos, incluindo falha ao iniciar, travado na inicialização e não registrado. Para máquinas de SO multi-sessão, as falhas também incluem máquinas atingindo a carga máxima.

Status de Licenciamento

Os alertas do Servidor de Licenças exibem alertas enviados pelo Servidor de Licenças e as ações necessárias para resolver os alertas. Requer Servidor de Licenças Versão 11.12.1 ou posterior. Os alertas do Delivery Controller exibem os detalhes do estado de licenciamento conforme visto pelo Controller e são enviados pelo Controller. Requer Controller para XenApp 7.6 ou XenDesktop 7.6 ou posterior. Você pode definir o limite para alertas no Studio. O status de licenciamento exibido em **Delivery Controllers** > **Detalhes** > **Edições do Produto** > **PLT** indica **Premium** e não **Platinum**.

Estado de Carência

O Director exibe um dos seguintes estados de carência. Esta informação é obtida do Delivery Controller.

1. **Não Ativo:** Não está em nenhum tipo de modo de cache de licença. Limites normais de licenciamento se aplicam.
2. **Carência de Emergência:** Entra em vigor quando o servidor de licenças está inacessível ou as informações de licença não podem ser obtidas durante a intermediação de uma conexão. Os usuários não são afetados. Os erros exibidos no Director não podem ser ignorados até que o servidor de licenças esteja acessível.
3. **Período de Carência Expirado:** O modo de cache de licença de emergência expirou.

Para obter mais informações, consulte Excesso de licença e Modo de intermitência de licença.

Sessões Conectadas

Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.

Duração Média do Logon

Dados de logon dos últimos 60 minutos. O número grande à esquerda é a duração média do logon ao longo da hora. Os dados de logon para VDAs anteriores ao XenDesktop 7.0 não estão incluídos nesta média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Infraestrutura

Lista a infraestrutura do seu site - hosts e Controladores. Para infraestrutura do XenServer ou VMware, você pode visualizar alertas de desempenho. Por exemplo, você pode configurar o XenCenter para gerar alertas de desempenho quando o uso da CPU, E/S de rede ou E/S de disco exceder um limite especificado em um servidor gerenciado ou máquina virtual. Por padrão, o

intervalo de repetição do alerta é de 60 minutos, mas você também pode configurá-lo. Para obter detalhes, consulte a seção Alertas de Desempenho do XenCenter na documentação do produto XenServer.

Observação:

Se nenhum ícone aparecer para uma métrica específica, isso indica que essa métrica não é suportada pelo tipo de host que você está usando. Por exemplo, nenhuma informação de saúde está disponível para hosts do System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

Continue a solucionar problemas usando estas opções (que estão documentadas nas seções a seguir):

- Controlar energia da máquina do usuário
- Impedir conexões com máquinas

Monitorar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

AÇÃO	DESCRIÇÃO
Visualizar a máquina ou sessão atualmente conectada de um usuário	Nas exibições Gerenciador de Atividades e Detalhes do Usuário, visualize a máquina ou sessão atualmente conectada do usuário e uma lista de todas as máquinas e sessões às quais este usuário tem acesso. Para acessar esta lista, clique no ícone do alternador de sessão na barra de título do usuário. Para obter mais informações, consulte Restaurar sessões.
Visualizar o número total de sessões conectadas em todos os grupos de entrega	No Painel, no painel **Sessões Conectadas**, visualize o número total de sessões conectadas em todos os grupos de entrega nos últimos 60 minutos. Em seguida, clique no grande número total, que abre a exibição Filtros, onde você pode exibir dados gráficos

AÇÃO	DESCRIÇÃO
	de sessão com base em grupos de entrega e intervalos selecionados e uso em todos os grupos de entrega.
Encerrar sessões ociosas	A exibição Filtros de Sessões exibe dados relacionados a todas as sessões ativas. Filtre as sessões com base no Usuário Associado, grupo de entrega, Estado da Sessão e Tempo Ocioso maior que um período de tempo limite. Na lista filtrada, selecione as sessões para fazer logoff ou desconectar. Para obter mais informações, consulte Solucionar problemas de aplicativos.
Visualizar dados por um período de tempo mais longo	Na exibição Tendências, selecione a guia **Sessões** para detalhar dados de uso mais específicos para sessões conectadas e desconectadas por um período de tempo mais longo (ou seja, totais de sessões de antes dos últimos 60 minutos). Para visualizar essas informações, clique em **Visualizar tendências históricas**.

Observação:

Se o dispositivo do usuário estiver executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7, ou um VDA Linux, o Director não poderá exibir informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem informando que as informações não estão disponíveis.

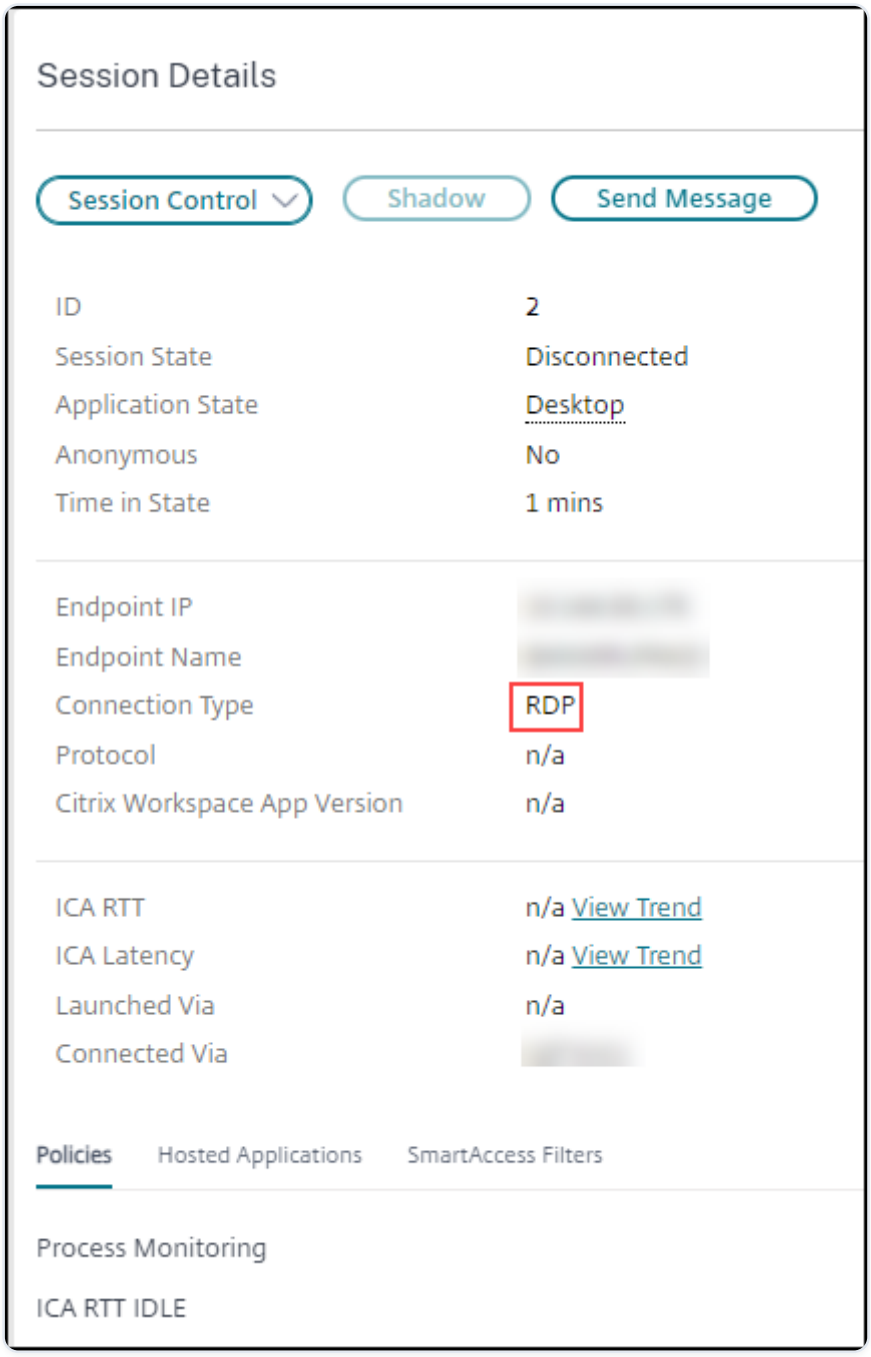
Limitação das Regras de Atribuição de Desktop: O Web Studio permite a atribuição de várias Regras de Atribuição de Desktop (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront™ exibe o desktop atribuído com o **Nome de Exibição** correspondente de acordo com a DAR para o usuário logado. No entanto, o Director não suporta DARs e exibe o desktop atribuído usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear um desktop específico para uma máquina no Director. Você pode mapear o desktop

atribuído exibido no StoreFront para o nome do grupo de entrega exibido no Director usando o seguinte comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

Protocolo de transporte da sessão

Visualize o protocolo de transporte em uso para o tipo de conexão HDX para a sessão atual no painel **Detalhes da Sessão**. Esta informação está disponível para sessões iniciadas em VDAs Versão 7.13 ou posterior.



- Para o tipo de conexão **HDX™**,
  - O Protocolo é exibido como **UDP**, se o EDT for usado para a conexão HDX.
  - O Protocolo é exibido como **TCP**, se o TCP for usado para a conexão HDX.
- Para o tipo de conexão **RDP**, o Protocolo é exibido como **n/a**.

Quando o transporte adaptável é configurado, o protocolo de transporte da sessão alterna dinamicamente entre EDT (sobre UDP) e TCP, com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ela retornará ao protocolo TCP.

Para obter mais informações sobre a configuração do transporte adaptativo, consulte Transporte Adaptativo.

Exportar relatórios

Você pode exportar dados de tendências para gerar relatórios regulares de uso e gerenciamento de capacidade. A exportação suporta formatos de relatório PDF, Excel e CSV. Relatórios nos formatos PDF e Excel contêm tendências representadas como gráficos e tabelas. Relatórios no formato CSV contêm dados tabulares que podem ser processados para gerar visualizações ou podem ser arquivados.

Para exportar um relatório:

1. Vá para a guia **Tendências**.
2. Defina os critérios de filtro e o período e clique em **Aplicar**. O gráfico de tendências e a tabela são preenchidos com dados.
3. Clique em **Exportar** e insira o nome e o formato do relatório.

O Director gera o relatório com base nos critérios de filtro selecionados. Se você alterar os critérios de filtro, clique em **Aplicar** antes de clicar em **Exportar**.

> **Observação:**
>
> A exportação de uma grande quantidade de dados causa um aumento significativo no consumo de memória e CPU no servidor do Director, no Delivery Controller e nos servidores SQL. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados são definidos para limites padrão para alcançar o desempenho ideal de exportação.

Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos para os critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados além dos limites padrão no número de linhas ou registros na tabela. O número padrão de registros suportados é definido com base no formato do relatório.

Você pode alterar o limite padrão configurando as Configurações do Aplicativo do Director no Internet Information Services (IIS).

FORMATO DO RELATÓRIO	NÚMERO PADRÃO DE REGISTROS SUPORTADOS	CAMPOS NAS CONFIGURAÇÕES DO APLICATIVO DO DIRECTOR	NÚMERO MÁXIMO DE REGISTROS SUPORTADOS
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100.000	UI.ExportExcelDrilldownLimit	100.000
CSV	100.000 (10.000.000 na guia **Sessões**)	UI.ExportCsvDrilldownLimit	100.000

Para alterar o limite do número de registros que você pode exportar:

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Default website.
3. Clique duas vezes em **Application Settings**.
4. Edite ou adicione uma configuração para os campos UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit ou UI.ExportCsvDrilldownLimit conforme necessário.

Adicionar esses valores de campo em Application Settings substitui os valores padrão.

> **Aviso:**
>
> Definir valores de campo maiores que o número máximo de registros suportados pode afetar o desempenho da Exportação e não é suportado.

Tratamento de Erros

Esta seção fornece informações sobre como lidar com erros que você pode encontrar durante a operação de Exportação.

- **O Director atingiu o tempo limite**

Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos no servidor Director ou com o Monitor Service.

A duração padrão do tempo limite é de 100 segundos. Para aumentar a duração do tempo limite do Director Service, defina o valor do campo **Connector.DataServiceContext.Timeout em** Director Application Settings no Internet Information Services (IIS):

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Default website.
3. Clique duas vezes em **Application Settings**.
4. Edite o valor **Connector.DataServiceContext.Timeout**.

- **O Monitor atingiu o tempo limite**

Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos com o Monitor Service ou no servidor SQL.

Para aumentar a duração do tempo limite do Monitor Service, execute os seguintes comandos PowerShell no Delivery Controller:

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **Operações de Exportação ou Visualização simultâneas máximas em andamento**

O Director suporta uma instância de Exportação ou Visualização. Se você receber o erro **Operações de Exportação ou Visualização simultâneas máximas em andamento**, tente a próxima operação de Exportação novamente mais tarde.

É possível aumentar o número de operações simultâneas de Exportação ou Visualização, no entanto, isso pode afetar o desempenho do Director e não é suportado:

1. Abra o console do Gerenciador do IIS.
2. Vá para o site do Director em Default website.
3. Clique duas vezes em **Application Settings**.
4. Edite o valor **UI.ConcurrentExportLimit**.

- **Espaço em disco insuficiente no Director**

Cada operação de Exportação requer um máximo de 2 GB de espaço em disco rígido na pasta Temp do Windows. Tente Exportar novamente depois de liberar espaço ou adicionar mais espaço em disco rígido no servidor Director.

Hotfixes do Monitor

Para visualizar os hotfixes instalados em um VDA de máquina específico (físico ou VM), escolha a exibição **Detalhes da Máquina**.

Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas que você seleciona no Director, use as opções de Controle de Energia. Essas opções estão disponíveis para máquinas de SO de sessão única, mas podem não estar disponíveis para máquinas de SO de múltiplas sessões.

Observação:

Essa funcionalidade não está disponível para máquinas físicas ou máquinas que usam o Acesso Remoto a PCs.

COMANDO	FUNÇÃO
Reiniciar	Executa um desligamento ordenado (suave) da VM e todos os processos em execução são interrompidos individualmente antes de reiniciar a VM. Por exemplo, selecione máquinas que aparecem no Director como "falha ao iniciar" e use este comando para reiniciá-las.
Forçar Reinício	Reinicia a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico e depois conectá-lo novamente e ligá-lo.
Desligar	Executa um desligamento ordenado (suave) da VM. Todos os processos em

COMANDO	FUNÇÃO
	execução são interrompidos individualmente.
Forçar Desligamento	Desliga a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico. Pode nem sempre desligar todos os processos em execução, e você corre o risco de perder dados se desligar uma VM dessa forma.
Suspender	Suspende uma VM em execução em seu estado atual e armazena esse estado em um arquivo no repositório de armazenamento padrão. Esta opção permite que você desligue o servidor host da VM e, posteriormente, após reiniciá-lo, retome a VM, retornando-a ao seu estado de execução original.
Retomar	Retoma uma VM suspensa e restaura seu estado de execução original.
Iniciar	Inicia uma VM quando ela está desligada (também conhecido como inicialização a frio).

Se as ações de controle de energia falharem, passe o mouse sobre o alerta e uma mensagem pop-up aparecerá com detalhes sobre a falha.

Impedir conexões a máquinas

Use o modo de manutenção para impedir novas conexões temporariamente enquanto o administrador apropriado executa tarefas de manutenção na imagem.

Quando você habilita o modo de manutenção nas máquinas, nenhuma nova conexão é permitida até que você o desabilite. Se os usuários estiverem atualmente logados, o modo de manutenção entra em vigor assim que todos os usuários fizerem logoff. Para usuários que não fazem logoff,

envie uma mensagem informando que as máquinas serão desligadas em um determinado horário e use os controles de energia para forçar o desligamento das máquinas.

1. Selecione a máquina, como na exibição Detalhes do Usuário, ou um grupo de máquinas na exibição Filtros.
2. Selecione **Modo de Manutenção** e ative a opção.

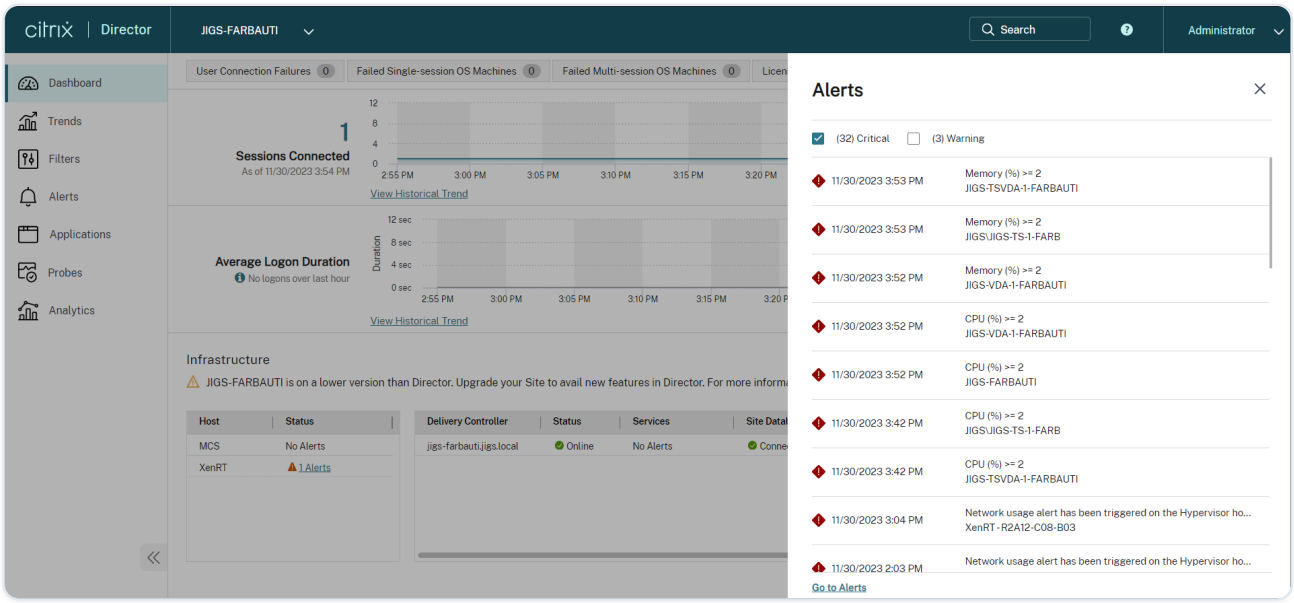
Se um usuário tentar se conectar a um desktop atribuído enquanto ele estiver no modo de manutenção, uma mensagem aparece indicando que o desktop está indisponível. Nenhuma nova conexão pode ser feita até que você desative o modo de manutenção.

Análise de Aplicativos

A guia **Aplicativos** exibe análises baseadas em aplicativos em uma visualização única e consolidada para ajudar a analisar e gerenciar o desempenho do aplicativo de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. Ele mostra métricas como os resultados da sondagem, o número de instâncias por aplicativo e as falhas e erros associados aos aplicativos publicados. Para obter mais informações, consulte a seção Análise de Aplicativos em **Solução de Problemas de Aplicativos**.

Alertas e notificações

Alertas são exibidos no Director no painel e em outras visualizações de alto nível com símbolos de alerta de aviso e críticos. Alertas estão disponíveis para sites com licença **Premium**. Os alertas são atualizados automaticamente a cada minuto; você também pode atualizar os alertas sob demanda.

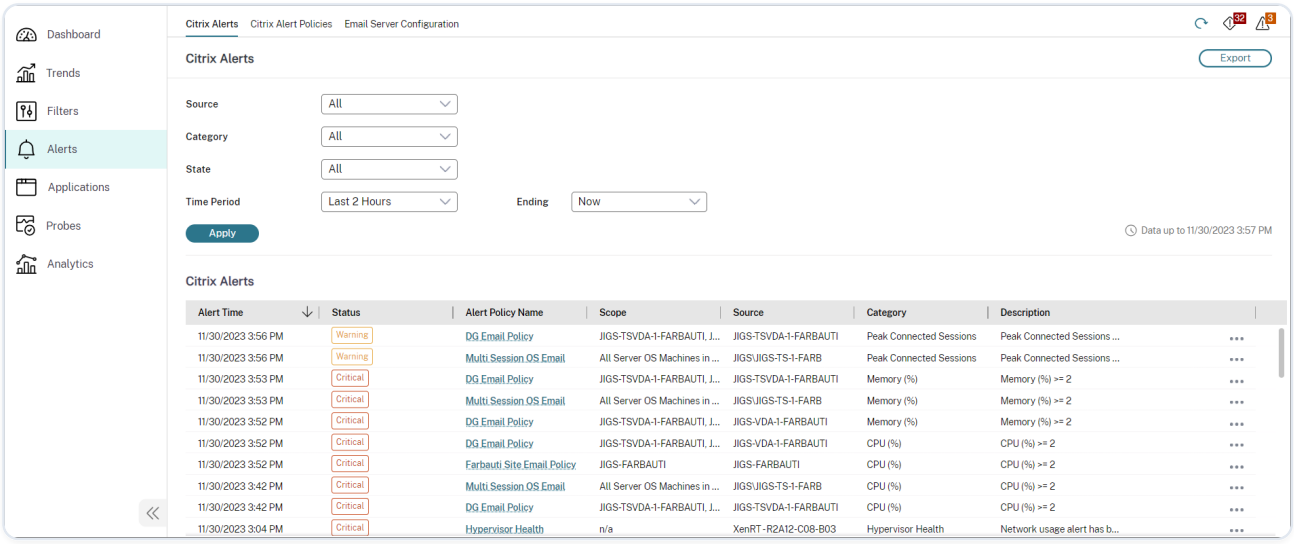


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre os alertas selecionando um alerta na barra lateral, clicando no link **Ir para Alertas** na parte inferior da barra lateral ou selecionando **Alertas** na parte superior da página do Director.

Na visualização Alertas, você pode filtrar e exportar alertas. Por exemplo, máquinas de SO multi-sessão com falha para um Grupo de Entrega específico no último mês, ou todos os alertas para um usuário específico. Para obter mais informações, consulte Exportar relatórios.



Alertas Citrix®

Os alertas Citrix são alertas monitorados no Director que se originam de componentes Citrix. Você pode configurar alertas Citrix dentro do Director em **Alertas** \> **Política de Alertas Citrix**. Como parte da configuração, você pode definir notificações para serem enviadas por e-mail a indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar Alertas Citrix, consulte Criar políticas de alerta.

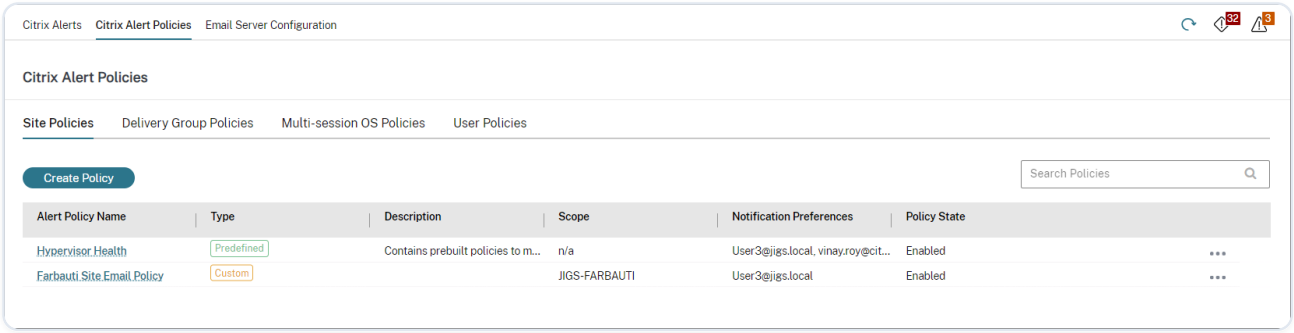
> **Observação:**
>
> Certifique-se de que seu firewall, proxy ou Microsoft Exchange Server não bloqueiem os alertas por e-mail.

Políticas de alerta inteligentes

Um conjunto de políticas de alerta integradas com valores de limite predefinidos está disponível para Grupos de Entrega e escopo de VDA de SO multi-sessão. Este recurso requer a versão 7.18 ou posterior do(s) Delivery Controller(s). Você pode modificar os parâmetros de limite das políticas de alerta integradas em **Alertas** \> **Política de Alertas Citrix**. Essas políticas são criadas quando há pelo menos um destino de alerta — um Grupo de Entrega ou um VDA de SO multi-sessão definido em seu site. Além disso, esses alertas integrados são adicionados automaticamente a um novo grupo de entrega ou a um VDA de SO multi-sessão.

Caso você atualize o Director e seu site, as políticas de alerta da sua instância anterior do Director são transferidas. As políticas de alerta integradas são criadas somente se nenhuma regra de alerta correspondente existir no banco de dados do Monitor.

Para os valores de limite das políticas de alerta integradas, consulte a seção Condições das políticas de alerta.



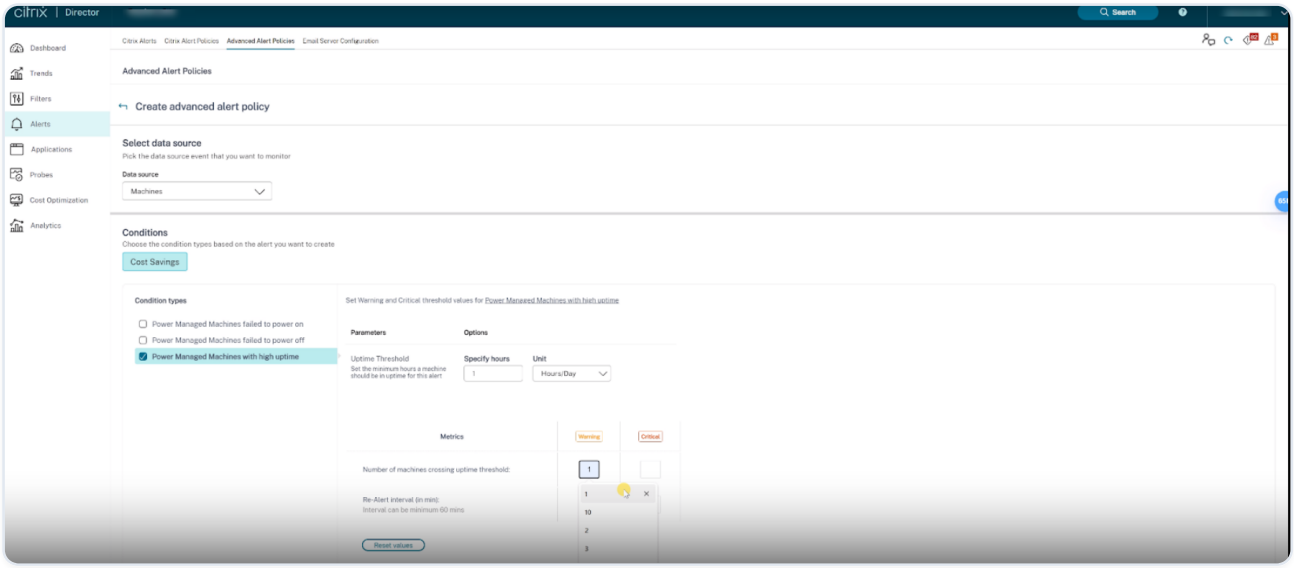
Políticas de alerta avançadas

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

Com a introdução das políticas de alerta avançadas, que são alertas orientados por fonte de dados, você pode usar a filtragem de escopo de múltiplas condições.

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

Você pode criar uma política de alerta avançada na seção **Alertas** > **Política de alerta avançada** > **Criar Política**.



Você pode selecionar a categoria como **Máquinas gerenciadas por energia que falharam ao ligar**, **Máquinas gerenciadas por energia que falharam ao desligar**, **Máquinas gerenciadas por energia com alto tempo de atividade** e, em seguida, selecionar as condições necessárias para a política. Para obter mais informações sobre como criar uma política, consulte Criar políticas de alerta. Após a criação da política, você pode editar, excluir ou desativar a política na página Alertas Citrix.

Você pode selecionar os parâmetros específicos e as opções correspondentes para cada uma das condições precedentes.

A categoria **Máquinas gerenciadas por energia com alto tempo de atividade** verifica as seguintes métricas:

- Número de máquinas que excedem o limite de tempo de atividade
- Intervalo de re-alerta (em min) o intervalo pode ser de no mínimo 60 min

As categorias **Máquinas gerenciadas por energia que falharam ao ligar** e **Máquinas gerenciadas por energia que falharam ao desligar** verificam as seguintes métricas:

- Número de máquinas que excedem o limite de tempo de atividade
- Intervalo de amostragem (em min) os intervalos podem ser múltiplos de 30 min
- Intervalo de re-alerta (em min) o re-alerta pode ser múltiplos de 60 min

Você pode definir a severidade das categorias precedentes conforme necessário. Você também pode agendar intervalos de re-alerta para esses alertas.

Definir o escopo da política

Você pode definir o escopo do seu alerta e adicionar exceções. O alerta é gerado apenas para o escopo selecionado e o subescopo excluído usando adicionar exceções não é incluído na geração do alerta. Este recurso ajuda você a criar alertas em um nível granular.

Você pode criar notificações por e-mail ou por URLs de webhook. Você também pode selecionar seu idioma preferido no qual gostaria de receber alertas. Você também pode selecionar uma opção para receber os parâmetros do alerta em um anexo de arquivo .CSV para e-mail ou em um payload JSON por meio de uma URL de webhook. O anexo inclui detalhes dos parâmetros necessários. Para obter mais informações, consulte Aprimoramentos no conteúdo do alerta.

Os seguintes dados são recebidos como um alerta por e-mail ou na página **Citrix Alerts**:

CAMPO	DESCRIÇÃO
ID do Cliente	O ID do cliente do site.
Nível do alerta	Este valor é o valor predefinido para cada condição de alerta. Os valores possíveis são Crítico e Aviso.
Condição	Este valor é a condição definida ao criar a política. Por exemplo, o número de máquinas não registradas é igual ou superior a 20.
Alvo	O nome do grupo de entrega ou site para o qual o alerta é acionado.
Site	O nome do site.
Escopo	O escopo da política. Este valor também inclui o subescopo.
Política	O nome da política.
Descrição	A descrição do problema para o qual o alerta é acionado.

Como criar uma política de alerta avançada usando um script PowerShell?

Script PowerShell para criar uma política de alerta:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

SUBSTITUA A SEGUINTE LINHA PELA CONDIÇÃO CORRETA PARA FAILEDMACHINEPERCENTAGE

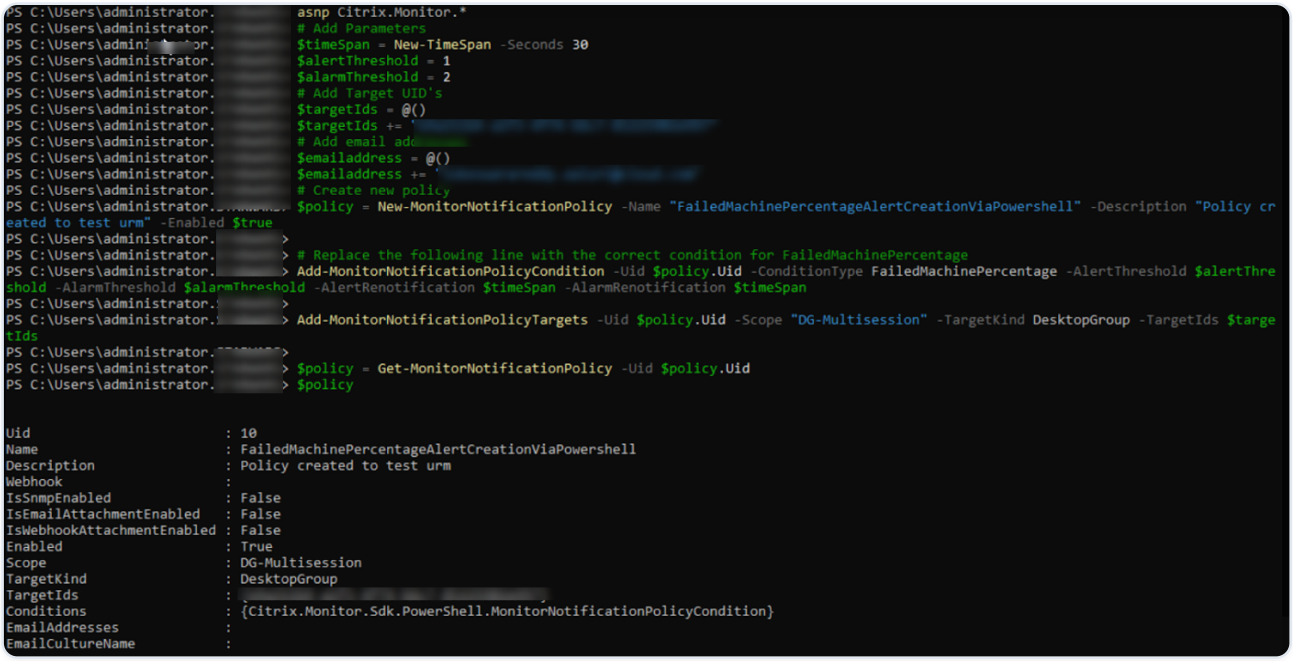
```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan



Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds
```

```
$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



Na imagem anterior, você pode ver que a política foi criada e o Uid é 10.

PARA ADICIONAR E-MAIL À CONFIGURAÇÃO

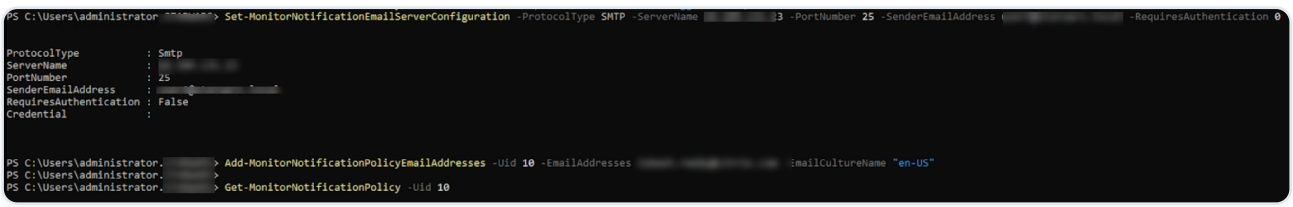
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

PARA ADICIONAR E-MAIL À POLÍTICA

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

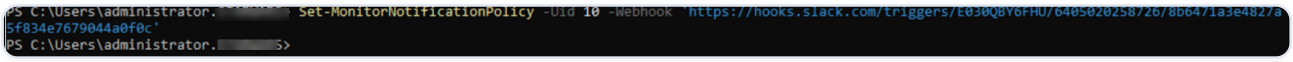
Script de exemplo para adicionar e-mail:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



PARA ADICIONAR URL DE WEBHOOK À POLÍTICA

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

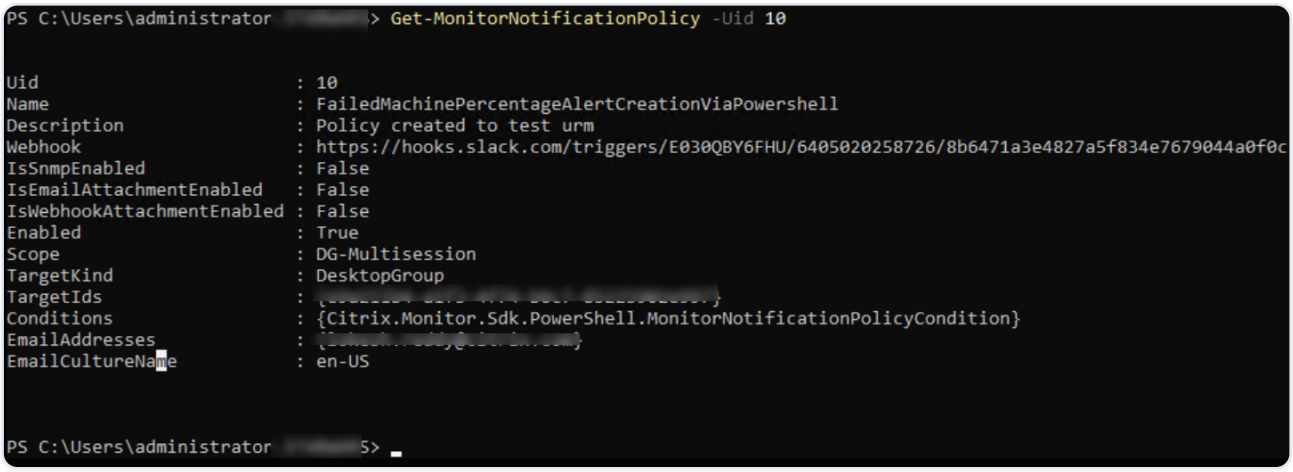


Script de exemplo para adicionar URL de webhook:

```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

OBTER DETALHES DA POLÍTICA CRIADA

```
Get-MonitorNotificationPolicy -Uid 10
```



Políticas de infraestrutura (Prévia)

Essas políticas são introduzidas para criar alertas relacionados à integridade dos componentes compatíveis do Citrix Virtual Apps and Desktops™.

Depois que a configuração do monitoramento de infraestrutura for concluída, você poderá usar os dados de integridade disponíveis no Director para configurar alertas para qualquer componente necessário. Os administradores podem definir condições, escopos e meios de notificação para receber alertas importantes por e-mail ou um payload JSON por meio de webhooks. Os alertas gerados também estão disponíveis na seção **Alertas Citrix** para análise e gerenciamento.

Como parte da política de infraestrutura recém-introduzida, as condições de alerta são categorizadas em quatro seções, conforme a seguir:

- Acessibilidade
- Serviços dependentes

- Impacto
- Utilização de recursos

As condições dentro de cada categoria podem ser definidas com a severidade de **Crítico** e **Aviso** com base nas prioridades da sua organização. Você também pode agendar intervalos de re-alerta para esses alertas.

Você pode criar uma política de infraestrutura na seção **Alertas** > **Políticas de Alerta Citrix**. Você pode selecionar a categoria necessária e, em seguida, selecionar as condições necessárias para a política. Para obter mais informações sobre como criar uma política, consulte Criar políticas de alerta. Depois que a política for criada, você poderá editá-la, excluí-la ou desativá-la na página Alertas Citrix.

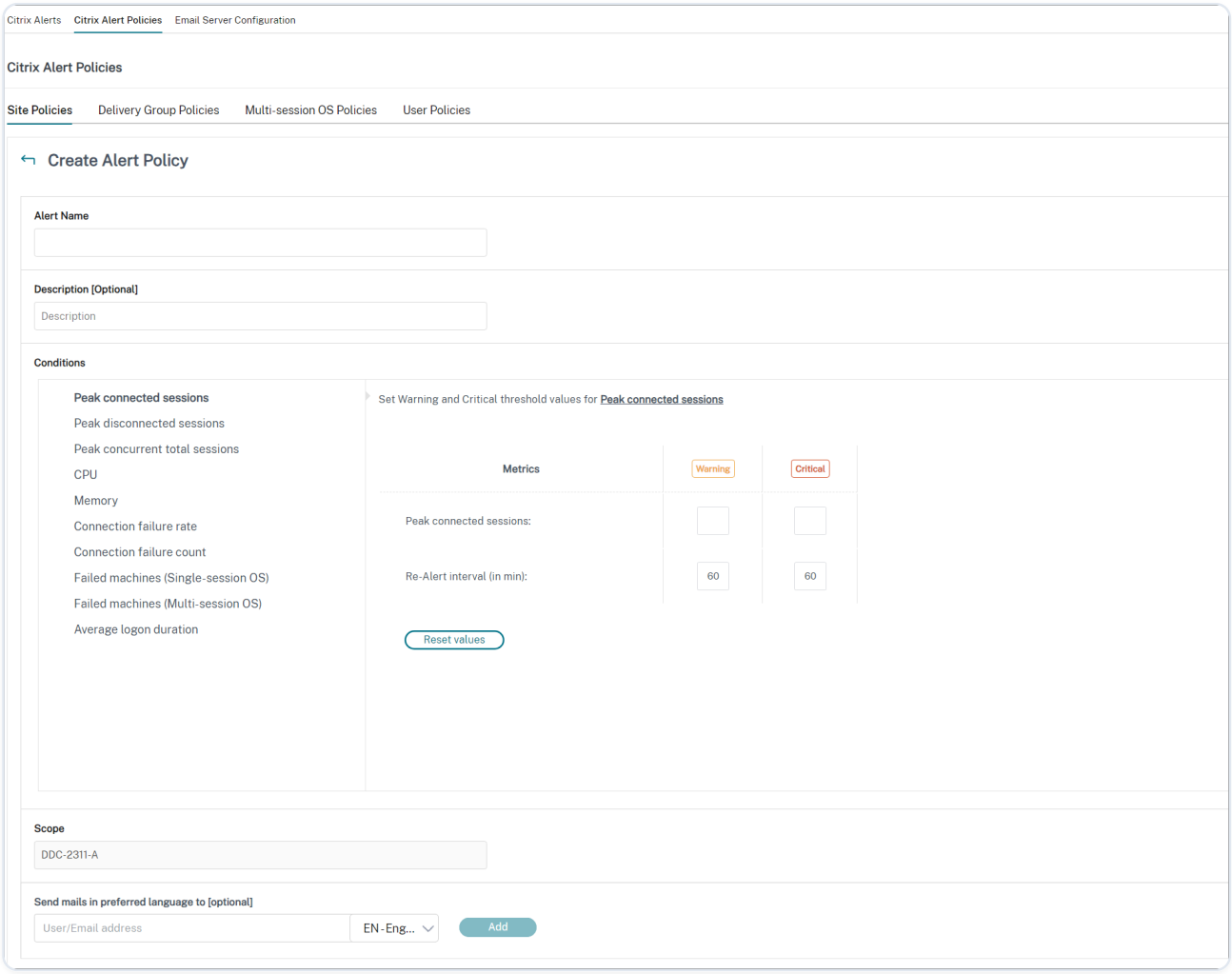
Para obter mais detalhes sobre as condições suportadas em cada categoria e componente, consulte o seguinte:

- Métricas de integridade do PVS
- Métricas de saúde do StoreFront

Os seguintes dados são recebidos como um alerta por e-mail ou na página de Alertas Citrix:

CAMPO	DESCRIÇÃO
ID do Cliente	O ID do cliente do site.
Nível de alerta	Os valores possíveis são Crítico e Aviso.
Destino	O nome da máquina para a qual o alerta é acionado.
Hora	A hora em que o alerta é acionado.
Escopo	O escopo da política.
Política	O nome da política.
Descrição	A descrição do problema para o qual o alerta é acionado.

Criar políticas de alerta



Para criar uma política de alerta, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alertas** > **Política de Alertas Citrix** e selecione, por exemplo, Política de SO multissessão.
2. Clique em **Criar**.
3. Nomeie e descreva a política, depois defina as condições que devem ser atendidas para que o alerta seja acionado. Por exemplo, especifique as contagens de Aviso e Crítico para Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico. Os valores de Aviso não devem ser maiores que os valores Críticos. Para obter mais informações, consulte Condições das políticas de alerta.
4. Defina o intervalo de Re-alerta. Se as condições para o alerta ainda forem atendidas, o alerta será acionado novamente neste intervalo de tempo e, se configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta ignorado não gera uma notificação por e-mail no intervalo de re-alerta.
5. Defina o Escopo. Por exemplo, defina para um Grupo de Entrega específico.

6. Em Preferências de notificação, especifique quem deve ser notificado por e-mail quando o alerta for acionado. Você deve especificar um servidor de e-mail na guia **Configuração do Servidor de E-mail** para definir as preferências de Notificação por e-mail nas Políticas de Alerta.

    a. Você também pode receber o conteúdo do alerta em um anexo .CSV ou por meio do payload JSON. Para isso, selecione as seguintes caixas de seleção:

    - **Incluir um payload JSON como anexo no webhook**
    - **Incluir um arquivo CSV como anexo no e-mail**

> **Observação:**
>
> As opções para receber conteúdo de alerta por meio de anexo .CSV e payload JSON estão disponíveis apenas para alguns alertas atualmente. Para obter mais informações, consulte Aprimoramentos no conteúdo do alerta

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 indicador de carregamento é exibido durante esse tempo.

A criação de mais de 50 políticas para até 20 Grupos de Entrega exclusivos (1000 alvos de Grupo de Entrega no total) pode resultar em um aumento no tempo de resposta (mais de 5 segundos).

Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro pode acionar alertas errôneos 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.

Aprimoramentos no conteúdo do alerta

O recurso de alerta do Director foi aprimorado para incluir um anexo CSV e um payload JSON. Com esse aprimoramento, você pode obter detalhes do alerta em um anexo CSV por e-mail ou

como um payload JSON se houver um webhook. Usando este anexo CSV ou payload JSON, você pode receber conteúdo enriquecido em um nível detalhado, auxiliando na rápida identificação e resolução de problemas.

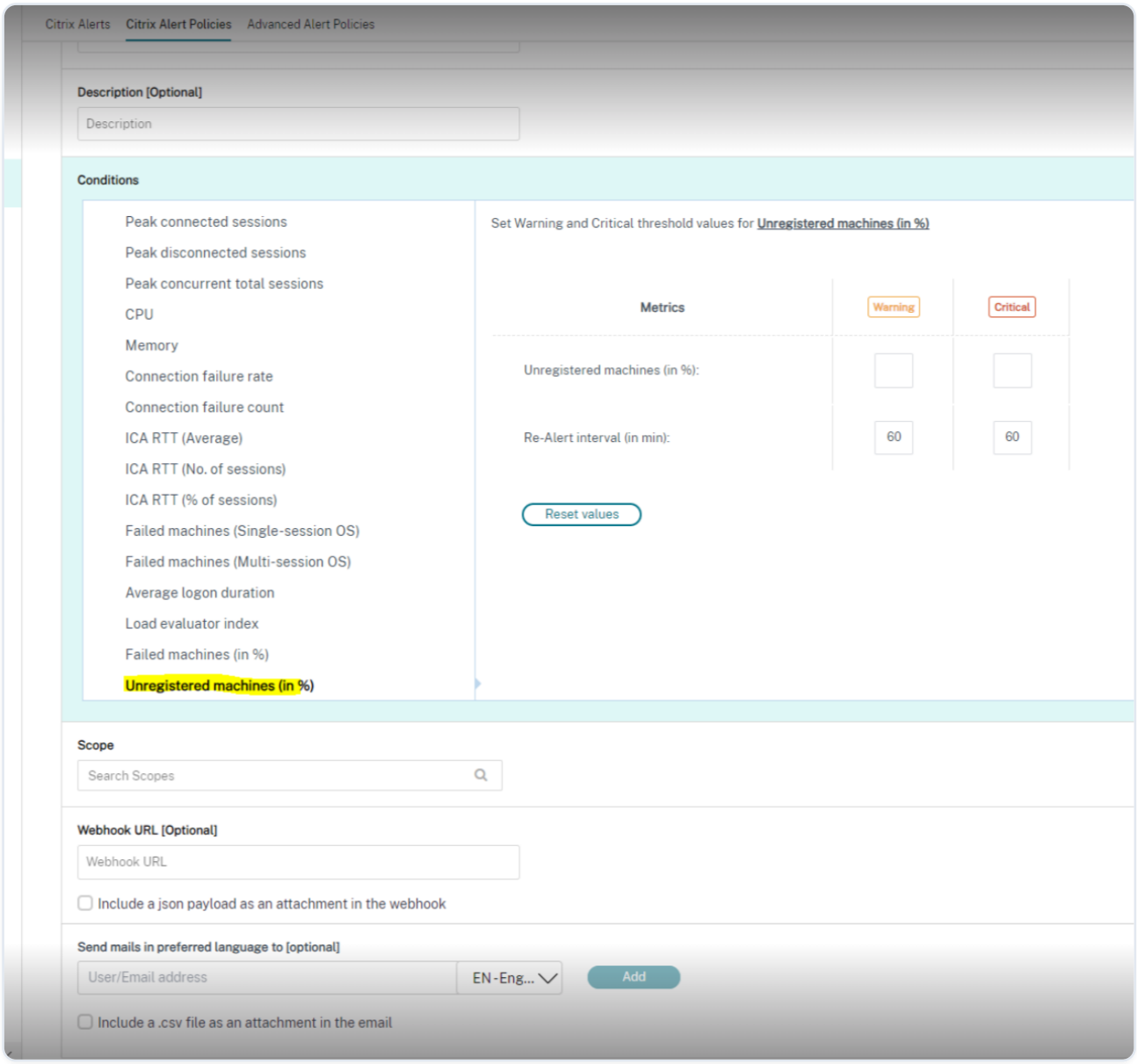
Atualmente, esse aprimoramento está disponível apenas nos seguintes alertas:

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

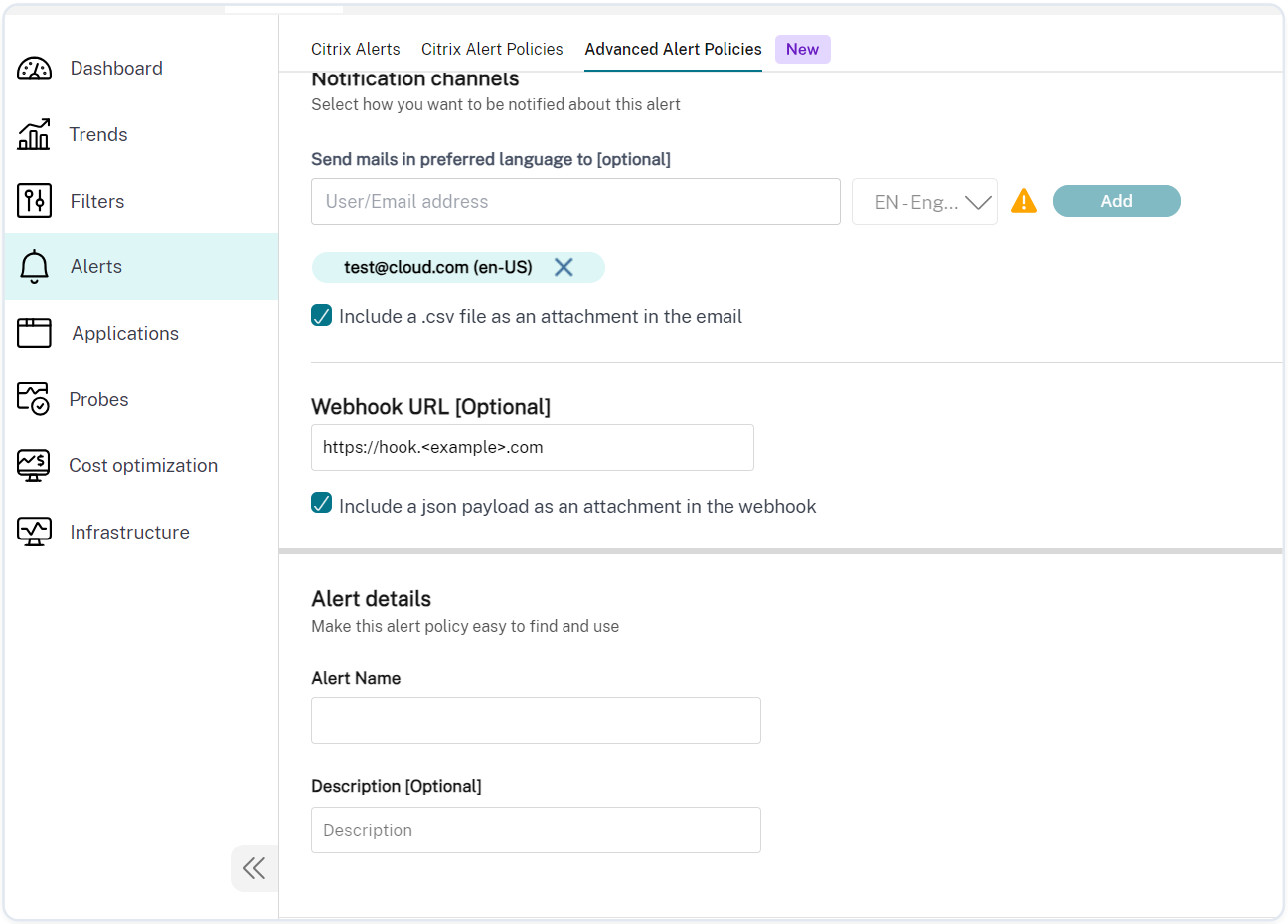
Para usar este recurso, navegar até o alerta e selecione as seguintes caixas de seleção:

- **Incluir um payload JSON como anexo no webhook**
- **Incluir um arquivo CSV como anexo no e-mail**

A seguir, uma captura de tela da seção **Políticas de Alerta do Citrix**:



Aqui está uma captura de tela da seção **Políticas de Alerta Avançadas**:



ANEXO CSV

A tabela a seguir fornece as colunas do anexo .CSV para todos os alertas suportados:

COLUNA	ALERTA APLICÁVEL
Nome da Máquina, Endereço IP e Nome do Grupo de Entrega	Tempo de atividade da máquina, Ação de desligamento falha e Ação de ligamento falha, e Máquinas não registradas (%)
Estado de Registro Atual, Data da Falha, Estado de Falha e Estado do Ciclo de Vida	Máquina não registrada (%)
Motivo da Falha da Última Ação de Energia, Última Ação de Energia Acionada Por, Tipo da Última Ação de Energia e Data de Conclusão da Última Ação de Energia	Ação de desligamento falha e Ação de inicialização falha
Estado de Energia, Data de Inicialização e Tempo Total de Atividade em Minutos	Tempo de atividade da máquina

PAYLOAD DO WEBHOOK

Alerta de Porcentagem de Máquinas Não Registradas

```
Webhook Payload

{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Unregistered machines (in %)",

    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "Current Registration State":
"Unregistered",
```

```
                                    "Failure Date": “<Date of Failure>”,

                                    "Fault State": "<Fault State of the
Machine>",

                                    "Lifecycle State": "<Lifecycle state
of the Machine>"

                                },

                               {

                                    "Machine Name": "<Name of the
Machine>",

                                    "IP Address": “<IP Address>”,

                                    "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                    "Current Registration State":
"Unregistered",

                                    "Failure Date": “<Date of Failure>”,

                                    "Fault State": "<Fault State of the
Machine>",

                                    "Lifecycle State": "<Lifecycle state
of the Machine>"

                                }]

}
```

Alerta de ações de inicialização falhas

```
Webhook Payload Body

{

    "Address": "<Webhook URL>",
```

```
    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Failure To PowerOn Action",

    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                       "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
```

```
"<Time string Eg: 2024-05-15T15:04:27.723>",

                                    {

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                     }]

}
```

Alerta de ações de desligamento falhas

```
{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Failure To PowerOff Action",
```

```
    "Value": "<Value Set as Threshold>",

    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                        "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                    },

                                   {

                                        "Machine Name": "<Name of the
```

```
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                       "Last Power Action Failure Reason":
"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Power
Action Type>",

                                        "Last Power Action Triggered By":
"<End-User,Administrator,Auto-Scale,Schedule>",

                                        "Last Power Action Type": “<PowerOn/
PowerOff>”,

                                        "Last Power Action Completed Date":
"<Time string Eg: 2024-05-15T15:04:27.723>"

                                    }]

}
```

Alerta de tempo de atividade da máquina

```
{

    "Address": "<Webhook URL>",

    "NotificationId": "<NotificationGUID>",

    "NotificationState": "NotificationActive",

    "Priority": "<Critical/Warning>",

    "Target": "<DeliveryGroupName>",

    "Condition": "Machine Uptime Alert",

    "Value": "<Value Set as Threshold>",
```

```
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)>",

    "PolicyName": "<Alert Policy Name>",

    "Description": "<Alert Policy Description>",

    "Scope": "DeliveryGroup",

    "Site": "<Name of the Site>",

    "AttachmentData": [{

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
Machine>",

                                        "Power State": "<On/Off>",

                                        "Powered On Date": "Time sting Eg:
2024-05-15T15:04:27.723",

                                        "Total Uptime In Minutes": 180

                                    },

                                   {

                                        "Machine Name": "<Name of the
Machine>",

                                        "IP Address": “<IP Address>”,

                                        "Delivery Group Name": "<Name of the
DeliveryGroup>",

                                        "IP Address": "<IPV4 Address of the
```

```
Machine>",
                                        "Power State": "<ON/OFF>",
                                        "Powered On Date": "<Time string Eg:
2024-05-15T15:04:27.723>",
                                        "Total Uptime In Minutes": <Uptime
Duration>
                                    }]
}
```

Condições das políticas de alertas

Encontre abaixo as categorias de alerta, as ações recomendadas para mitigar o alerta e as condições de política integradas, se definidas. As políticas de alerta integradas são definidas para intervalos de alerta e realerta de 60 minutos.

Pico de Sessões Conectadas

- Verifique a exibição Tendências de Sessão do Director para sessões conectadas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário

Pico de Sessões Desconectadas

- Verifique a exibição Tendências de Sessão do Director para sessões desconectadas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

Pico de Sessões Totais Concorrentes

- Verifique a exibição Tendências de Sessão do Director no Director para sessões simultâneas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

CPU

A porcentagem de uso da CPU indica o consumo geral da CPU no VDA, incluindo o dos processos. Você pode obter mais informações sobre a utilização da CPU por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem a CPU. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Encerrar o processo faz com que os dados não salvos sejam perdidos.
- Se tudo estiver funcionando como esperado, adicione recursos de CPU adicionais no futuro.

> **Nota:**
>
> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se esta configuração de política estiver desabilitada, alertas com condições de CPU e memória não serão acionados. Para obter mais informações, consulte Configurações de política de monitoramento
>
> **Condições de política inteligente:**

- **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
- **Valores de limite:** Aviso - 80%, Crítico - 90%

Memória

A porcentagem de uso da memória indica o consumo geral de memória no VDA, incluindo o dos processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem memória. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.

- Encerrar o processo causa a perda de dados não salvos.
- Se tudo estiver funcionando como esperado, adicione memória adicional no futuro.

> **Nota:**
>
> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se esta configuração de política estiver desabilitada, alertas com condições de CPU e memória não serão acionados. Para obter mais informações, consulte Configurações de política de monitoramento
>
> **Condições de política inteligente:**
>
> - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
> - **Valores de limite:** Aviso - 80%, Crítico - 90%

Taxa de Falha de Conexão

Porcentagem de falhas de conexão na última hora.

- Calculado com base no total de falhas em relação ao total de conexões tentadas.
- Verifique a exibição Tendências de Falhas de Conexão do Director para eventos registrados no log de Configuração.
- Determine se aplicativos ou desktops estão acessíveis.

Contagem de Falhas de Conexão

Número de falhas de conexão na última hora.

- Verifique a exibição Tendências de Falhas de Conexão do Director para eventos registrados no log de Configuração.
- Determine se aplicativos ou desktops estão acessíveis.

ICA® RTT (Média)

Tempo médio de ida e volta do ICA.

- Verifique o Citrix ADM para uma análise detalhada do ICA RTT para determinar a causa raiz. Para obter mais informações, consulte a documentação Citrix ADM.

- Se o Citrix ADM não estiver disponível, verifique a exibição Detalhes do Usuário do Director para o ICA RTT e Latência, e determine se é um problema de rede ou um problema com aplicativos ou desktops.

ICA RTT (Nº de Sessões)

Número de sessões que excedem o tempo de ida e volta ICA limite.

- Verifique o Citrix ADM para o número de sessões com ICA RTT alto. Para obter mais informações, consulte a documentação Citrix ADM.
- Se o Citrix ADM não estiver disponível, trabalhe com a equipe de rede para determinar a causa raiz.

  Condições da política inteligente:

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 300 ms para 5 ou mais sessões, Crítico - 400 ms para 10 ou mais sessões

RTT ICA (% de Sessões)

Porcentagem de sessões que excedem o tempo médio de ida e volta ICA.

- Verifique o Citrix ADM para o número de sessões com ICA RTT alto. Para obter mais informações, consulte a documentação Citrix ADM.
- Se o Citrix ADM não estiver disponível, trabalhe com a equipe de rede para determinar a causa raiz.

RTT ICA (Usuário)

Tempo de ida e volta ICA que é aplicado às sessões iniciadas pelo usuário especificado. O alerta é acionado se o RTT ICA for maior que o limite em pelo menos uma sessão.

Máquinas com Falha (SO de sessão única)

Número de máquinas SO de sessão única com falha. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz.

  Condições de política inteligente:

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 1, Crítico - 2

Máquinas com falha (SO multiusuário)

Número de máquinas SO multi-sessão com falha. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz.

  Condições de política inteligente:

  - **Escopo:** Grupo de Entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 1, Crítico - 2

Máquinas com falha (em %)

A porcentagem de máquinas SO de sessão única e multi-sessão com falha em um grupo de entrega, calculada com base no número de máquinas com falha. Esta condição de alerta permite configurar limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega e é calculada a cada 30 segundos. As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director. Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Solucionar problemas do usuário.

Ação de ligar com falha e ação de desligar com falha

Número de ações de ligar com falha e número de ações de desligar com falha em um grupo de entrega, calculados com base no número de **Máquinas Gerenciadas por Energia** que falharam ao ligar ou desligar. Essa condição de alerta permite configurar limites de alerta como o número de **Máquinas Gerenciadas por Energia** que falharam ao ligar ou desligar em um grupo de entrega e é calculada a cada 30 minutos.

O administrador pode configurar os seguintes parâmetros para esses alertas na política de alerta avançada:

- Acionado por: O que acionou a ação de energia
- Motivo da falha: Por que a ação falhou
- Limite: Número limite de máquinas que falharam na ação de energia para acionar a política
- Intervalo de amostragem: O intervalo em que a ação de energia com falha deve ser verificada
- Intervalo de reenvio de alerta: Após quanto tempo o alerta deve ser reenviado

As falhas podem ocorrer por várias razões, conforme mostrado nas exibições Painel e Filtros do Director. Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Solucionar problemas do usuário.

Máquinas não registradas (em %)

Uma máquina é considerada não registrada quando se torna instável devido a uma reinicialização ou quando há um problema de comunicação entre o delivery controller™ e as máquinas virtuais. A **Máquinas não registradas (em %)** é a porcentagem de máquinas OS de sessão única e multissessão não registradas em um grupo de entrega, calculada com base no número de máquinas não registradas. Esta condição de alerta permite configurar valores de limite de aviso e críticos como uma porcentagem de máquinas não registradas em um grupo de entrega. Você pode definir um intervalo para o reenvio do alerta. Você também pode adicionar um e-mail para receber uma notificação quando as condições forem atendidas para **Máquinas não registradas (em %)**. Quando o valor limite crítico ou de aviso é excedido, alertas e e-mails são gerados. Você pode visualizar alertas em **Alertas do Citrix**. Você pode filtrá-lo pela categoria **Máquinas não registradas (em %)** e para o estado e tempo necessários.

Você também pode receber detalhes do alerta em um anexo CSV se houver um e-mail ou através de um payload JSON se houver um webhook.

> **Nota:**
>
> O valor crítico deve ser maior que o valor de aviso.

> **Condições da política:**

- **Escopo**: OS de sessão única e grupo de entrega de OS multissessão
- **Valores limite**: Aviso e Crítico

Alerta de tempo de atividade da máquina

O tempo de atividade da máquina em um grupo de entrega é calculado com base no número de horas por dia, horas por semana ou horas por mês para uma máquina que está ligada em um grupo de entrega. Esta condição de alerta permite configurar limites de alerta como as horas em que uma máquina está ligada em um grupo de entrega. Os alertas de tempo de atividade da máquina funcionam da seguinte forma no caso de:

- Horas por dia - Você pode especificar o número de horas em que uma máquina fica ligada por dia e é calculado a cada 30 minutos. O número máximo de horas por dia que você pode definir é de 24 horas.

- Horas por semana - Você pode especificar o número de horas que uma máquina fica ligada por semana e é calculado a cada seis horas. O número máximo de horas por semana que você pode definir é de 168 horas.
- Horas por mês - Você pode especificar o número de horas que uma máquina fica ligada por mês e é calculado uma vez por dia. O número máximo de horas por mês é de 720 horas. O valor mínimo do intervalo de re-alerta que você pode definir é de 60 minutos. Você pode inserir o número de máquinas que excedem o valor limite de tempo de atividade da máquina na seção de alertas de Aviso e Crítico. Você também pode adicionar exceções para quaisquer máquinas.

Por exemplo, se houver cinco grupos de entrega adicionados para este alerta e se no primeiro grupo de entrega e no quarto grupo de entrega, o número de máquinas exceder os valores limite de aviso ou crítico, o alerta será acionado separadamente para o primeiro grupo de entrega e para o quarto grupo de entrega.

Este alerta ajuda os administradores a analisar o tempo de atividade das máquinas e, com base nessa análise, os administradores podem ajudar a otimizar o custo. Você também pode receber detalhes do alerta em um anexo CSV se houver um e-mail ou por meio de um payload JSON se houver um webhook.

Duração Média do Logon

Duração média do logon para logons que ocorreram na última hora.

- Verifique o Painel do Director para obter métricas atualizadas sobre a duração do logon. Muitos usuários fazendo logon em um curto período de tempo podem aumentar a duração do logon.
- Verifique a linha de base e o detalhamento dos logons para restringir a causa. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

  Condições da política inteligente:

  - **Escopo:** Grupo de Entrega, escopo de SO multissessão
  - **Valores limite:** Aviso - 45 segundos, Crítico - 60 segundos

Duração do Logon (Usuário)

Duração do logon para logons do usuário especificado que ocorreram na última hora.

Índice do Avaliador de Carga

Valor do Índice do Avaliador de Carga nos últimos 5 minutos.

- Verifique o Director para Máquinas de SO multissessão que possam ter uma carga de pico (Carga máxima). Visualize o Painel (falhas) e o relatório de Tendências do Índice do Avaliador de Carga.

  Condições de política inteligente:

  - **Escopo:** Grupo de Entrega, escopo de SO multissessão
  - **Valores de limite:** Aviso - 80%, Crítico - 90%

Configurar políticas de alerta com webhooks

Além das notificações por e-mail, você pode configurar políticas de alerta com webhooks.

Nota: Este recurso requer a versão 7.11 ou posterior do(s) Delivery Controller(s).

Você pode configurar uma política de alerta com um callback HTTP ou um POST HTTP usando cmdlets do PowerShell. Eles foram estendidos para suportar webhooks.

Para obter informações sobre a criação de um novo fluxo de trabalho do Octoblu e a obtenção do URL de webhook correspondente, consulte o Octoblu Developer Hub.

Para configurar um URL de webhook para uma nova política de alerta ou para uma política existente, use os seguintes cmdlets do PowerShell.

Crie uma nova política de alertas com um URL de webhook:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

Adicionar um URL de webhook a uma política de alerta existente:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

Para obter ajuda sobre os comandos do PowerShell, use a ajuda do PowerShell, por exemplo:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

As notificações geradas a partir da política de alerta acionam o webhook com uma chamada POST para o URL do webhook. A mensagem POST contém as informações da notificação em formato JSON:

```
{"NotificationId" : \<Notification Id\>,

"Target" : \<Notification Target Id\>,

"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,

"Site" : \<Site name\>}
```

Monitoramento de Alertas de Hypervisor

O Director exibe alertas para monitorar a integridade do hipervisor. Alertas do XenServer® e VMware vSphere ajudam a monitorar parâmetros e estados do hipervisor. O status da conexão com o hipervisor também é monitorado para fornecer um alerta se o cluster ou pool de hosts for reiniciado ou estiver indisponível.

Filtro de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2407/media/hypervisor_alerts_filter.png)

Para receber alertas do hipervisor, certifique-se de que uma conexão de hospedagem seja criada no Web Studio. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas para alertas do hipervisor.

Esses alertas são exibidos assim que os limites são atingidos ou excedidos. Os alertas do hipervisor podem ser:

- Crítico — limite crítico da política de alarme do hipervisor atingido ou excedido
- Aviso — limite de aviso da política de alarme do hipervisor atingido ou excedido
- Ignorado — alerta não mais exibido como um alerta ativo

Exibição de Alertas do Hipervisor(/en-us/citrix-virtual-apps-desktops/2407/media/hypervisor_alerts_display.png)

Este recurso requer o Delivery Controller versão 7 1811 ou posterior. Se você estiver usando uma versão mais antiga do Director com sites 7 1811 ou posterior, apenas a contagem de alertas do hipervisor será exibida. Para visualizar os alertas, você deve atualizar o Director.

A tabela a seguir descreve os vários parâmetros e estados dos alertas do Hypervisor.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Uso da CPU	XenServer, VMware vSphere	Hypervisor	O limite de alerta de uso da CPU é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Uso de memória	XenServer, VMware vSphere	Hypervisor	O limite de alerta de uso de memória é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de rede	XenServer, VMware vSphere	Hypervisor	O limite de alerta de uso de rede é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de disco	VMware vSphere	Hypervisor	O limite de alerta de uso de disco é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Conexão do host ou estado de energia	VMware vSphere	Hypervisor	O Host do Hypervisor foi reiniciado ou está indisponível	Os alertas são pré-construídos no VMware vSphere. Nenhuma configuração adicional é necessária.
Conexão do Hypervisor indisponível	XenServer, VMware vSphere	Delivery Controller	A conexão com o hypervisor (pool ou cluster) foi perdida, desligada ou reiniciada. Este alerta é gerado a cada hora enquanto a conexão estiver indisponível.	Os alertas são pré-construídos com o Delivery Controller. Nenhuma configuração adicional é necessária.

Nota:

Para obter mais informações sobre a configuração de alertas, consulte Alertas do Citrix XenCenter ou verifique a documentação de Alertas do VMware vCenter.

A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > Site Policy > Hypervisor Health**. As condições de limite para as políticas de alerta do Hypervisor podem ser configuradas, editadas, desativadas ou excluídas apenas do hypervisor e não do Director. No entanto, a modificação das preferências de e-mail e o descarte de um alerta podem ser feitos no Director. Você pode desativar o alerta se sua função não envolver o monitoramento da infraestrutura.

Importante:

- Os alertas acionados pelo Hypervisor são buscados e exibidos no Director. No entanto, as alterações no ciclo de vida/estado dos alertas do Hypervisor não são refletidas no Director.
- Alertas que estão íntegros, descartados ou desativados no console do Hypervisor continuam a aparecer no Director e precisam ser descartados explicitamente.
- Alertas que são descartados no Director não são descartados automaticamente no console do Hypervisor.

Monitoramento do uso de aplicativos

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

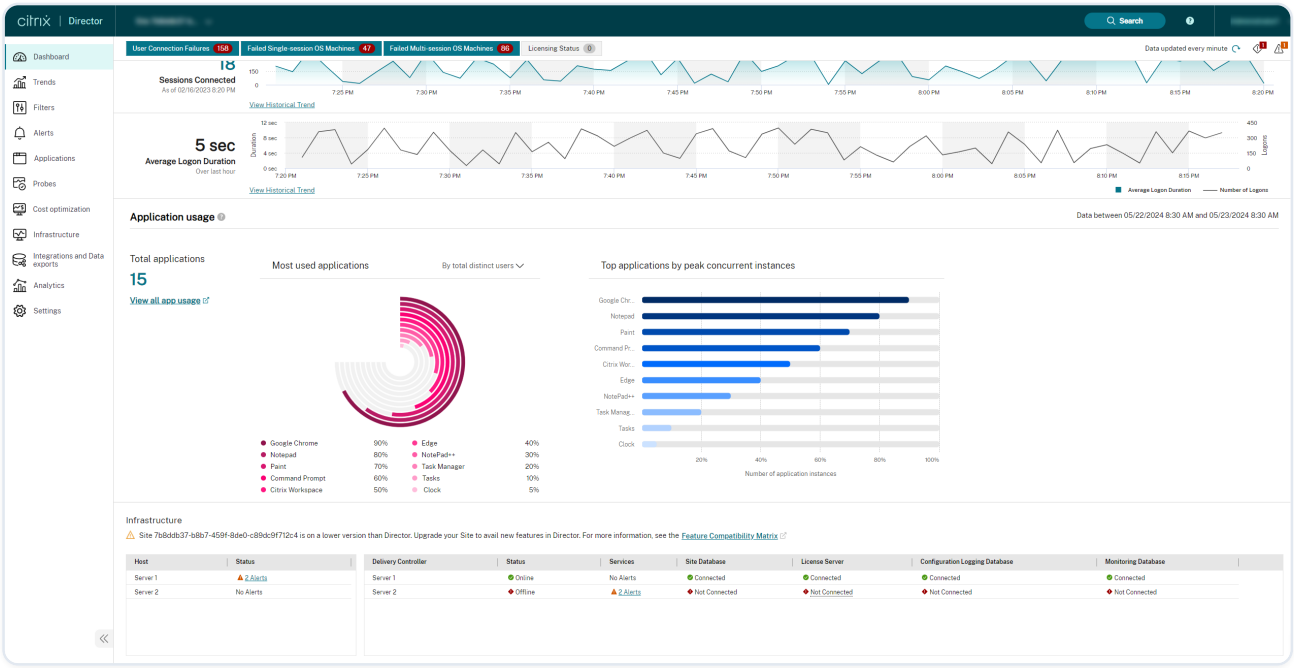
Observação:

Este recurso está disponível apenas para sites com licença Platinum.

Com este recurso, um administrador pode visualizar quais aplicativos publicados são os mais usados. Usando esses dados, os administradores podem aprofundar-se na extensão do uso. O administrador pode analisar os detalhes dos aplicativos populares nas últimas 24 horas pelos seguintes pontos de dados:

- Número total de aplicativos - Identifica o número total de aplicativos em uso por todos os usuários no site da empresa.
- Aplicativos mais usados pelo número total de usuários distintos - Identifica os 10 principais aplicativos pelo número total de usuários únicos.
- Aplicativos mais usados pelo número total de inicializações de aplicativos - Identifica os 10 principais aplicativos com base no número total de inicializações de aplicativos.
- Principais instâncias de aplicativos simultâneas de pico - Identifica os 10 principais aplicativos com base no maior número de instâncias simultâneas de uso de cada aplicativo. Esta informação fornece a demanda máxima para os aplicativos listados.

Este gráfico está presente na parte inferior da página do Painel. No entanto, você pode clicar em **Verificar** na parte superior da tela para acessar o gráfico diretamente.



Você também pode clicar em **Ver todo o uso do aplicativo** para visualizar os detalhes de um único aplicativo. Este link abre a página **Tendências** > **Gerenciamento de Capacidade** > **Uso de Aplicativos Hospedados**.

O gráfico fornece uma representação visual do uso do aplicativo. Além disso, ao passar o mouse sobre o gráfico, você obtém as contagens absolutas respectivas dos pontos de dados selecionados. Ao clicar em qualquer ponto de dados no gráfico, a página **Tendências** >

Gerenciamento de Capacidade > **Uso de Aplicativos Hospedados** é aberta com o nome do aplicativo específico selecionado. Esses dados servem para representar um valor comparativo em relação a todos os aplicativos presentes no sistema da empresa. O valor absoluto do ponto de dados também é mencionado separadamente no mesmo hover.

Filtrar dados para solucionar falhas

Quando você clica em números no Painel ou seleciona um filtro predefinido no menu Filtros, a exibição Filtros é aberta para exibir dados com base na máquina ou tipo de falha selecionado.

Filtros predefinidos não podem ser editados, mas você pode salvar um filtro predefinido como um filtro personalizado e depois modificá-lo. Além disso, você pode criar exibições filtradas personalizadas de máquinas, conexões, sessões e instâncias de aplicativos em todos os grupos de entrega.

1. Selecione uma exibição:

    - **Máquinas**. Selecione Máquinas de SO de sessão única ou Máquinas de SO de múltiplas sessões. Essas exibições mostram o número de máquinas configuradas. A guia Máquinas de SO de múltiplas sessões também inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.
    - **Sessões**. Filtre sessões por diferentes períodos de tempo, incluindo últimos 60 minutos, últimas 24 horas, últimos 7 dias ou período de tempo personalizado. Você também pode ver a contagem de sessões na exibição Sessões. Use as medições de tempo ocioso para identificar sessões que estão ociosas além de um período de tempo limite. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário. Clicar no nome do **Ponto de Extremidade** abre o Gerenciador de Atividades para o Ponto de Extremidade. Clicar em **Ver Detalhes** abre a página **Detalhes do Usuário** ou **Detalhes do Ponto de Extremidade**, respectivamente. Para obter mais informações, consulte Detalhes do Usuário.
    - **Conexões**. Filtre conexões por diferentes períodos de tempo, incluindo últimos 60 minutos, últimas 24 horas, últimos 7 dias ou período de tempo personalizado.
    - **Instâncias de Aplicativo**. Filtre instâncias de aplicativo por diferentes períodos de tempo, incluindo últimos 60 minutos, últimas 24 horas, últimos 7 dias ou período de tempo personalizado. Esta exibição mostra as propriedades de todas as instâncias de aplicativo em VDAs de Servidor e SO de sessão única. As medições de tempo ocioso da sessão estão disponíveis para instâncias de aplicativo em VDAs de SO de múltiplas sessões.

> **Nota:**
>
> Se você iniciou sessões de Área de Trabalho em VDAs instalados em um computador Windows 10 1809, o Gerenciador de Atividades no Director pode, às vezes, exibir o Microsoft Edge e o Office como aplicativos em execução ativa, enquanto eles estão, na verdade, sendo executados apenas em segundo plano.

2. Para **Filtrar por**, selecione os critérios.
3. Use as guias adicionais para cada exibição, conforme necessário, para completar o filtro.
4. Selecione colunas extras, conforme necessário, para solucionar problemas adicionais.
5. Salve e nomeie seu filtro.
6. Para acessar filtros de vários servidores Director, armazene os filtros em uma pasta compartilhada acessível a partir desses servidores:
   - A pasta compartilhada deve ter permissões de modificação para as contas no servidor Director.
   - Os servidores Director devem ser configurados para acessar a pasta compartilhada. Para configurar, execute o **IIS Manager**. Em **Sites \> Default Web Site \> Director\ > Application Settings**, modifique a configuração **Service.UserSettingsPath** para refletir o caminho UNC da pasta compartilhada.
7. Para abrir o filtro mais tarde, no menu **Filtros**, selecione o tipo de filtro (Máquinas, Sessões, Conexões ou Instâncias de Aplicativo) e, em seguida, selecione o filtro salvo.
8. Clique em **Exportar** para exportar os dados para arquivos no formato CSV. Dados de até 100.000 registros podem ser exportados. Este recurso está disponível no Delivery Controller™ versão 1808 e posterior.
9. Se necessário, para as exibições de **Máquinas** ou **Conexões**, use os controles de energia para todas as máquinas selecionadas na lista filtrada. Para a exibição de Sessões, use os controles de sessão ou a opção de enviar mensagens.
10. Nas exibições de **Máquinas** e **Conexões**, clique em **Motivo da Falha** de uma máquina ou conexão com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de Máquina e Conexão estão disponíveis em Motivos de falha e solução de problemas do Citrix Director.

11. Na exibição de **Máquinas**, clique em um link de nome de máquina para ir para a página correspondente de **Detalhes da Máquina**. Esta página exibe os detalhes da máquina, fornece controles de energia, exibe os gráficos de monitoramento de CPU, memória, disco e GPU. Além disso, clique em **Exibir Utilização Histórica** para ver as tendências de utilização de recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
12. Na exibição **Instâncias de Aplicativo**, classifique ou filtre com base no **Tempo Ocioso** maior que um período de tempo limite. Selecione a instância de aplicativo ociosa para encerrar. O Logoff ou Desconexão de uma instância de aplicativo encerra todas as instâncias de aplicativo ativas na mesma sessão. Para obter mais informações, consulte Solucionar problemas de aplicativos. A página de filtro Instâncias de Aplicativo e as medições de tempo ocioso nas páginas de filtro Sessões estão disponíveis se o Director, os Delivery Controllers e os VDAs forem da versão 7.13 ou posterior.

Nota: O Web Studio permite a atribuição de várias Regras de Atribuição de Área de Trabalho (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront™ exibe a área de trabalho atribuída com o Nome de Exibição correspondente de acordo com a DAR para o usuário logado. No entanto, o Director não oferece suporte a DARs e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear uma área de trabalho específica para uma máquina no Director. Para mapear a área de trabalho atribuída exibida no StoreFront para o nome do grupo de entrega exibido no Director, use o seguinte comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina

- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site.

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar por gráficos de tendências, ampliando um período de tempo (clicando em um ponto de dados no gráfico) e detalhando para ver os detalhes associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que é afetado.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

Escolha um período para o qual você precisa das informações de tendências históricas. A disponibilidade do período depende da sua implantação do Director da seguinte forma:

- Relatórios de tendências de até Último ano (365 dias) estão disponíveis em sites com licença Premium.
- Relatórios de tendências de até Último mês (31 dias) estão disponíveis em sites com licença Advanced.
- Relatórios de tendências de até Últimos 7 dias em sites com licença não Premium e não Advanced.

> **Observação:**

> - Em todas as implantações do Director, as informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Último mês (**Terminando agora**) ou menor. Para o período escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendências estão disponíveis como gráficos e não como tabelas.
> - Os valores de retenção de limpeza do Serviço de Monitoramento controlam a disponibilidade dos dados de tendências. Os valores padrão estão disponíveis em

Granularidade e retenção de dados. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção.

- Os seguintes parâmetros no Gerenciador do IIS controlam o intervalo de datas de término personalizadas disponíveis para seleção. No entanto, a disponibilidade dos dados para as datas selecionadas depende da configuração de retenção de limpeza para a métrica específica que está sendo medida.

PARÂMETRO	VALORES PADRÃO
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

Tendências disponíveis

Exibir tendências para sessões: Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas de Confiabilidade da Sessão ou de Reconexão Automática do Cliente estão em vigor. Quando há uma interrupção de rede no endpoint, as seguintes políticas entram em vigor:

- A confiabilidade da sessão entra em vigor (por padrão, por 3 minutos) onde o Citrix Receiver™ ou o aplicativo Citrix Workspace™ tenta se conectar ao VDA.
- A reconexão automática do cliente entra em vigor entre 3 e 5 minutos, onde o cliente tenta se conectar ao VDA.

Ambas as reconexões são capturadas e exibidas para o usuário. Essas informações podem levar no máximo 5 minutos para aparecer na interface do usuário do Director após a reconexão ter ocorrido.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções. Também analisam redes com uma experiência contínua. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período

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

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Esse recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Esse recurso requer o Delivery Controller™ versão 7 1906 ou posterior e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações de política de reconexão automática do cliente e Configurações de política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Director pelos seguintes motivos:

- O aplicativo Workspace não está enviando dados de reconexão automática para o VDA.
- O VDA não está enviando dados para o serviço de monitoramento.
- Os Delivery Controllers descartam as cargas úteis do VDA, pois podem não ter as sessões correspondentes.

> **Observação:**
>
> Às vezes, o endereço IP do cliente pode não ser obtido corretamente se certas políticas do Citrix Gateway estiverem definidas.

> **Ver tendências de falhas de conexão:** Na guia Falhas, selecione a conexão, o tipo de máquina, o tipo de falha, o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em seu site.

Ver tendências de falhas de máquina: Na guia **Falhas de Máquina de SO de Sessão Única** ou na guia Máquinas de SO de Múltiplas Sessões, selecione o tipo de falha, o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de máquina em seu site.

Ver tendências de desempenho de logon: Na guia **Desempenho de Logon**, selecione o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em seu site e se o número de logons afeta o

desempenho. Esta exibição também mostra a duração média das fases de logon, como duração de corretagem e tempo de inicialização da VM. Esses dados são especificamente para logons de usuário e não incluem usuários tentando se reconectar de sessões desconectadas. A tabela abaixo do gráfico mostra a Duração do Logon por Sessão do Usuário. Você pode escolher as colunas a serem exibidas e classificar o relatório por qualquer uma das colunas. Você também pode exportar esses relatórios para um arquivo .CSV. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

Ver tendências de avaliação de carga: Na guia **Índice do Avaliador de Carga**, visualize um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas de SO de Múltiplas Sessões. As opções de filtro para este gráfico incluem o Delivery Group ou a máquina de SO de Múltiplas Sessões em um Delivery Group, a máquina de SO de Múltiplas Sessões (disponível apenas se a máquina de SO de Múltiplas Sessões em um Delivery Group tiver sido selecionada) e o intervalo.

Ver uso de aplicativos hospedados: A disponibilidade deste recurso depende da licença da sua organização. Na guia **Gerenciamento de Capacidade**, selecione a guia **Uso de Aplicativos Hospedados**. Selecione o Delivery Group e o período para visualizar um gráfico exibindo o pico de uso simultâneo e uma tabela exibindo o uso baseado em aplicativo. Na tabela Uso Baseado em Aplicativo, você pode escolher um aplicativo específico para ver detalhes e uma lista de usuários que estão usando ou usaram o aplicativo.

Ver uso de SO de Sessão Única e Múltiplas Sessões: A exibição Tendências mostra o uso de SO de Sessão Única por site e por Delivery Group. Ao selecionar **Site**, o uso é mostrado por Delivery Group. Ao selecionar Delivery Group, o uso é mostrado por Usuário. A exibição Tendências também mostra o uso de SO de Múltiplas Sessões por site, por Delivery Group e por Máquina. Ao selecionar **Site**, o uso é mostrado por Delivery Group. Ao selecionar Delivery Group, o uso é mostrado por Máquina e por Usuário. Quando Máquina é selecionada, o uso é mostrado por Usuário.

Ver uso de máquina virtual: Na guia **Uso da Máquina**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter uma visualização em tempo real do uso da sua VM, permitindo que você avalie rapidamente as necessidades de capacidade do seu site. Disponibilidade de SO de Sessão Única - exibe o estado atual das máquinas de SO de Sessão Única (VDIs) por disponibilidade para todo o site ou um Delivery Group específico. Disponibilidade de SO de Múltiplas Sessões - exibe o estado atual das máquinas de SO de Múltiplas Sessões por disponibilidade para todo o site ou um Delivery Group específico.

Nota: O número de máquinas exibidas em Contador Disponível inclui máquinas em modo de manutenção.

Ver utilização de recursos: Na guia **Utilização de Recursos**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter informações sobre dados de tendências históricas para uso de CPU e memória, e IOPS e latência de disco para cada máquina VDI para um melhor planejamento de capacidade. Este recurso requer Delivery Controllers e VDAs **versão 7.11** ou posterior. Os gráficos mostram dados para CPU média, memória média, IOPS médio, latência de disco e pico de sessões simultâneas. Você pode detalhar a máquina e visualizar dados e gráficos para os 10 principais processos que consomem CPU.

Filtre por Delivery Group e Período. Os gráficos de uso de CPU, memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, mês e ano. Os gráficos de IOPS médio e latência de disco estão disponíveis para as últimas 24 horas, mês e ano.

Observação:

- A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como **Permitido** para coletar e exibir dados na tabela dos 10 Principais Processos na página Utilização Histórica da Máquina. A política é definida como **Proibido** por padrão. Todos os dados de utilização de recursos são coletados por padrão. Isso pode ser desabilitado usando a configuração da política **Habilitar Monitoramento de Recursos**. A tabela abaixo dos gráficos mostra os dados de utilização de recursos por máquina. Para obter mais informações, consulte Configurações da política de monitoramento.
- O IOPS médio mostra as médias diárias. O IOPS de pico é calculado como o maior das médias de IOPS para o intervalo de tempo selecionado. (Uma média de IOPS é a média horária de IOPS coletados durante a hora no VDA).
- O detalhamento da máquina lista processos com uso médio de CPU ou memória média superior a 1%, o que pode significar que, às vezes, menos de 10 processos são listados.

Ver dados de análise de rede: A disponibilidade deste recurso depende da licença da sua organização e das suas permissões de administrador. Este recurso requer Delivery Controllers **versão 7.11** ou posterior.

Na guia **Rede**, monitore sua análise de rede, que fornece uma visão contextual de usuário, aplicativo e desktop da rede. Com este recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação por meio de relatórios HDX Insight do Citrix ADM. Para obter mais informações, consulte Configurar análise de rede

Visualizar falhas de aplicativo: A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de múltiplas sessões executando Windows Server 2008 e posterior são suportados. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas falhas de aplicativo de VDAs de SO de múltiplas sessões são exibidas. Você pode configurar o monitoramento de falhas de aplicativo usando políticas de Monitoramento. Para obter mais informações, consulte Configurações de política de monitoramento.

Visualizar resultados da sondagem: A guia **Resultados da Sondagem** exibe os resultados da sondagem para aplicativos e desktops que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha ocorreu é registrado.

Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

Criar relatórios personalizados: A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados em tempo real e históricos do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatório Personalizado salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente, ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique condições de filtro com base em campos como máquina, Grupo de Entrega ou período de tempo. Especifique colunas adicionais necessárias em seu Relatório Personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta de Relatório Personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta de Relatório Personalizado com base em uma consulta OData copiada. Para fazer isso, selecione a opção Consulta OData e cole a consulta OData copiada. Você pode salvar a consulta resultante para execução posterior.

Nota: Os nomes das colunas no relatório de Visualização e Exportação gerado usando consultas OData não são localizados, mas aparecem em inglês.

Os ícones de bandeira no gráfico indicam eventos ou ações significativas para aquele intervalo de tempo específico. Passe o mouse sobre a bandeira e clique para listar eventos ou ações.

Observação:

- Os dados de logon de conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
- Os Grupos de Entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros de Tendências do Director até que os dados relacionados a eles sejam removidos. A seleção de um Grupo de Entrega excluído exibe gráficos para os dados disponíveis até a retenção. No entanto, as tabelas não mostram dados.
- Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro faz com que as tabelas de **Utilização de Recursos e Índice do Avaliador de Carga** do novo Grupo de Entrega exibam métricas consolidadas dos Grupos de Entrega antigo e novo.

Monitorar máquinas gerenciadas pelo Autoscale

Autoscale é um recurso de gerenciamento de energia que permite o gerenciamento proativo de energia de todas as máquinas de SO de sessão única e multissessão registradas em um grupo de entrega. Você pode configurar o Autoscale para um grupo de entrega selecionado no Web Studio. Para obter mais informações, consulte Autoscale. Você pode monitorar as principais métricas das máquinas habilitadas para Autoscale usando o Director.

Uso da Máquina

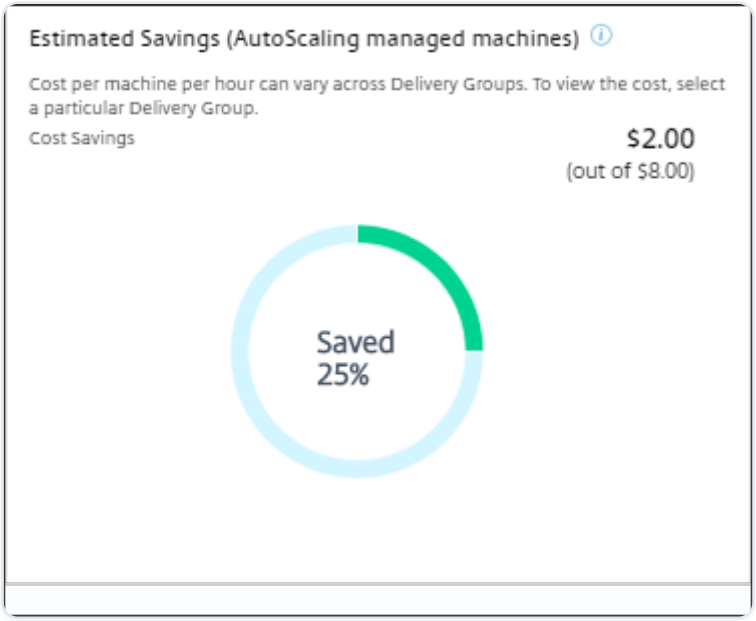
A página **Uso da Máquina** exibe o número total de máquinas de SO de sessão única e multissessão habilitadas para Autoscale que estão ligadas para um grupo de entrega e período de tempo selecionados. Essa métrica indica o uso real das máquinas no grupo de entrega. Na guia **Máquinas de SO de sessão única** ou **Máquinas de SO multissessão**, selecione o grupo de entrega e o período de tempo.

O gráfico plota as seguintes métricas:

- **Máquinas Ligadas** - o número de máquinas habilitadas para Autoscale que estão ligadas
- **Máquinas Registradas** - o número de máquinas de SO de sessão única ou multissessão registradas
- **Máquinas em Manutenção** - o número de máquinas de SO de sessão única ou multissessão com o modo de manutenção ativado

Economia Estimada

A página **Uso da Máquina** também exibe a economia de custos estimada alcançada ao habilitar o Autoscale no grupo de entrega selecionado.



A Economia Estimada é calculada como a porcentagem de economia por máquina por hora (em US$) conforme configurado em **Editar Grupo de Entrega** > **Autoscale**. Para obter mais informações sobre como configurar a economia por máquina, consulte Autoscale.

Quando você seleciona todos os grupos de entrega, o valor médio da Economia Estimada em todos os grupos de entrega é exibido.

A economia estimada ajuda os administradores a consolidar a infraestrutura existente e planejar a capacidade para alcançar a máxima economia e utilização.

Notificações de alerta para máquinas e sessões

O Painel do Director exibe notificações de alerta que podem ser detalhadas. Os detalhes do alerta são exibidos na página **Alertas**.

- Para criar uma política de alerta em um grupo de entrega, vá para **Alertas** > **Política de Alertas Citrix** > **Política de Grupo de Entrega**.
- Aqui, você pode definir os seguintes limites de Aviso e Crítico:
  - Máquinas com Falha (SO de sessão única) e Máquinas com Falha (SO de múltiplas sessões),
  - Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico no grupo de entrega.
- Os alertas são gerados quando a métrica correspondente no grupo de entrega atinge o limite.

Para mais detalhes sobre as condições da política de alerta e a criação de novas políticas de alerta, consulte Alertas e notificações.

Status da máquina

- **Filtros** > **Máquinas** exibe o estado de energia de todas as máquinas em formato tabular. Você pode filtrar por um grupo de entrega específico.
- **Filtros** > **Sessões** exibe o filtro pelo nome da Máquina para ver as sessões associadas e seu status em tempo real.
- Em **Tendências** > **Sessões**, selecione seu grupo de entrega e período para ver a tendência das sessões e suas métricas associadas.

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

Tendências de Avaliação de Carga

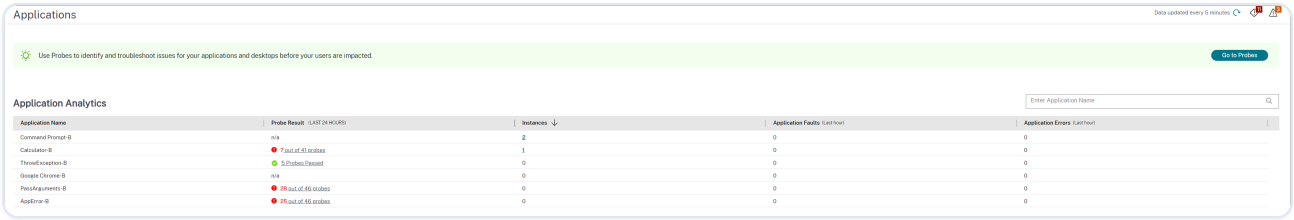
A página **Tendências** > **Índice do Avaliador de Carga** exibe um gráfico com informações detalhadas sobre a carga distribuída entre as máquinas de SO de múltiplas sessões. As opções de filtro para este gráfico incluem o grupo de entrega ou máquina de SO de múltiplas sessões em um grupo de entrega, máquina de SO de múltiplas sessões (disponível apenas se a máquina de SO de múltiplas sessões em um grupo de entrega foi selecionada) e intervalo. O Índice do Avaliador de Carga é exibido como porcentagens de CPU Total, Memória, Disco ou Sessões e é mostrado em comparação com o número de usuários conectados no último intervalo.

Solucionar problemas de implantações

Solucionar problemas de aplicativos

Análise de Aplicativos

A exibição **Aplicativos** exibe análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. A exibição padrão ajuda a identificar os principais aplicativos em execução. Este recurso requer Delivery Controllers Versão 7.16 ou posterior e VDAs Versão 7.15 ou posterior.



A coluna **Resultado da Sondagem** exibe o resultado da sondagem de aplicativos executada nas últimas 24 horas. Clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** \> **Resultados da Sondagem de Aplicativos**. Para obter mais detalhes sobre como configurar sondagens de aplicativos, consulte Sondagem de Aplicativos e Desktops.

A coluna **Instâncias** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativos atualmente em execução (instâncias conectadas e desconectadas). Para solucionar problemas adicionais, clique no campo **Instâncias** para ver a página de filtros **Instâncias de Aplicativos** correspondente. Aqui, você pode selecionar instâncias de aplicativos para fazer logoff ou desconectar.

> **Observação:**
>
> Para administradores de escopo personalizado, o Director não exibe instâncias de aplicativos criadas em grupos de aplicativos. Para visualizar todas as instâncias de aplicativos, você deve ser um administrador completo. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX256001.

> Monitore a integridade dos aplicativos publicados em seu site com as colunas **Falhas de Aplicativos** e **Erros de Aplicativos**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao iniciar o aplicativo correspondente na última hora. Clique no campo

> **Falhas de Aplicativos** ou **Erros de Aplicativos** para ver os detalhes da falha na página **Tendências** \> **Falhas de Aplicativos** correspondente ao aplicativo selecionado.

As configurações da política de falha de aplicativo governam a disponibilidade e a exibição de falhas e erros. Para obter mais informações sobre as políticas e como modificá-las, consulte Políticas para monitoramento de falhas de aplicativos nas configurações de **política de monitoramento**.

Monitoramento de aplicativos em tempo real

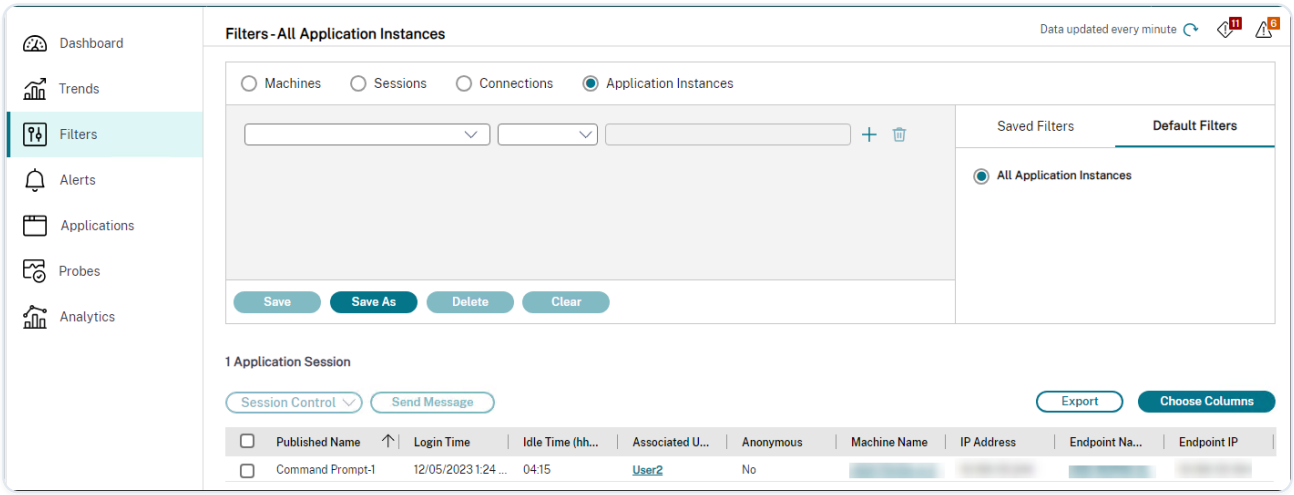
Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas baseada em aplicativos são no setor de saúde, onde os funcionários compartilham licenças de aplicativos. Lá, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente Citrix Virtual Apps and Desktops™, reconfigurar servidores com baixo desempenho ou manter e atualizar aplicativos.

A página de filtro **Instâncias de Aplicativos** lista todas as instâncias de aplicativos em VDAs de SO de Servidor e de Sessão Única. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativos em VDAs de SO de Múltiplas Sessões que estiveram ociosas por pelo menos 10 minutos.

> **Nota:** As métricas de Instâncias de Aplicativos estão disponíveis em sites de todas as edições de licença.

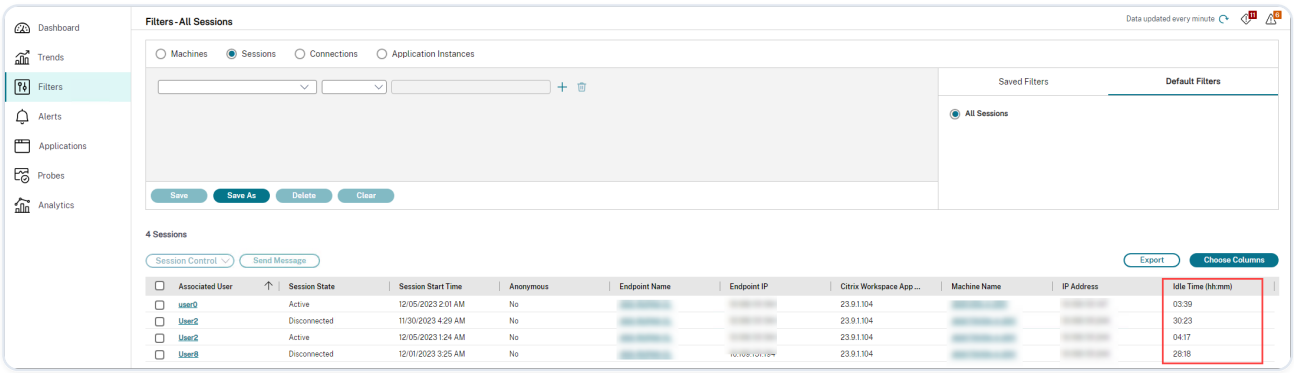
> Use essas informações para identificar as instâncias de aplicativos que estão ociosas além de um período de tempo específico e faça logoff ou desconecte-as conforme apropriado. Para fazer isso, selecione **Filtros \> Instâncias de Aplicativos** e selecione um filtro pré-salvo ou escolha **Todas as Instâncias de Aplicativos** e crie seu próprio filtro.



Um exemplo de filtro seria o seguinte. Como critérios de **Filtrar por**, escolha **Nome Publicado** (do aplicativo) e **Tempo Ocioso**. Em seguida, defina **Tempo Ocioso** como **maior ou igual a** um limite de tempo específico e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias do aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Controle de Sessão**, escolha **Logoff** ou **Desconectar** para encerrar as instâncias.

> **Nota:** Fazer logoff ou desconectar uma instância de aplicativo faz logoff ou desconecta a sessão atual, encerrando assim todas as instâncias de aplicativo que pertencem à mesma sessão.

Você pode identificar sessões ociosas na página de filtro **Sessões** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Tempo Ocioso** ou defina um filtro para identificar sessões que estão ociosas além de um limite de tempo específico. O tempo ocioso é listado para sessões em VDAs de SO de múltiplas sessões que estiveram ociosas por pelo menos 10 minutos.



O **Tempo ocioso** é exibido como **N/A** quando a sessão ou instância do aplicativo

- não esteve ociosa por mais de 10 minutos,
- é iniciada em um VDA de SO de sessão única, ou

- é iniciada em um VDA executando a Versão 7.12 ou anterior.

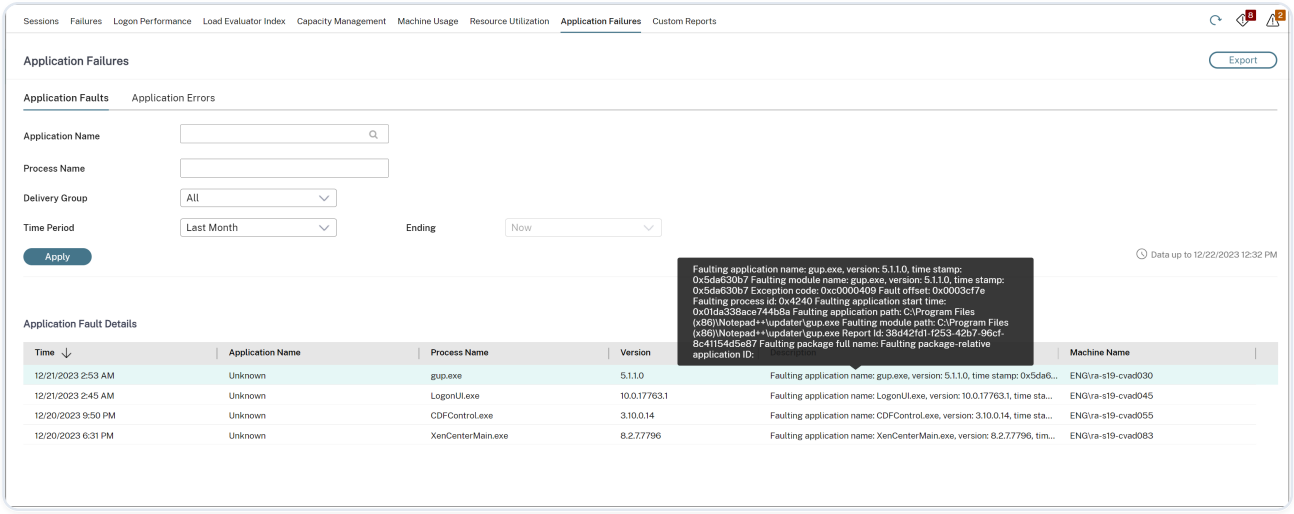
Monitoramento histórico de falhas de aplicativos

A guia **Tendências** -\> **Falhas de Aplicativos** exibe falhas associadas aos aplicativos publicados nos VDAs.

As tendências de falha de aplicativos estão disponíveis para as últimas 2 horas, 24 horas, 7 dias e mês para sites com licença Premium e Advanced. Elas estão disponíveis para as últimas 2 horas, 24 horas e 7 dias para outros tipos de licença. As falhas de aplicativos que são registradas no Visualizador de Eventos com a origem "Erros de Aplicativo" são monitoradas. Clique em **Exportar** para gerar relatórios nos formatos CSV, Excel ou PDF.

As configurações de retenção de limpeza para monitoramento de falhas de aplicativos, GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays, são definidas como um dia por padrão para sites com licença Premium e não Premium. Você pode alterar essa configuração usando o comando PowerShell:

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```



As falhas são exibidas como **Falhas de Aplicativo** ou **Erros de Aplicativo** com base em sua gravidade. A guia Falhas de Aplicativo exibe falhas associadas à perda de funcionalidade ou dados. Erros de Aplicativo indicam problemas que não são imediatamente relevantes; eles significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Nome do Aplicativo Publicado**, **Nome do Processo** ou **Grupo de Entrega** e **Período de Tempo**. A tabela exibe o código da falha ou erro e uma breve descrição da falha. A descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:** O nome do aplicativo publicado é exibido como “Desconhecido” quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de desktop ou quando falha devido a uma exceção não tratada causada por um executável dependente.

> Por padrão, apenas falhas de aplicativos hospedados em VDAs de SO de múltiplas sessões são monitoradas. Você pode modificar as configurações de monitoramento por meio das Políticas de Grupo de Monitoramento: Habilitar monitoramento de falhas de aplicativos, Habilitar monitoramento de falhas de aplicativos em VDAs de SO de sessão única e Lista de aplicativos excluídos do monitoramento de falhas. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da política de monitoramento.

A página **Tendências \> Resultados da Sondagem de Aplicativos** exibe os resultados da sondagem de aplicativos executada no site nas últimas 24 horas e 7 dias. Para obter mais detalhes sobre como configurar sondagens de aplicativos, consulte Sondagem de Aplicativos.

Solucionar problemas de máquinas

> **Observação:**

> **Citrix Health Assistant** é uma ferramenta para solucionar problemas de configuração em VDAs não registrados. A ferramenta automatiza várias verificações de integridade para identificar possíveis causas raiz para falhas de registro de VDA e problemas no lançamento de sessão e na configuração de redirecionamento de fuso horário. O artigo da Central de Conhecimento, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém o download da ferramenta **Citrix Health Assistant** e instruções de uso.

> A exibição **Filtros > Máquinas** no console do Director exibe as máquinas configuradas no site. A guia Máquinas de SO de Múltiplas Sessões inclui o índice do avaliador de carga, que indica a distribuição dos contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.

Clique na coluna **Motivo da Falha** de uma máquina com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e

as ações recomendadas para falhas de máquina e conexão estão disponíveis em Citrix Director failure reasons and troubleshooting.

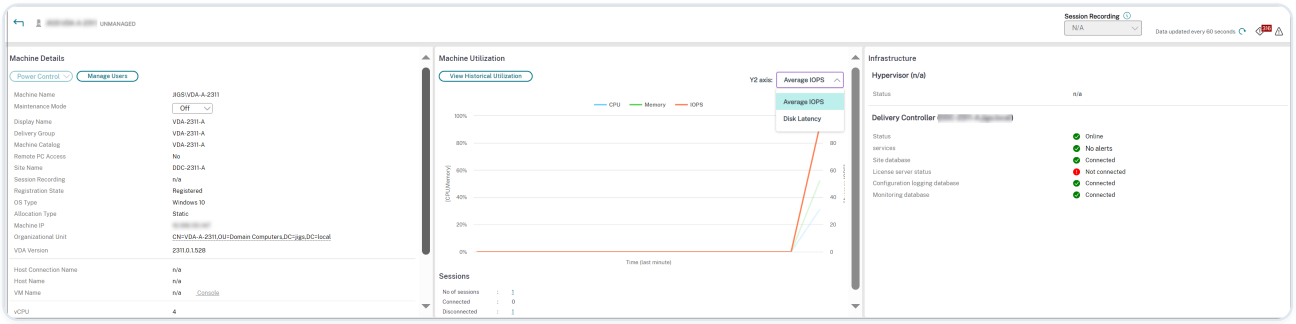
Clique no link do nome da máquina para ir para a página **Detalhes da Máquina**.

A página Detalhes da Máquina lista os detalhes da máquina, detalhes da infraestrutura e detalhes dos hotfixes aplicados na máquina.

Utilização de recursos em tempo real baseada em máquina

O painel **Utilização da Máquina** exibe gráficos mostrando a utilização em tempo real da CPU e da memória. Além disso, gráficos de monitoramento de disco e GPU estão disponíveis para sites com Delivery Controllers e versões de VDA **7.14** ou posteriores.

Gráficos de monitoramento de disco, IOPS médio e latência de disco são medidas de desempenho importantes que ajudam a monitorar e solucionar problemas relacionados a discos VDA. O gráfico de IOPS Médio exibe o número médio de leituras e gravações em um disco. Selecione **Latência do Disco** para ver um gráfico do atraso entre uma solicitação de dados e seu retorno do disco, medido em milissegundos.



Utilização da GPU

Selecione **Utilização da GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do Codificador e do Decodificador para solucionar problemas relacionados à GPU em VDAs de SO de múltiplas sessões e de sessão única.

Versões de GPU compatíveis:

- GPUs NVIDIA Tesla M60 executando a versão 369.17 ou posterior do Display Driver. Para obter mais informações, consulte NVIDIA vGPU Software.
- GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12(Rome). Para obter mais informações, consulte AMD Drivers and Support.

Drivers:

Os drivers ou extensões apropriados devem ser instalados nos VDAs.

- Para GPUs NVIDIA, instale os drivers GRID manualmente ou via extensões. Para obter mais informações, consulte NVIDIA vGPU Software.
    - Para NVIDIA, apenas os drivers GRID são suportados. Os drivers CUDA não funcionam com a série NVadsA10 v5 e não são suportados.
    - Para um processo de exemplo de instalação de drivers de GPU NVIDIA Grid via extensões em máquinas baseadas no Azure, consulte NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
    - Para um processo de exemplo de instalação manual de drivers de GPU NVIDIA Grid, consulte Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Para GPUs AMD, instale os drivers gráficos AMD manualmente ou via extensões. Para obter mais informações, consulte AMD Drivers and Support.
    - Para um processo de exemplo de instalação de drivers de GPU AMD via extensões em máquinas baseadas no Azure, consulte AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
    - Para um processo de exemplo de instalação manual de drivers de GPU AMD em máquinas Azure, consulte Install AMD GPU drivers on N-series VMs running Windows.

Notas de Uso:

- Os gráficos de Utilização da GPU estão disponíveis apenas para VDAs que executam Windows de 64 bits.
- Os VDAs devem ter o HDX 3D Pro habilitado para fornecer aceleração de GPU. Para obter mais informações, consulte GPU acceleration for Windows Single-session OS e GPU acceleration for Windows Multi-session OS.
- Quando um VDA acessa mais de uma GPU, o gráfico de utilização exibe a média das métricas de GPU coletadas das GPUs individuais. As métricas de GPU são coletadas para todo o VDA e não para processos individuais.
- Para AMD, o uso do codificador e decodificador não é suportado separadamente. Qualquer carga de trabalho de codificação/decodificação usando a GPU será relatada como a carga 3D geral no uso da GPU.
- Certifique-se de instalar o NVIDIA WMI durante a instalação. Esta janela está disponível apenas durante a instalação manual.
- Se os drivers estiverem instalados, mas o Director não detectar a GPU

    - Verifique o Gerenciador de Tarefas. Se os drivers estiverem instalados corretamente, a GPU deverá aparecer no Gerenciador de Tarefas.
    - Verifique se a máquina está registrada. Às vezes, as máquinas podem levar algum tempo para serem detectadas como online.

- Se o uso da GPU não mostrar atividade no Director, certifique-se de que a carga de trabalho que você está executando esteja usando a GPU. Para cargas de trabalho gráficas, isso pode ser ativado em Configurações > Sistema > Tela > Configurações de gráficos > Escolha o aplicativo para definir a preferência. Certifique-se de ativar o Alto Desempenho. Às vezes, o Windows usa a CPU por padrão para cargas de trabalho gráficas quando isso é definido como padrão do sistema ou economia de energia, com base em outras configurações.
- Os dados são atualizados a cada minuto e a visualização dos dados começa em um minuto após a seleção de **Utilização da GPU**.

Utilização histórica de recursos baseada em máquina

No painel **Utilização da Máquina**, clique em **Exibir Utilização Histórica** para ver o uso histórico de recursos na máquina selecionada. Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, sessões simultâneas de pico, IOPS médio e latência de disco.

> **Observação:**

> A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como Permitido para coletar e exibir dados na tabela Top 10 Processos na página Utilização Histórica da Máquina. A coleta é proibida por padrão.

> Os dados de utilização de CPU e memória, IOPS médio e latência de disco são coletados por padrão. Você pode desabilitar a coleta usando a configuração de política **Habilitar Monitoramento de Recursos**.



1. No painel **Utilização da Máquina** na exibição **Detalhes da Máquina**, selecione **Exibir Utilização Histórica**.
2. Na página **Utilização Histórica da Máquina**, defina o **Período de Tempo** para visualizar o uso das últimas 2 horas, 24 horas, 7 dias, mês ou ano.

> **Observação:**
>
> Os dados de uso de IOPS médio e latência de disco estão disponíveis apenas para as últimas 24 horas, mês e ano terminando agora. Horário de término personalizado não é suportado.

3. Clique em **Aplicar** e selecione os gráficos necessários.
4. Passe o mouse sobre diferentes seções do gráfico para ver mais informações para o período de tempo selecionado.



Por exemplo, se você selecionar **Últimas 2 horas**, o período de linha de base são as 2 horas anteriores ao intervalo de tempo selecionado. Visualize a tendência de CPU, memória e sessão nas últimas 2 horas e no tempo de linha de base. Se você selecionar **Último mês**, o período de linha de base é o mês anterior. Selecione para visualizar a média de IOPS e a latência de disco no último mês e no tempo de linha de base.

1. Clique em **Exportar** para exportar os dados de utilização de recursos para o período selecionado. Para obter mais informações, consulte a seção Exportar relatórios em Monitorar Implantações.
2. Abaixo dos gráficos, a tabela lista os 10 principais processos com base na utilização de CPU ou memória. Você pode classificar por qualquer uma das colunas, que mostram Nome do Aplicativo, Nome de Usuário, ID da Sessão, CPU Média, Pico de CPU, Memória Média e Pico de Memória no intervalo de tempo selecionado. As colunas IOPS e Latência de Disco não podem ser classificadas.

   > **Observação:**
   >
   > O ID da sessão para processos do sistema é exibido como "0000".

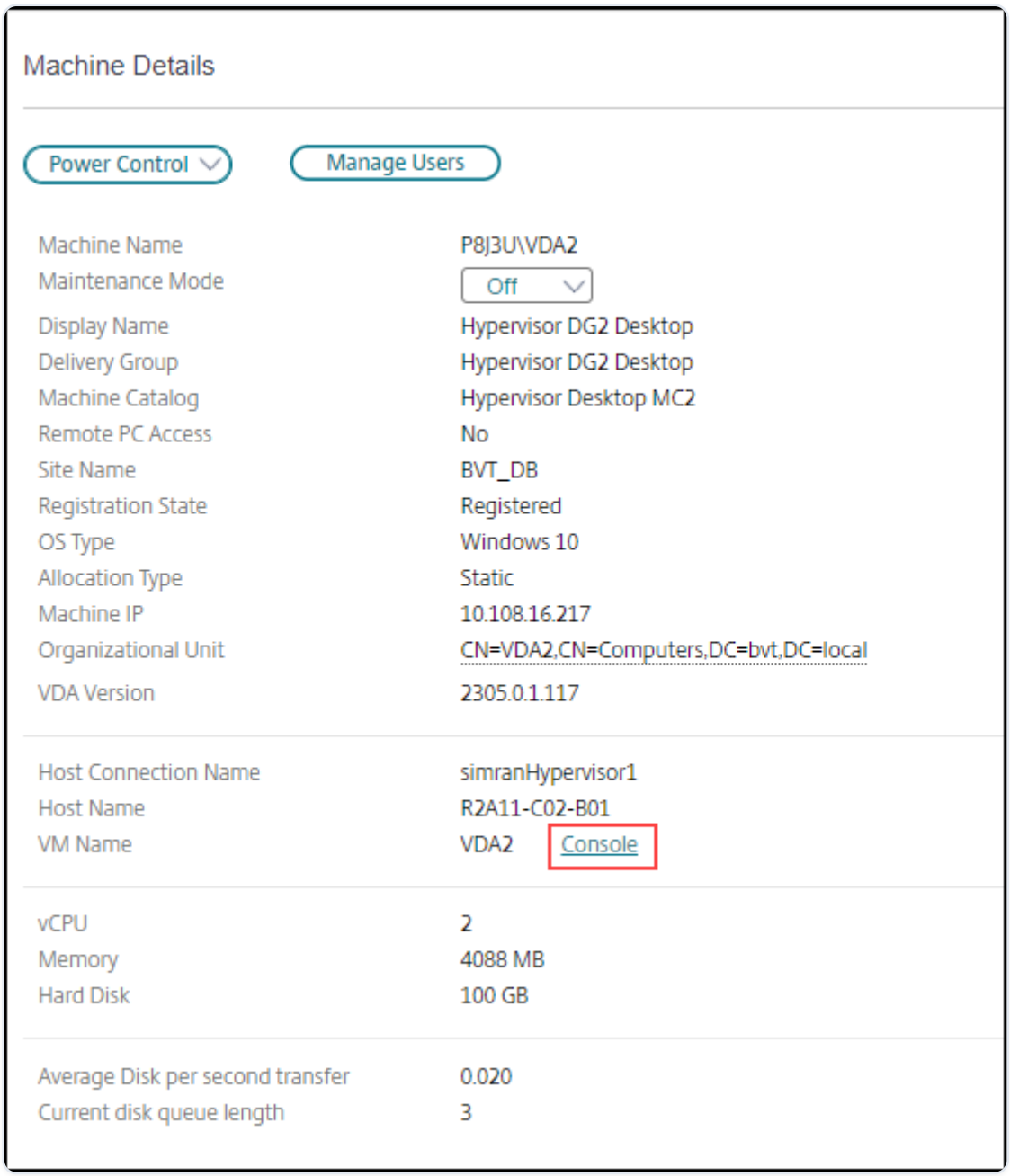
3. Para visualizar a tendência histórica do consumo de recursos de um processo específico, explore qualquer um dos 10 principais processos.

Acesso ao Console da Máquina

Você pode acessar os consoles de máquinas de SO de sessão única e multi-sessão hospedadas no XenServer Versão 7.3 e posterior diretamente do Director. Dessa forma, você não precisa do

XenCenter para solucionar problemas em VDAs hospedados no XenServer. Para que este recurso esteja disponível:

- É necessário o Delivery Controller Versão 7.16 ou posterior.
- O XenServer que hospeda a máquina deve ser da Versão 7.3 ou posterior e deve estar acessível a partir da interface do usuário do Director.



Para solucionar problemas em uma máquina, clique no link **Console** no painel Detalhes da Máquina correspondente. Após a autenticação das credenciais do host que você fornecer, o console da máquina é aberto em uma nova guia usando noVNC, um cliente VNC baseado na web. Agora você tem acesso ao console com teclado e mouse.

Observação:

- Este recurso não é compatível com o Internet Explorer 11.
- Se o ponteiro do mouse no console da máquina estiver desalinhado, consulte CTX230727 para obter as etapas para corrigir o problema.
- O Director inicia o acesso ao console em uma nova guia, certifique-se de que as configurações do seu navegador permitam pop-ups.
- Por motivos de segurança, a Citrix® recomenda que você instale certificados SSL em seu navegador.

Inspecionar máquinas com ações de energia recentes

Agora você pode inspecionar máquinas com o status das ações de energia bem-sucedidas e falhas. Este recurso ajuda você a analisar o seguinte:

- Falha ao ligar que causa problemas ao usuário
- Falha ao desligar que aumenta o custo

Observação:

Os dados estão disponíveis apenas para a máquina com gerenciamento de energia. Os dados não estão disponíveis para as ações de energia realizadas antes que o recurso fosse suportado.

Você pode visualizar o status da ação de energia das máquinas das seguintes maneiras:

Na guia **Filtros** -> **Máquinas**. Nesse caso, por padrão, as colunas **Hora da Ação de Energia** e **Resultado da Ação de Energia** ficam visíveis. Você também pode selecionar as colunas que deseja que fiquem visíveis.

Na guia **Otimização de Custos**. Neste caso, o filtro padrão **Ação de Energia Acionada Por** é definido como *Autoscale*™ e o **Resultado da Ação de Energia** é definido como *Falha*.

Com este recurso, você pode visualizar os detalhes dos controles de ação de energia. Por exemplo, você pode visualizar quem acionou a ação, qual ação alterou o estado de energia, o

motivo da falha e a hora em que a ação foi concluída. Você também pode exportar esses detalhes.

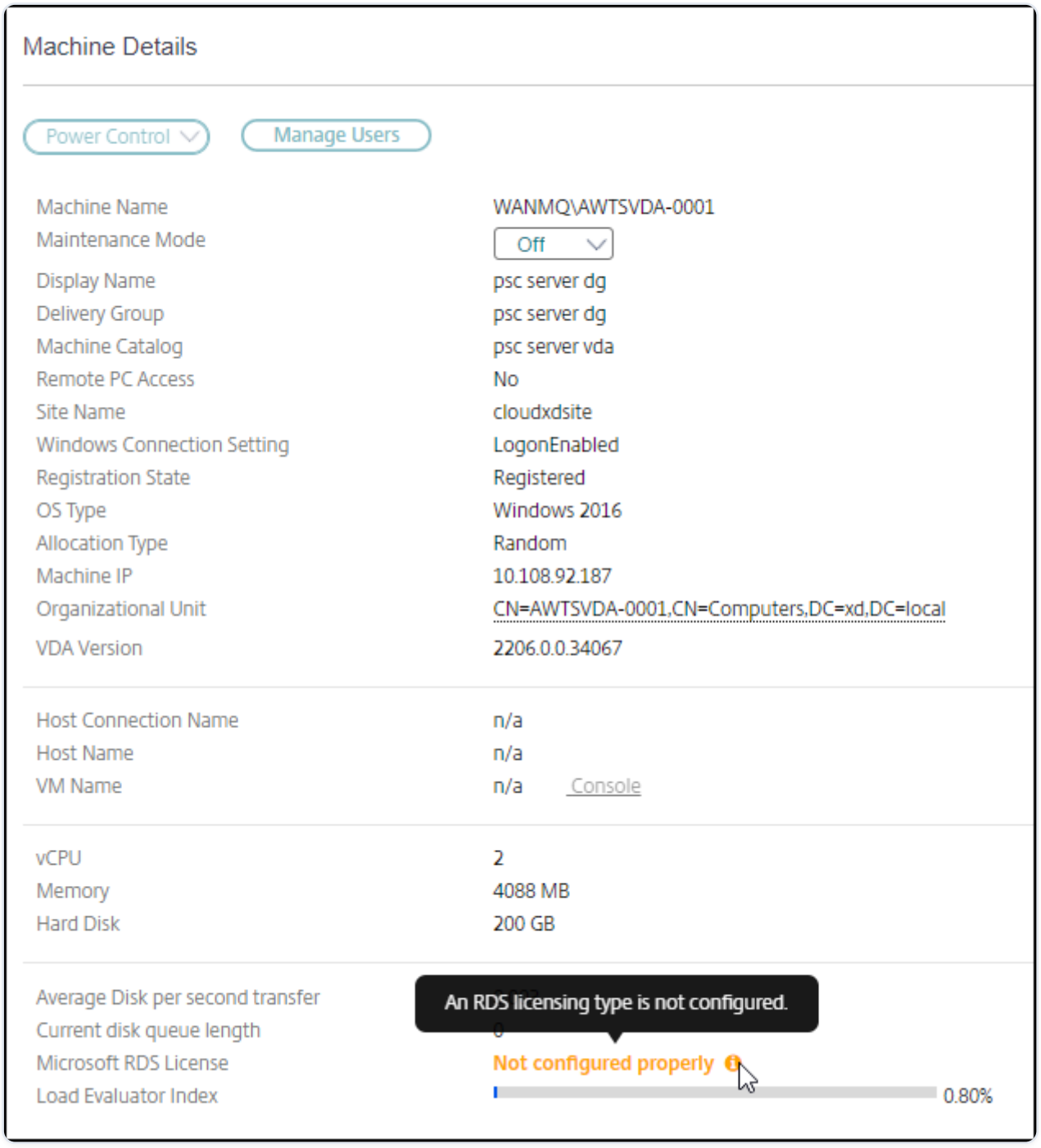
Os seguintes filtros são adicionados para visualizar o status da ação de energia:

FILTRO	DESCRIÇÃO
Resultado da Ação de Energia	Exibe o resultado da ação de energia. Os valores de filtro possíveis são sucesso e falha.
Ação de Energia Acionada Por	Exibe quem ou o que acionou a ação de energia. Os possíveis valores de filtro são os seguintes
	• Autoscale - Este valor aparece quando uma ação de energia é acionada pelo seguinte
	• Quando o administrador desliga uma VM para limpar o disco do SO da VM de volta ao seu estado inicial
	• Quando uma VM é desligada ou suspensa com base nas políticas definidas
	• Quando uma VM é disponibilizada com base no tamanho do pool ou na configuração do tamanho do buffer
	• Administrador - Este valor aparece quando uma ação de energia é acionada por um administrador. Os exemplos possíveis são quando o administrador solicita desligar, ligar, suspender,

FILTRO	DESCRIÇÃO
	retomar, reiniciar ou reinicializar uma VM.
	• Usuário - Este valor aparece quando uma ação de energia é acionada por um usuário. Os exemplos são quando um usuário redefine, liga ou retoma o trabalho na VM.
	• Outros - Este valor aparece quando a ação de energia é acionada por motivos programados e desconhecidos.
Última Ação de Energia	Exibe a ação de energia exata que ocorreu na máquina, como ligar, desligar, encerrar, reiniciar, redefinir, retomar
Hora da Ação de Energia	A hora em que a ação de energia é concluída. Os possíveis valores de filtro são último minuto, últimos 5 minutos, últimos 30 minutos, última hora, hoje, últimas 24 horas e ontem.
Motivo da Falha da Ação de Energia	Exibe o motivo da falha. Os possíveis valores de filtro são falha relatada pelo hipervisor, limite de taxa do hipervisor excedido, erro desconhecido e nenhum. Se houver uma ação bem-sucedida, ele mostra "Nenhum".

Integridade da licença RDS da Microsoft

Você pode visualizar o status da licença RDS da Microsoft no painel **Detalhes da Máquina** nas páginas **Detalhes da Máquina** e **Detalhes do Usuário** para máquinas com SO de múltiplas sessões.



Uma das seguintes mensagens é exibida:

- Licença disponível
- Não configurado corretamente (aviso)
- Erro de licença (erro)
- Versão VDA incompatível (erro)

> **Observação:**

O status de integridade da licença RDS da Microsoft para máquinas em período de carência com licença válida exibe uma mensagem **Licença disponível** em verde. Renove suas licenças antes que elas expirem.

Para mensagens de aviso e erro, passe o mouse sobre o ícone de informações para visualizar informações adicionais, conforme indicado na tabela a seguir.

TIPO DE MENSAGEM	MENSAGENS NO DIRECTOR
Erro	Disponível para VDAs versão 7.16 e posterior.
Erro	Novas conexões RDS não são permitidas.
Erro	A licença Microsoft RDS excedeu seu período de carência.
Erro	Um Servidor de Licenças não está configurado para o nível de SO exigido com o tipo de licenciamento Per Device Client Access.
Erro	O Servidor de Licenças configurado é incompatível com o nível de SO do Host RDS com o tipo de licenciamento Per Device Client Access.
Aviso	Personal Terminal Server não é um tipo de licenciamento RDS válido em uma implantação Citrix Virtual Apps and Desktops™.
Aviso	Remote Desktop for Administration não é um tipo de licenciamento válido em uma implantação Citrix Virtual Apps and Desktops.
Aviso	Um tipo de licenciamento RDS não está configurado.
Aviso	O Controlador de Domínio ou Servidor de Licenças está inacessível com o tipo de licenciamento RDS Per User Client Access.

TIPO DE MENSAGEM	MENSAGENS NO DIRECTOR
Aviso	Com o tipo de licenciamento Per Device Client Access, a licença Client Device não pode ser determinada, pois o servidor de licenças para o nível de SO exigido está inacessível.

Observação:

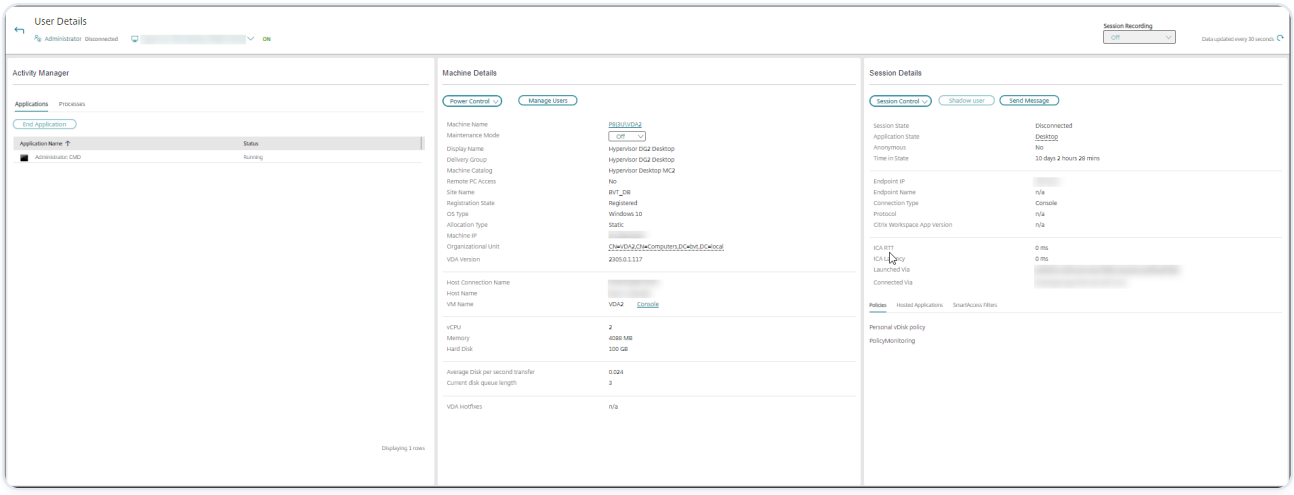
Este recurso é aplicável apenas para Microsoft RDS CAL (Client Access License).

Solucionar problemas do usuário

Use a exibição **Help Desk** do Director (página **Activity Manager**) para visualizar informações sobre o usuário ou a sessão:

Detalhes do usuário(/en-us/citrix-virtual-apps-desktops/2407/media/dir-user-details-summary.png)

Clicar em **View Details** no Activity Manager para um usuário abre a página **User Details**. Clicar em **View Details** no Activity Manager para um endpoint abre a página **Endpoint Details**.



Seletor de sessão

Se o usuário iniciou várias sessões, o seletor de sessão ajuda a selecionar uma sessão.

Seletor de sessão(/en-us/citrix-virtual-apps-desktops/2407/media/dir-session-selector.png)

Escolha uma sessão para visualizar os detalhes.

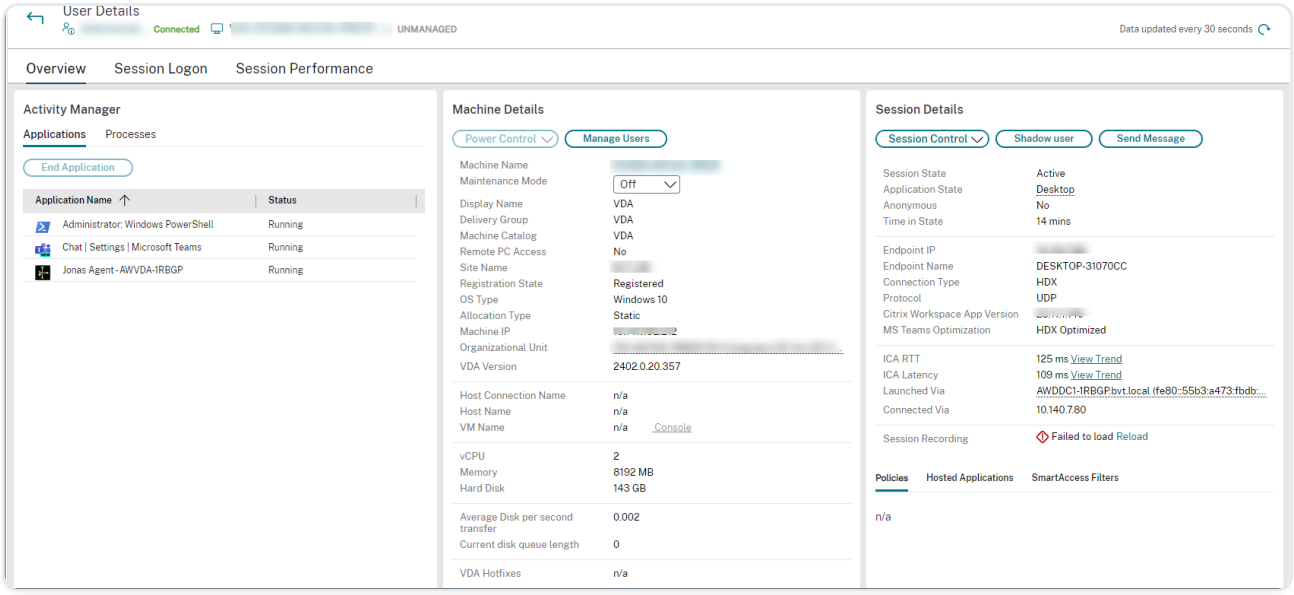
- Verifique os detalhes sobre a sessão, a experiência de logon do usuário, a inicialização da sessão, a conexão e os aplicativos.
- você pode fazer Shadow da máquina do usuário.
- Grave a sessão ICA®.

Status de otimização do Microsoft Teams

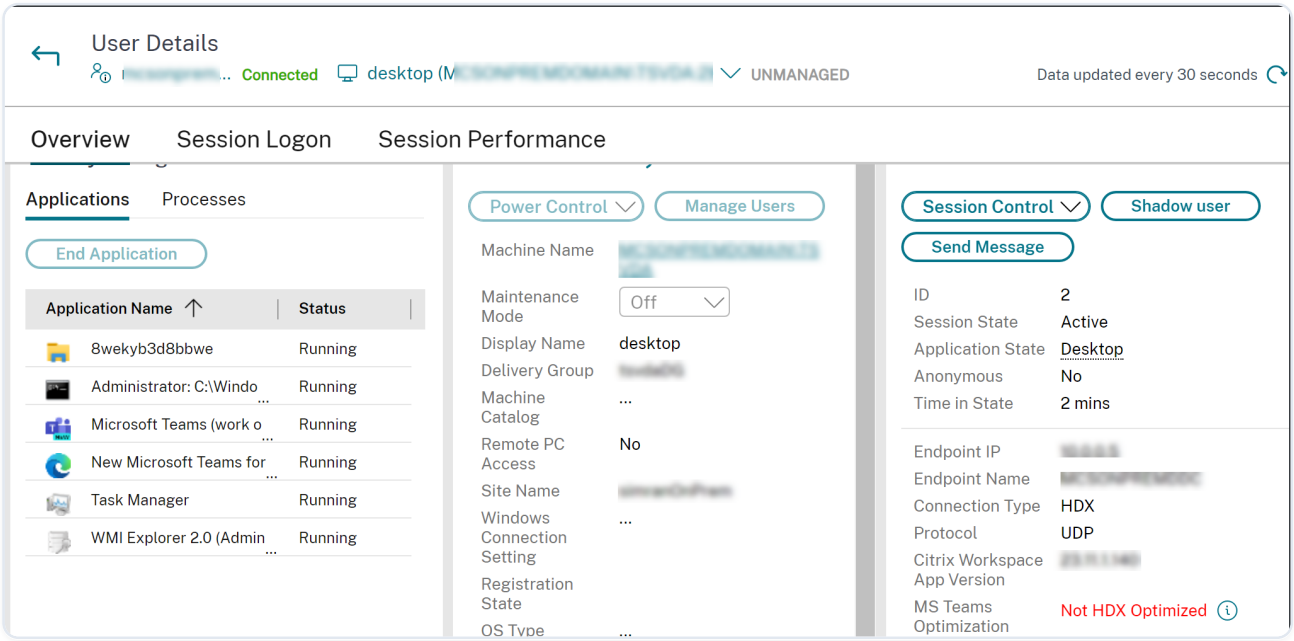
O Director exibe o status de otimização do Microsoft Teams para sessões HDX™ na página **User Details** > painel **Session Details** > campo **MS Teams Optimization**. O Microsoft Teams otimizado é fundamental para uma melhor experiência do usuário, como áudio e vídeo nítidos. A visibilidade do status de otimização do Microsoft Teams é útil para reduzir o tempo necessário para resolver tickets e ajuda os administradores a identificar métricas importantes durante a solução de problemas.

> **Observação:**
>
> O Citrix Director oferece suporte ao Microsoft Teams versão 2.1 ou anterior.
>
> Pré-requisitos:

- Os VDAs estão executando a versão 2311 e posterior.
- As versões compatíveis do aplicativo Citrix Workspace estão listadas em Otimização para Microsoft Teams.
- O Microsoft Teams é executado como um aplicativo publicado ou dentro de uma área de trabalho publicada.
- Serviços cruciais, como o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX, estão em execução.



Se o Microsoft Teams não estiver otimizado, a dica de ferramenta fornece um link para um artigo de solução de problemas externo ao vivo do HDX contendo dicas para otimizar o Microsoft Teams. Solução de problemas de otimização do HDX.



Dicas de solução de problemas

Solucione o problema com as ações recomendadas na tabela a seguir e, se necessário, escale o problema para o administrador apropriado.

PROBLEMA DO USUÁRIO	SUGESTÕES
O logon demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de logon do usuário

PROBLEMA DO USUÁRIO	SUGESTÕES
A inicialização da sessão demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de inicialização da sessão
A resposta da sessão está lenta ou não responde	Diagnosticar problemas de desempenho da sessão
Aplicativo está lento ou não responde	Resolver falhas de aplicativo
Conexão falhou	Restaurar conexões de desktop
Sessão está lenta ou não responde	Restaurar sessões
Gravar sessões	Gravar sessões
Vídeo está lento ou com baixa qualidade	Executar relatórios do sistema de canal HDX

Nota: Para garantir que a máquina não esteja em modo de manutenção, na exibição Detalhes do Usuário, revise o painel Detalhes da Máquina.

Logon da Sessão

A exibição **Detalhes do Usuário** > guia **Logon da Sessão** exibe uma visão abrangente do processo de logon da sessão. A guia contém o gráfico de fases de Duração do Logon com as várias fases de logon plotadas. Use esses dados para solucionar problemas de logon do usuário. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Desempenho da Sessão

A guia **Desempenho da Sessão** possui fluxos de trabalho de solução de problemas aprimorados, começando com a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. O painel **Topologia da Sessão** fornece uma representação visual do caminho em sessão para sessões HDX conectadas. O painel **Métricas de Desempenho** fornece tendências para as métricas de sessão como ICARTT, Latência ICA, Quadros por Segundo, Largura de Banda de Saída Disponível e Largura de Banda de Saída Consumida, ajudando a indicar como essas métricas se comportaram ao longo do tempo. Para obter mais informações, consulte Diagnosticar problemas de desempenho da sessão.

Dicas de pesquisa

Quando você digita o nome do usuário em um campo de Pesquisa, o Director pesquisa usuários no Active Directory em todos os sites configurados para oferecer suporte ao Director.

Quando você digita um nome de máquina multiusuário em um campo de Pesquisa, o Director exibe os Detalhes da Máquina para a máquina especificada.

Quando você digita um nome de endpoint em um campo de Pesquisa, o Director usa as sessões não autenticadas (anônimas) e autenticadas que estão conectadas a um endpoint específico. Essa pesquisa permite solucionar problemas de sessões não autenticadas. Certifique-se de que os nomes de endpoint sejam exclusivos para permitir a solução de problemas de sessões não autenticadas.

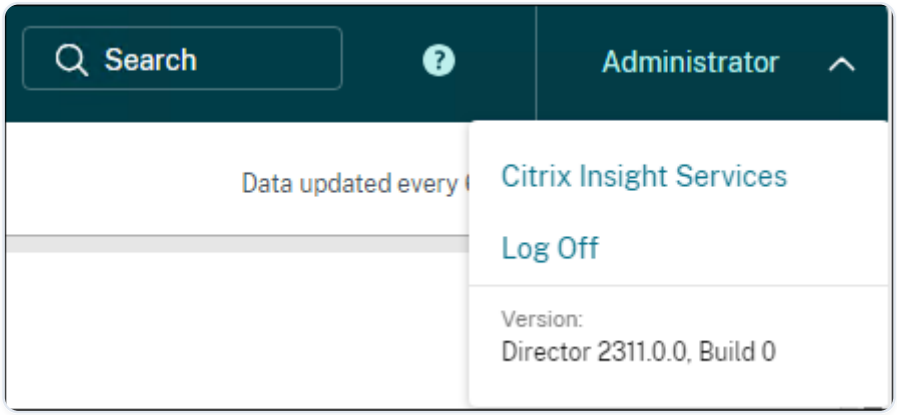
Os resultados da pesquisa também incluem usuários que não estão usando ou atribuídos a uma máquina no momento.

- As pesquisas não diferenciam maiúsculas de minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome composto, separadas por um espaço, os resultados incluem correspondências para ambas as strings. Os exemplos de nomes compostos são nome de usuário, sobrenome e primeiro nome, ou nome de exibição. Por exemplo, se você digitar jo rob, os resultados podem incluir strings como “John Robertson” ou "Robert Jones".

Para retornar à página inicial, clique no **logotipo do Director**.

Acessar o Citrix Insight Services

Você pode acessar Citrix Insight Services (CIS) na lista suspensa **Usuário** no Director para obter insights de diagnóstico adicionais. Os dados disponíveis no CIS vêm de fontes como Call Home e Citrix Scout.



Carregar informações de solução de problemas para o Suporte Técnico da Citrix

Execute o Citrix Scout a partir de um único Delivery Controller™ ou VDA para capturar pontos de dados importantes e rastreamentos do Citrix Diagnostics Facility (CDF) para solucionar problemas em computadores selecionados. O Scout oferece a capacidade de carregar os dados com segurança para a plataforma CIS para auxiliar o Suporte Técnico da Citrix na solução de problemas. O Suporte Técnico da Citrix usa a plataforma CIS para reduzir o tempo de resolução de problemas relatados pelos clientes.

O Scout é instalado com os componentes do Citrix Virtual Apps and Desktops™. Dependendo da versão do Windows, o Scout aparece no menu **Iniciar do Windows** ou na Tela Inicial quando você instala ou atualiza para o Citrix Virtual Apps and Desktops.

Para iniciar o Scout, no menu Iniciar ou na tela Iniciar, selecione **Citrix \> Citrix Scout**.

Para obter informações sobre como usar e configurar o Scout, e para um FAQ, consulte CTX130147.

Diagnosticar problemas de inicialização de sessão

Além das fases do processo de logon mencionadas na seção Diagnosticar problemas de logon do usuário, o Director exibe a duração da inicialização da sessão. Isso é dividido em duração de inicialização da sessão do Workspace App e duração de inicialização da sessão do VDA nas páginas **Detalhes do Usuário** e **Detalhes da Máquina**. Essas duas durações contêm ainda fases individuais cujas durações de inicialização também são exibidas. Esses dados ajudam você a entender e solucionar problemas de alta duração de inicialização da sessão. Além disso, a duração de cada fase envolvida na inicialização da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de Mapeamento de Unidade for alto, você pode verificar se todas as unidades válidas estão mapeadas corretamente no GPO ou script. Este recurso está disponível no Delivery Controller versão 7 1906 e posterior e VDAs 1903 e posterior.

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração de inicialização da sessão sejam exibidos:

- Delivery Controller™ 7 1906 ou posterior.
- VDA 1903 ou posterior.
- O serviço Citrix End User Experience Monitoring (EUEM) deve estar em execução no VDA.

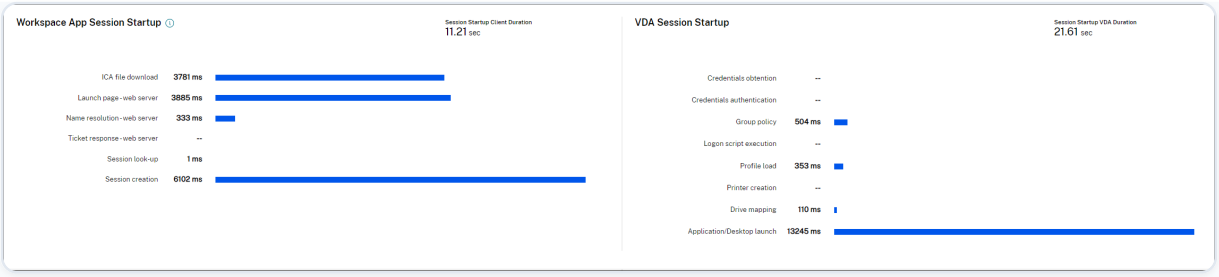
Limitações

As seguintes limitações se aplicam quando o Director exibe os dados de duração de inicialização da sessão.

- A duração da inicialização da sessão está disponível apenas para sessões HDX™.
- Para inicializações de sessão de iOS e Android OS, apenas a Duração de Inicialização do VDA está disponível.
- A Duração de Download de Arquivo ICA® (IFDCD) está disponível apenas quando o Workspace App é detectado ao iniciar a partir de um navegador.
- Para inicializações de sessão de Mac OS, o IFDCD está disponível apenas para o Workspace App 1902 ou posterior.
- Para inicializações de sessão de Windows OS, o IFDCD está disponível para o Workspace app 1902 e posterior. Para versões anteriores, o IFDCD é exibido apenas para inicializações de aplicativos a partir do navegador com o Workspace app detectado.

Notas:

- Se você enfrentar problemas na exibição da duração da inicialização das sessões após o cumprimento dos pré-requisitos, visualize os logs do servidor Director e do VDA conforme descrito em CTX130320. Para sessões compartilhadas (vários aplicativos iniciados na mesma sessão), as métricas de inicialização do Workspace App são exibidas para a conexão mais recente ou o lançamento de aplicativo mais recente.
- Algumas métricas na Inicialização da Sessão VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.



Fases de inicialização da sessão do Workspace App

DURAÇÃO DE INICIALIZAÇÃO DO CLIENTE DA SESSÃO (SSCD)

Quando essa métrica é alta, indica um problema do lado do cliente que está causando longos tempos de inicialização. Revise as métricas subsequentes para determinar a provável causa raiz do problema. O SSCD começa o mais próximo possível do momento da solicitação (clique do mouse). Ele termina quando a conexão ICA entre o dispositivo cliente e o VDA é estabelecida. No caso de uma sessão compartilhada, essa duração é muito menor, pois grande parte dos custos de configuração associados à criação de uma nova conexão com o servidor não são incorridos. No nível seguinte, há várias métricas detalhadas disponíveis.

DURAÇÃO DO DOWNLOAD DO ARQUIVO ICA

Este é o tempo que o cliente leva para baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou desktop) no aplicativo Workspace.
2. Uma solicitação do usuário é enviada ao StoreFront™ através do Citrix Gateway (se configurado), que envia a solicitação ao Delivery Controller.
3. O Delivery Controller encontra uma máquina disponível para a solicitação e envia as informações da máquina e outros detalhes para o StoreFront. Além disso, o StoreFront solicita e recebe um tíquete único da Secure Ticket Authority.
4. O StoreFront gera um arquivo ICA e o envia ao usuário via Citrix Gateway (se configurado).

O IFDCD representa o tempo que leva para o processo completo (etapas 1 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 for normal), o processamento do lançamento no lado do servidor foi bem-sucedido, mas houve problemas de comunicação entre o dispositivo cliente e o StoreFront. Isso resulta de problemas de rede entre as duas máquinas. Portanto, você pode solucionar possíveis problemas de rede primeiro.

DURAÇÃO DO SERVIDOR WEB DA PÁGINA DE LANÇAMENTO (LPWD)

Este é o tempo que leva para processar a página de lançamento (launch.aspx) no StoreFront. Se o LPWD for alto, pode haver um gargalo no StoreFront.

As possíveis causas incluem:

- Carga alta no StoreFront. Tente identificar a causa da lentidão verificando os logs do Internet Information Services (IIS) e ferramentas de monitoramento, Gerenciador de Tarefas, Monitor de Desempenho e assim por diante.
- O StoreFront está com problemas para se comunicar com outros componentes, como o Delivery Controller. Verifique se a conexão de rede entre o StoreFront e o Delivery Controller está lenta ou se alguns Delivery Controllers estão inativos ou sobrecarregados.

DURAÇÃO DO SERVIDOR WEB DE RESOLUÇÃO DE NOMES (NRWD)

Este é o tempo que o Delivery Controller leva para resolver o nome de um aplicativo/desktop publicado para um endereço IP de Máquina VDA.

Quando essa métrica é alta, indica que o Delivery Controller está demorando muito para resolver o nome de um aplicativo publicado para um endereço IP.

As possíveis causas incluem um problema no cliente, problemas com o Delivery Controller, como o Delivery Controller estar sobrecarregado, ou um problema com o link de rede entre eles.

DURAÇÃO DO SERVIDOR WEB DE RESPOSTA DE TICKET (TRWD)

Esta duração indica o tempo que leva para obter um ticket (se necessário) do Servidor Secure Ticket Authority (STA) ou do Delivery Controller. Quando esta duração é alta, indica que o servidor STA ou o Delivery Controller estão sobrecarregados.

DURAÇÃO DA PESQUISA DE SESSÃO DO CLIENTE (SLCD)

Esta duração representa o tempo levado para consultar cada sessão para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode manipular a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

DURAÇÃO DA CRIAÇÃO DE SESSÃO DO CLIENTE (SCCD)

Esta duração representa o tempo levado para criar uma sessão, desde o momento em que wfica32.exe (ou um arquivo equivalente similar) é iniciado até o momento em que a conexão é estabelecida.

Fases de inicialização da sessão VDA

DURAÇÃO DA INICIALIZAÇÃO DA SESSÃO VDA (SSVD)

Esta duração é a métrica de alto nível de inicialização de conexão do lado do servidor que engloba o tempo que o VDA leva para realizar toda a operação de inicialização. Quando esta métrica é alta, indica que há um problema no VDA que aumenta os tempos de inicialização da sessão. Isso inclui o tempo gasto no VDA realizando toda a operação de inicialização.

DURAÇÃO DA OBTENÇÃO DE CREDENCIAIS DO VDA (COVD)

O tempo que o VDA leva para obter as credenciais do usuário.

Esta duração pode aumentar artificialmente se um usuário não fornecer as credenciais em tempo hábil. Portanto, não está incluída na Duração de Inicialização do VDA. Este tempo provavelmente será significativo apenas se o login manual estiver sendo usado e a caixa de diálogo de credenciais do lado do servidor for exibida (ou se um aviso legal for exibido antes do início do login).

DURAÇÃO DA AUTENTICAÇÃO DE CREDENCIAIS DO VDA (CAVD)

Este é o tempo que o VDA leva para autenticar as credenciais do usuário contra o provedor de autenticação. Eles podem ser Kerberos, Active Directory ou uma Interface de Provedor de Suporte de Segurança (SSPI).

DURAÇÃO DA POLÍTICA DE GRUPO DO VDA (GPVD)

Esta duração é o tempo necessário para aplicar objetos de política de grupo durante o logon.

DURAÇÃO DA EXECUÇÃO DE SCRIPT DE LOGIN DO VDA (LSVD)

Este é o tempo que o VDA leva para executar os scripts de login do usuário.

Considere tornar assíncronos os scripts de login do usuário ou do grupo. Considere otimizar quaisquer scripts de compatibilidade de aplicativos ou usar variáveis de ambiente em vez disso.

DURAÇÃO DO CARREGAMENTO DE PERFIL DO VDA (PLVD)

Este é o tempo que o VDA leva para carregar o perfil do usuário.

Se esta duração for alta, considere sua configuração de Perfil de Usuário. O tamanho e a localização do perfil móvel contribuem para inícios de sessão lentos. Quando um usuário faz logon em uma sessão onde perfis móveis do Terminal Services e pastas pessoais estão habilitados, o conteúdo do perfil móvel e o acesso a essa pasta são mapeados durante o logon. Isso consome recursos extras. Às vezes, isso pode consumir uma quantidade significativa do uso da CPU. Considere usar as pastas **Terminal Services home** com pastas pessoais redirecionadas para mitigar este problema. Em geral, considere usar o Citrix Profile Management para gerenciar perfis de usuário em ambientes Citrix. Se você estiver usando o Citrix Profile Management e tiver tempos de logon lentos, verifique se o seu software antivírus está bloqueando a ferramenta Citrix Profile Management.

DURAÇÃO DA CRIAÇÃO DE IMPRESSORA DO VDA (PCVD)

Este é o tempo que o VDA leva para mapear as impressoras cliente do usuário de forma síncrona. Se a configuração for definida para que a criação da impressora seja realizada de forma

assíncrona, o valor não é registrado para PCVD, pois não afeta a conclusão da inicialização da sessão.

O tempo excessivo gasto no mapeamento de impressoras é frequentemente o resultado das configurações da política de criação automática de impressoras. O número de impressoras adicionadas localmente nos dispositivos cliente dos usuários e sua configuração de impressão podem afetar diretamente os tempos de início da sua sessão. Quando uma sessão é iniciada, o Citrix Virtual Apps and Desktops™ precisa criar cada impressora mapeada localmente no dispositivo cliente. Considere reconfigurar suas políticas de impressão para reduzir o número de impressoras que são criadas, especificamente quando os usuários têm muitas impressoras locais. Para fazer isso, edite a política de criação automática de impressoras no Delivery Controller e no Citrix Virtual Apps and Desktops.

DURAÇÃO DO MAPEAMENTO DE UNIDADE VDA (DMVD)

Este é o tempo levado pelo VDA para mapear as unidades cliente, dispositivos e portas do usuário.

Certifique-se de que suas políticas base incluam configurações para desabilitar canais virtuais não utilizados. Por exemplo, mapeamento de áudio ou porta COM, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

DURAÇÃO DO LANÇAMENTO DE APLICATIVO/DESKTOP VDA (ALVD/DLVD)

Esta fase é uma combinação da duração do Userinit e do Shell. Quando um usuário faz logon em uma máquina Windows, o winlogon executa userinit.exe. Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia Explorer.exe. Userinit representa a duração entre o início de userinit.exe e o início da interface do usuário para o desktop virtual ou aplicativo. 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.

DURAÇÃO DA CRIAÇÃO DE SESSÃO VDA (SCVD)

Este tempo inclui qualquer atraso diverso no tempo de criação da sessão no VDA.

Diagnosticar problemas de logon do usuário

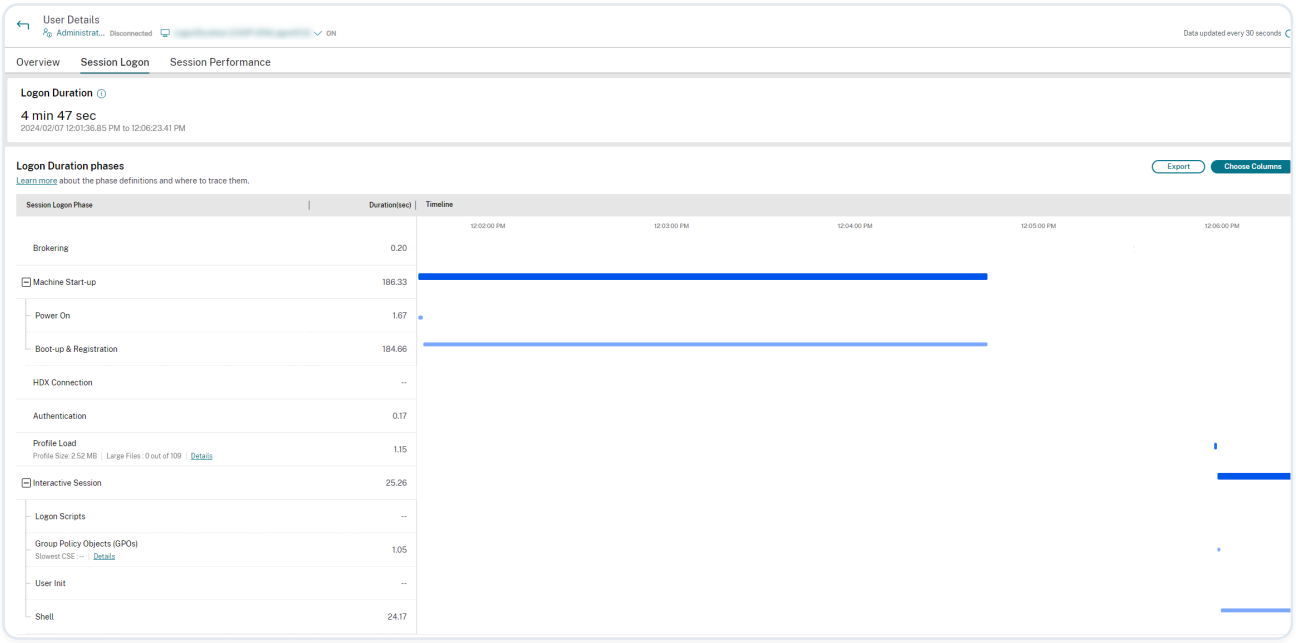
A visualização **Detalhes do Usuário** > guia **Logon da Sessão** exibe uma visão abrangente do processo de logon da sessão. Use esses dados para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a um desktop ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o Protocolo de Área de Trabalho Remota ou reconectar-se de sessões desconectadas. Especificamente, a duração do

logon não é medida quando um usuário se conecta inicialmente usando um protocolo não-HDX e se reconecta usando HDX.

À medida que os usuários fazem logon no Citrix Virtual Apps and Desktops™, o Serviço de Monitoramento rastreia as fases do processo de logon. As fases começam desde o momento em que o usuário se conecta do aplicativo Citrix Workspace™ até o momento em que o aplicativo ou desktop está pronto para uso.

A guia **Logon da Sessão** contém o gráfico de fases de Duração do Logon com as várias fases de logon plotadas. A Duração do Logon representa o tempo gasto para estabelecer a conexão e obter um aplicativo ou desktop do Delivery Controller™ e o tempo gasto para autenticar e fazer logon em um aplicativo ou desktop virtual. As informações de duração são apresentadas em segundos (ou frações de segundos).



O gráfico de fases de Duração do Logon fornece uma visão clara das diferentes fases de logon e seus tempos de início e término. O gráfico mostra a sobreposição das fases de logon individuais. O tempo total de logon pode não ser a soma das durações das fases de logon individuais. Isso ocorre porque as fases individuais podem se sobrepor e nem todas as fases de logon fazem parte desta representação. Além disso, certas fases podem se estender mesmo depois que o usuário começa a interagir com o aplicativo ou desktop virtual, e essa duração não é medida como parte da duração geral do logon.

Use esta visualização para identificar fases de logon específicas que causam um atraso no lançamento da sessão. A definição para cada fase de logon e a fonte do evento de onde você pode rastrear informações ajudam na solução de problemas. Passar o mouse sobre o gráfico exibe uma dica de ferramenta contendo a duração da fase para a sessão atual, bem como a média de 7 dias do usuário e a média de 7 dias do grupo de entrega. Essas informações ajudam a

comparar a duração do logon da sessão atual com os valores médios de 7 dias. Você pode aprofundar-se nas medições de subfases no caso de GPO e Detalhes do Perfil. Esta visualização ajuda a entender e solucionar facilmente problemas relacionados à duração do logon.

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração do logon e os detalhamentos apareçam:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Serviço de Gerenciamento de Perfil do Citrix esteja em execução.
3. Para sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Não processar a lista de execução herdada**.
4. O rastreamento de processo de auditoria deve ser habilitado para o detalhamento da Sessão Interativa.
5. Para o detalhamento de GPO, aumente o tamanho dos logs operacionais da Política de Grupo.

> **Notas:**
>
> - A duração do logon é suportada apenas no shell padrão do Windows (explorer.exe) e não em shells personalizados.
> - A duração do logon para Acesso Remoto a PC está disponível apenas quando o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** são instalados como componentes extras durante a instalação do Acesso Remoto a PC. Para obter mais informações, consulte a Etapa 4 em Considerações sobre configuração e sequência do Acesso Remoto a PC.

Etapas para solucionar problemas de logon do usuário

1. Na visualização **Detalhes do Usuário** > guia **Logon da Sessão**, solucione o estado do logon usando o gráfico de Duração do Logon.
   - Se o usuário estiver fazendo logon, a exibição reflete o processo de logon.
   - Se o usuário estiver logado, o painel Duração do Logon exibe o tempo que o usuário levou para fazer logon na sessão atual.
2. Examine as fases do processo de logon.

Fases do processo de logon

INTERMEDIAÇÃO

Tempo levado para decidir qual desktop atribuir ao usuário.

INICIALIZAÇÃO DA MÁQUINA

Se a sessão exigiu o início de uma máquina, este é o tempo levado para iniciar a máquina virtual. A subseção a seguir fornece um detalhamento do tempo levado para iniciar uma máquina virtual durante diferentes fases:

- **Ligar** - Exibe o tempo necessário para ligar uma máquina virtual
- **Inicialização e registro** - Exibe o tempo necessário para inicializar e registrar uma máquina virtual

Você pode usar o botão recolhível para recolher ou expandir as opções em **Inicialização da Máquina**.

CONEXÃO HDX

Tempo necessário para concluir as etapas exigidas na configuração da conexão HDX do cliente para a máquina virtual.

AUTENTICAÇÃO

Tempo necessário para concluir a autenticação na sessão remota.

GPOS

Se as configurações de Política de Grupo estiverem habilitadas nas máquinas virtuais, este é o tempo necessário para aplicar os objetos de política de grupo durante o logon. O detalhamento do tempo necessário para aplicar cada política de acordo com as CSEs (Extensão do Lado do Cliente) está disponível como uma dica de ferramenta ao passar o mouse sobre a barra GPO.



Clique em **Detalhes** para ver uma tabela com o status da política e o nome GPO correspondente. As durações de tempo no detalhamento representam apenas o tempo de processamento do CSE e não somam o tempo total do GPO. Você pode copiar a tabela de detalhamento para solução de problemas adicionais ou uso em relatórios. O tempo GPO para as políticas é recuperado dos logs do Visualizador de Eventos. Os logs podem ser sobrescritos dependendo da memória alocada para os logs operacionais (o tamanho padrão é 4 MB). Para obter mais informações sobre como aumentar o tamanho do log para os logs operacionais, consulte o artigo do Microsoft TechNet Configuring the Event Logs.

SCRIPTS DE LOGON

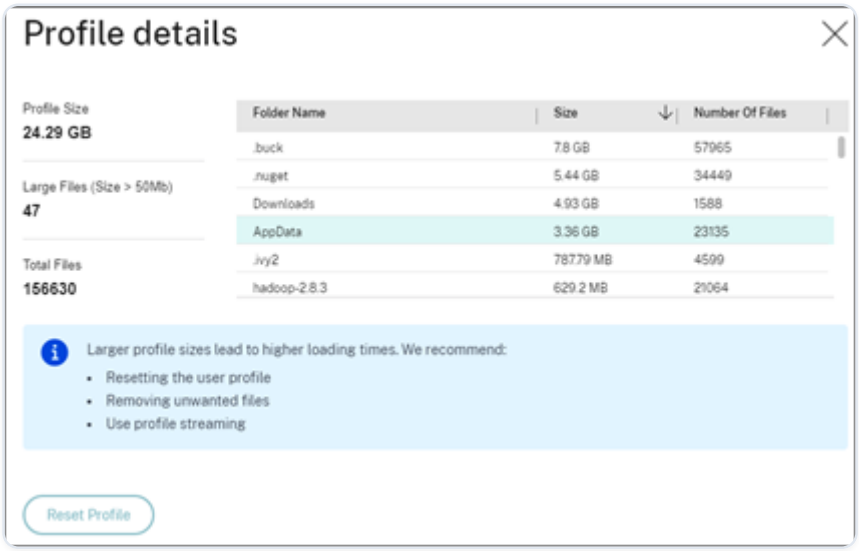
Se os scripts de logon estiverem configurados para a sessão, este é o tempo necessário para que os scripts de logon sejam executados.

CARREGAMENTO DE PERFIL

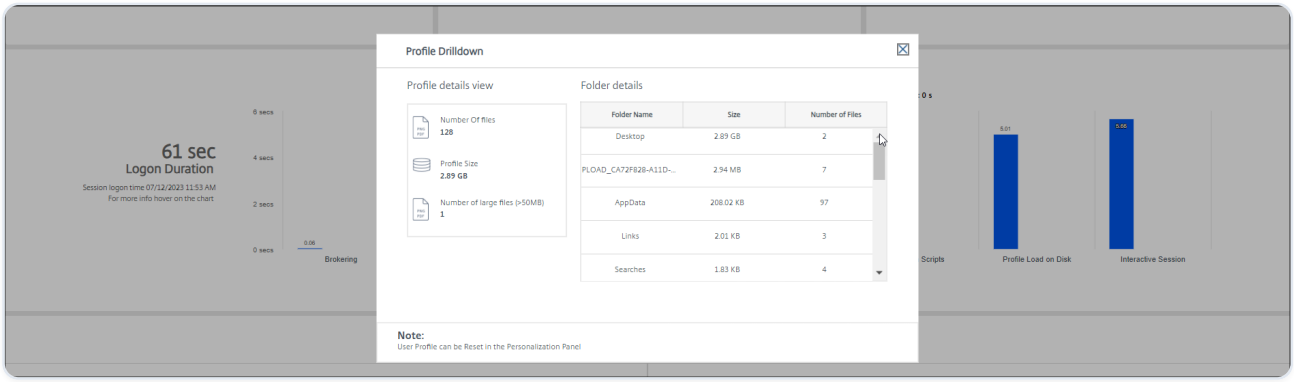
Se as configurações de perfil estiverem configuradas para o usuário ou a máquina virtual, este é o tempo necessário para o perfil carregar.

Se o Citrix Profile Management e o FSLogix estiverem configurados, a barra de Carga de Perfil inclui o tempo gasto pelo Citrix Profile Management e pelo FSLogix para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management e o FSLogix estão configurados, a barra de Carga de Perfil exibe uma duração aumentada. Esse aumento é causado por essa melhoria e não reflete uma degradação de desempenho. Essa melhoria está disponível nas versões VDA 2407 ou posteriores.

Passar o mouse sobre a barra de Carga de Perfil exibe uma dica de ferramenta mostrando os detalhes do perfil do usuário para a sessão atual.



Clique em **Detalhes** para aprofundar ainda mais em cada pasta individual na pasta raiz do perfil (por exemplo, C:/Users/username), seu tamanho e o número de arquivos (incluindo arquivos dentro de pastas aninhadas).



O detalhamento do perfil está disponível no Delivery Controller versão 7 1811 ou posterior e em VDAs 1811 ou posterior. Usando as informações de detalhamento do perfil, você pode resolver problemas que envolvem um tempo de carregamento de perfil alto. Você pode:

- Redefinir o perfil do usuário
- Otimizar o perfil removendo arquivos grandes indesejados
- Reduzir o número de arquivos para diminuir a carga da rede
- Usar streaming de perfil

Por padrão, todas as pastas na raiz do perfil são exibidas no detalhamento. Para ocultar a visibilidade da pasta, edite o seguinte valor de registro na máquina VDA:

> **Aviso:**
>
> Adicionar e editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não garante que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

1. No VDA, adicione um novo valor de registro **ProfileFoldersNameHidden** em HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Defina o valor como 1. Este valor deve ser um valor DWORD (32 bits). A visibilidade dos nomes das pastas agora está desativada.
3. Para tornar os nomes das pastas visíveis novamente, defina o valor como 0.

> **Nota:**
>
> Você pode usar comandos GPO ou PowerShell para aplicar a alteração do valor do registro em várias máquinas. Para obter mais informações sobre como usar GPO para implantar alterações de registro, consulte o blog.

Informações adicionais

- A análise detalhada do perfil não considera pastas redirecionadas.
- Os arquivos NTUser.dat na pasta raiz podem não estar visíveis para os usuários finais. No entanto, eles são incluídos no detalhamento do perfil e exibidos na lista de arquivos em **Pasta Raiz**.
- Certos arquivos ocultos na pasta AppData não estão incluídos no detalhamento do Perfil.
- O número de arquivos e os dados de tamanho do perfil podem não corresponder aos dados no painel de Personalização devido a certas limitações do Windows.

SESSÃO INTERATIVA

Sessão Interativa é o tempo necessário para "entregar" o controle do teclado e do mouse ao usuário após o carregamento do perfil do usuário. Normalmente, é a duração mais longa de todas as fases do processo de logon e é calculada como **duração da Sessão Interativa = Carimbo de Data/Hora do Evento Desktop Ready (EventId 1000 no VDA) - Carimbo de Data/Hora do Evento User Profile Loaded (EventId 2 no VDA)**. A Sessão Interativa tem três subfases: Pre-userinit, Userinit e Shell. Passe o mouse sobre Sessão Interativa para ver uma dica de ferramenta mostrando o seguinte:

- subfases
- tempo gasto para cada subfase
- atraso total cumulativo entre essas subfases

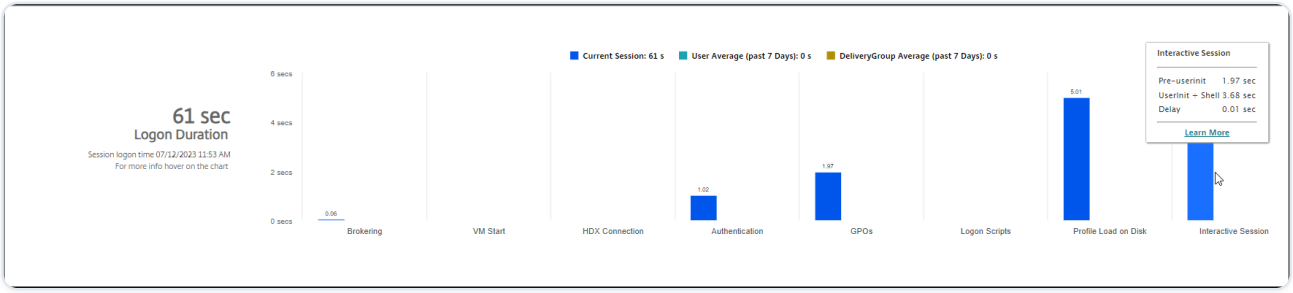
Você pode usar o botão recolhível para recolher ou expandir as opções em **Sessão Interativa**.

> **Nota:**
>
> Este recurso está disponível em VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores à versão 7.18 e depois atualizou para a versão 7.18 ou posterior, uma mensagem 'Detalhes indisponíveis devido a erro do servidor' é exibida. No entanto, se você iniciou sessões após a atualização, nenhuma mensagem de erro é exibida.

> Para visualizar a duração de cada subfase, habilite o rastreamento de processo de auditoria (Audit process tracking) na VM (VDA). Quando o rastreamento de processo de auditoria está desabilitado (padrão), a duração de Pre-userinit e a duração combinada de Userinit e Shell são exibidas. Você pode habilitar o rastreamento de processo de auditoria por meio de um Objeto de Política de Grupo (GPO) da seguinte forma:

1. Crie um GPO e edite-o usando o editor de GPO.
2. Vá para **Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Política de Auditoria**.
3. No painel direito, clique duas vezes em **Rastreamento de processo de auditoria**.
4. Selecione **Êxito** e clique em OK.
5. Aplique este GPO aos VDAs ou Grupo necessários.

Para obter mais informações sobre o rastreamento de processos de auditoria e como habilitá-lo ou desabilitá-lo, consulte Rastreamento de processos de auditoria na documentação da Microsoft.



Painel Duração do Logon na visualização Detalhes do Usuário.

- **Sessão Interativa – Pre-userinit:** O segmento da Sessão Interativa que se sobrepõe a Objetos de Política de Grupo e scripts. Esta subfase pode ser reduzida otimizando os GPOs e scripts.
- **Sessão Interativa – Userinit:** Quando um usuário faz logon em uma máquina Windows, o Winlogon executa userinit.exe. O Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface do usuário do Windows. Esta subfase da Sessão Interativa representa a duração entre o início do Userinit.exe e o início da interface do usuário para o desktop virtual ou aplicativo.
- **Sessão Interativa – Shell:** Na fase anterior, o Userinit inicia a inicialização da interface de usuário do Windows. A subfase Shell captura a duração entre a inicialização da interface de usuário e o momento em que o usuário recebe o controle do teclado e do mouse.
- **Atraso:** Este é o atraso de tempo cumulativo entre as subfases **Pré-userinit e Userinit** e as subfases **Userinit e Shell**.

O tempo total de logon não é a soma exata dessas fases. Por exemplo, algumas fases ocorrem em paralelo, e em algumas fases, mais processamento ocorre, o que pode resultar em uma duração de logon mais longa do que a soma. O tempo total de logon não inclui o tempo ocioso do ICA®, que é o tempo entre o download do arquivo ICA e o lançamento do arquivo ICA para um aplicativo. Para habilitar a abertura automática do arquivo ICA no lançamento do aplicativo, configure seu navegador para o lançamento automático do arquivo ICA após o download de um arquivo ICA. Para obter mais informações, consulte CTX804493.

Nota:

O gráfico Duração de Logon mostra as fases de logon em segundos. Quaisquer valores de duração abaixo de um segundo são exibidos como valores de subsegundo. Os valores acima de um segundo são arredondados para o 0,5 segundo mais próximo. O gráfico foi projetado para mostrar o valor mais alto do eixo y como 200 segundos. Qualquer valor maior que 200 segundos é mostrado com o valor real exibido acima da barra.

EXPORTAR DADOS

Juntamente com as opções padrão da tabela Fases de Duração de Logon, que são Fase de Logon da Sessão e Duração, você também pode escolher as seguintes colunas na página Logon da Sessão:

- Hora de início
- Hora de término
- Grupo de Entrega - Média de 7d (seg)
- Usuário - Média de 7d (seg)

Você também pode exportar os dados precedentes para um arquivo .CSV.

Dicas de solução de problemas

Para identificar valores incomuns ou inesperados no gráfico, compare a quantidade de tempo gasto em cada fase da sessão atual com a duração média para este usuário nos últimos sete dias e a duração média para todos os usuários neste grupo de entrega nos últimos sete dias.

Escalone conforme necessário. Por exemplo, se a **Inicialização da Máquina** estiver lenta, o problema pode estar no hypervisor, então você pode escalá-lo para o administrador do hypervisor.

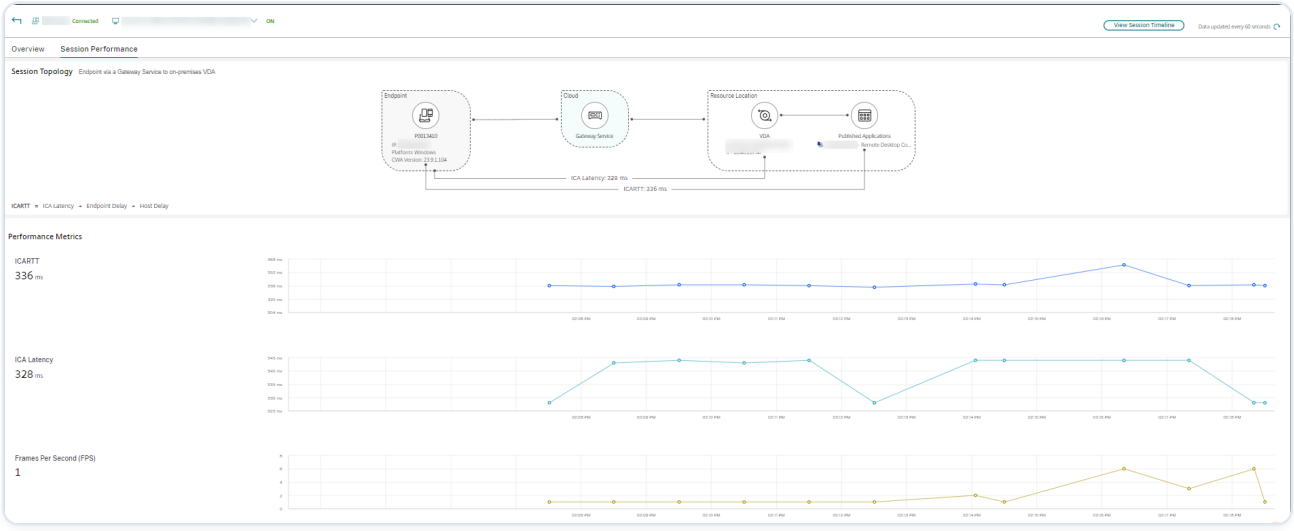
Examine as diferenças incomuns, incluindo:

- Barras de logon (atuais) ausentes
- Grande discrepância entre a duração atual e a duração média deste usuário. As causas incluem:
  - Uma nova aplicação foi instalada.
  - Uma atualização do sistema operacional ocorreu.
  - Alterações de configuração foram feitas.
  - O tamanho do perfil do usuário é alto. Neste caso, a Carga do Perfil é alta.
- Grande discrepância entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

Se necessário, clique em **Reiniciar** para observar o processo de logon do usuário e solucionar problemas, como **Inicialização da Máquina** ou **Brokering**.

Diagnosticar problemas de desempenho da sessão

A guia **Desempenho da Sessão** na Página de Detalhes do Usuário possui fluxos de trabalho de solução de problemas aprimorados para ajudar a identificar problemas em sessões de usuário HDX™. Os painéis **Topologia da Sessão e Métricas de Desempenho** ajudam a correlacionar a visualização de componentes e múltiplas métricas de desempenho de uma sessão em uma única visualização e reduzem o tempo médio para a resolução de problemas de experiência da sessão.



Visualização de Salto de Rede de Ponta a Ponta

A visualização de salto de rede de ponta a ponta melhora a solução de problemas, fornecendo uma representação visual de todo o caminho da sessão. Clique em **Detalhes do Usuário** > **Desempenho da Sessão** > **Topologia da Sessão** para encontrar a visualização de salto de rede

de ponta a ponta. Esta visualização exibe componentes, metadados, links e aplicativos publicados para sessões HDX conectadas.

Esta visualização ajuda os administradores a:

- Compreender o fluxo de dados da sessão.
- Identificar gargalos de desempenho em saltos específicos.

> **Observação:**
>
> As métricas de desempenho estão disponíveis apenas para sessões HDX conectadas.

MÉTRICAS DE DESEMPENHO DA SESSÃO

As seguintes métricas estão disponíveis contextualmente para ajudar os administradores a entender o desempenho da sessão em questão. Os dados disponíveis na visualização de salto são atualizados periodicamente com intervalos indicados na interface do usuário.

Métricas de endpoint:

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO APLICATIVO CITRIX WORKSPACE™ PARA WINDOWS	VERSÃO DO VIRTUAL DELIVERY AGENT
Detalhes da rede do endpoint	Tipo de interface de rede	Versão 2405.10 ou posterior do aplicativo Citrix Workspace para Windows	Citrix Virtual Apps and Desktops 2407 ou posterior
	Força do sinal Wi-Fi		
	Taxa de transferência de entrada ou saída		
	Velocidade do link		

Métricas HDX:

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO CITRIX WORKSPACE APP PARA WINDOWS	VERSÃO DO VIRTUAL DELIVERY AGENT
Métricas ICA	ICA RTT	Versão 2405.10 ou posterior do aplicativo Citrix Workspace para Windows	Citrix Virtual Apps and Desktops 2407 ou posterior
	Latência ICA®		

Definições de dados:

PARÂMETRO DA IU	DESCRIÇÃO
ICA RTT	Mede o tempo entre a ação do usuário e a resposta da tela, incluindo latência ICA, atraso do endpoint e atraso do host.
Latência ICA	Indica latência de rede e possível lentidão.
Força do sinal Wi-Fi	Exibe a qualidade e a força do sinal sem fio.
Taxa de transferência de entrada e saída	Indica a taxa de transferência de dados para dentro e para fora da interface de rede.
Tipo de interface de rede	Especifica o tipo de conexão de rede, como Ethernet, Wi-Fi ou celular.
Velocidade do link	Representa a taxa máxima de transferência de dados da conexão de rede.

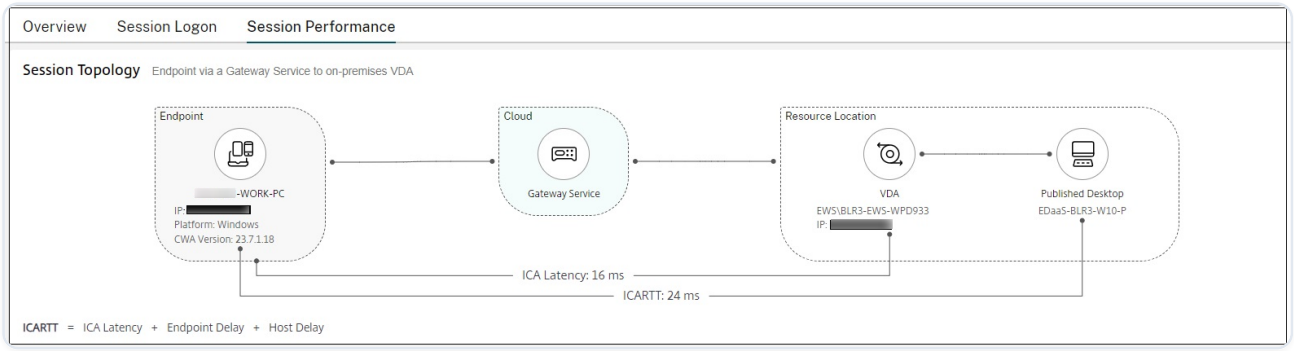
CENÁRIOS DE TOPOLOGIA DE SESSÃO

Dependendo do cenário de implantação do site, os componentes envolvidos em uma sessão são todos ou qualquer um dos seguintes:

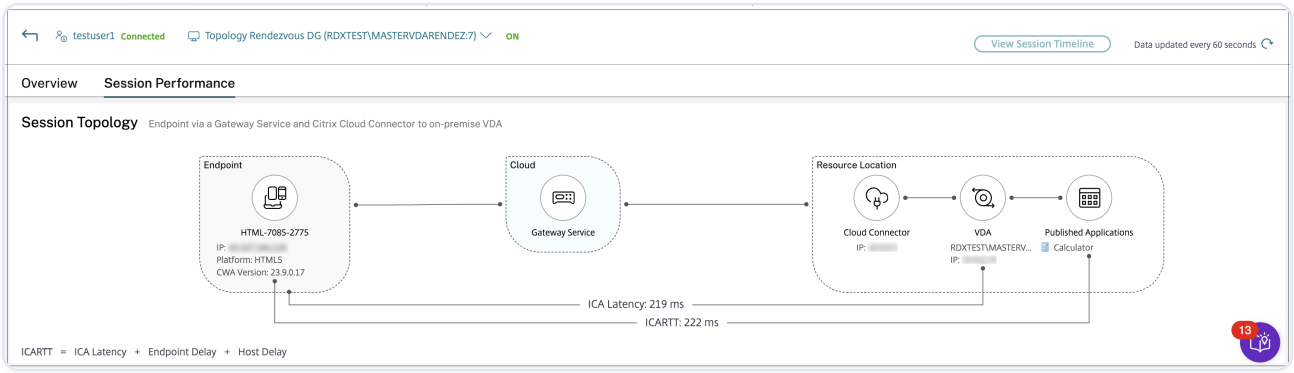
- Aplicativo Citrix Workspace no Endpoint
- Serviço Gateway/Gateway local
- Cloud Connector – O Gateway está conectado ao DaaS por meio de um Cloud Connector no caso de conexões híbridas.
- VDAs

Consequentemente, as possíveis topologias de rede são as seguintes:

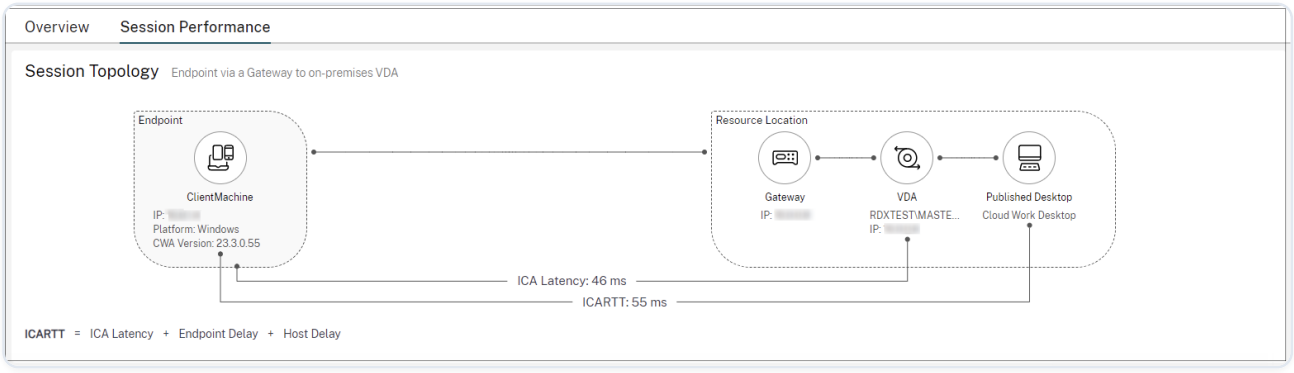
- O aplicativo Citrix Workspace no endpoint se conecta via Citrix Workspace e Gateway Service a um VDA local. Nenhum Cloud Connector é usado para se conectar ao VDA.



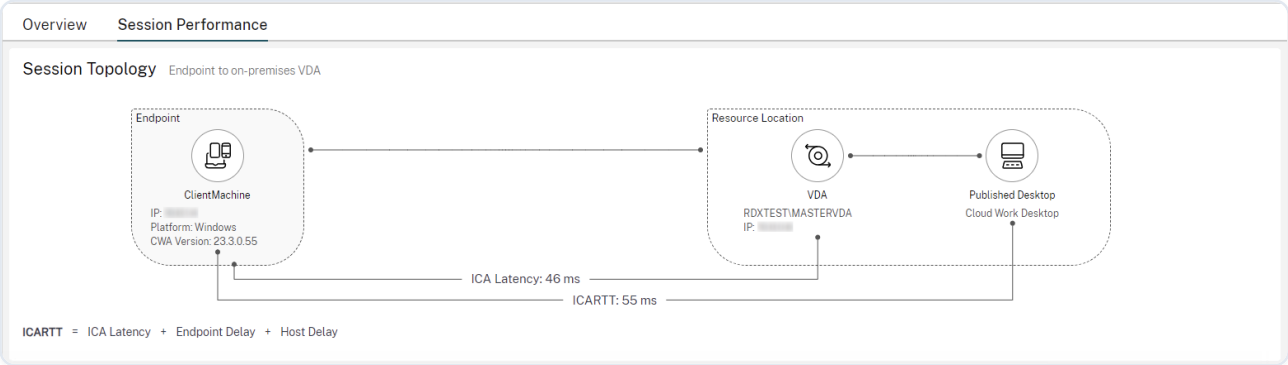
- O aplicativo Citrix Workspace no endpoint se conecta via Citrix Workspace e Gateway Service a um VDA local via Cloud Connector.



- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront™ e Gateway local a um VDA local.



- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront a um VDA local.



Métricas de Desempenho

O painel **Métricas de Desempenho** oferece a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. As tendências para as métricas de sessão ajudam a indicar como essas métricas se comportaram ao longo do tempo. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados em tempo real, você pode visualizar os dados dos últimos 15 minutos e 24 horas. Os gráficos ajudam a correlacionar várias métricas de desempenho de componentes em uma única visualização.



Observação:

- Com o suporte a métricas dos últimos 15 minutos, o gráfico é plotado para a duração em que a sessão está conectada e desconectada. A métrica da sessão desconectada é exibida com o valor zero.
- Com o suporte a métricas das últimas 24 horas, os gráficos de ICARTT e Latência ICA são atualizados com as métricas de dados históricos.

> Além de ICARTT e Latência ICA, as seguintes métricas estão disponíveis para métricas em tempo real e dos últimos 15 minutos:

- Quadros por Segundo - Quadros por Segundo é uma métrica importante que indica a capacidade de resposta da sessão. Largura de Banda de Saída Disponível - Largura de Banda de Saída Disponível é uma medida da largura de banda total disponível para transmitir dados do VDA para o endpoint.
- Largura de Banda de Saída Consumida - Largura de Banda de Saída Consumida indica a quantidade real de dados transmitidos do VDA para o endpoint para exibir sessões aos usuários.

Analisar a Largura de Banda de Saída Disponível e a Largura de Banda de Saída Consumida ajuda a verificar se há largura de banda suficiente para atender às sessões e a detectar se uma sessão é afetada por largura de banda insuficiente.

Solucionar problemas quando os dados de ICA RTT ou Duração de Logon da Sessão não são preenchidos

Anteriormente, quando o serviço EUEM ou o serviço Profile Management falhava ao ser executado, o motivo da falha na obtenção dos dados relacionados ao ICA RTT ou Duração de Logon da Sessão não era exibido. Com este novo recurso, você pode obter o motivo da falha e a solução correspondente para essa falha. Os links **Saiba mais** fornecem os erros de ICA RTT e Duração de Logon da Sessão, o motivo da falha e a solução, conforme mencionado na tabela a seguir:

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**O Citrix End User Experience Monitoring não está em execução.**	`1.` Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite **Serviços**. `2.` Certifique-se de que o Serviço de Monitoramento da Experiência do Usuário Final do Citrix esteja em execução.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			3. Reabra a sessão da área de trabalho e tente novamente. O valor de ICA RTT deve ser exibido.
			4. Se o problema persistir, entre em contato com o administrador Citrix.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**O Monitoramento da Experiência do Usuário Final do Citrix não está instalado.**	1. Reinstale o VDA.
			2. Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços
			3. Certifique-se de que o Serviço de Monitoramento da Experiência do Usuário Final do Citrix esteja em execução.
			4. Reabra a sessão da área de trabalho e tente novamente. O valor de ICA RTT deve ser exibido agora.
			5. Se o problema persistir, entre em contato com o administrador Citrix.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**Erro ao buscar dados.**	`1.` Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços. `2.` Certifique-se de que o **Serviço de Instrumentação de Gerenciamento do Windows** esteja em execução. `3.` Além disso, certifique-se de que o processo WfShell.exe/ PicaShell.exe esteja em execução em **Gerenciador de Atividades** > guia **Processo**. Se não estiver em execução, reabra a sessão da área de trabalho. `4.` Se as etapas anteriores não estiverem funcionando, execute o seguinte comando para garantir que a instância Citrix_Euem_Round Trip esteja presente: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select`

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			`* from Citrix_Euem_RoundTrip"`
			`5.` Se a instância Citrix_Euem_RoundTrip estiver presente, reabra a sessão da área de trabalho.
			`6.` Se o problema persistir, entre em contato com o administrador Citrix.
Erro de Duração de Logon da Sessão	O gráfico não é carregado.	**O Citrix Profile Management não está em execução**	`1.` Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços.
			`2.` Certifique-se de que o **Citrix Profile Management Service** esteja em execução.
			`3.` Reabra a sessão da área de trabalho e tente. O gráfico deve ser exibido.
			`4.` Se o problema persistir, entre em contato com o administrador Citrix.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
Erro de Duração de Logon da Sessão	O gráfico não é carregado.	**O Citrix Profile Management não está instalado.**	`1.` Instale o Serviço de Gerenciamento de Perfil Citrix. `2.` Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços. `3.` Certifique-se de que o **Citrix Profile Management Service** esteja em execução. `4.` Reabra a sessão da área de trabalho e tente. O gráfico deve ser exibido. `5.` Se o problema persistir, entre em contato com o administrador Citrix.
Erro de Duração de Logon da Sessão	O gráfico não é carregado.	**Erro ao buscar dados.**	`1.` Abra o console de **Serviços**. Para abrir este console, clique em **Iniciar** e digite Serviços. `2.` Certifique-se de que o **Serviço de Instrumentação de Gerenciamento do Windows** esteja em execução.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			`3.` Se o serviço anterior já estiver em execução, execute o seguinte comando para garantir que `LogonTimings instance is present`: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` Se o problema persistir, entre em contato com o administrador Citrix.

Diagnosticar sessões de usuário históricas

O Citrix Director agora exibe os detalhes das sessões em estado ativo, desconectado ou encerrado. Anteriormente, você só podia ver os detalhes das sessões ativas. Com este recurso, os administradores de help desk podem solucionar problemas com uma sessão que foi encerrada ou está em estado encerrado. Os detalhes das sessões encerradas estão disponíveis para as últimas 24 horas e os últimos 2 dias. Você pode visualizar os seguintes detalhes de uma sessão encerrada ou terminada:

- Painel Detalhes da Máquina - Exibe os detalhes disponíveis da máquina onde a sessão selecionada foi iniciada
- Painel Detalhes da Sessão - Exibe os detalhes disponíveis da sessão selecionada.
- Duração do logon da sessão - Exibe as informações sobre a duração do logon para a sessão selecionada. Você pode visualizar o gráfico sobre o tempo gasto para o seguinte:
  - Intermediação
  - Inicialização da máquina

- Conexão HDX™
- Autenticação
- GPOs
- Scripts de logon
- Carregamento de perfil em disco
- Sessão interativa

Observação:

Este recurso está disponível apenas para clientes do Citrix Director com direito a Citrix Analytics e Performance.

Para visualizar as sessões de usuário históricas, faça o seguinte:

1. Clique em **Filtrar** > visualização **Sessão**.
2. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário.

   Gerenciador de Atividades de sessões de usuário históricas(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-am.png)
3. Selecione a sessão necessária na seção **Sessões Encerradas**.
4. Visualize os painéis **Detalhes da Máquina** e **Detalhes da Sessão**.

   Detalhes das sessões de usuário históricas(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-details.png)
5. Role para baixo e visualize a **duração do logon da sessão** para a sessão encerrada.

   Duração das sessões de usuário históricas(/en-us/citrix-virtual-apps-desktops/2407/media/dir-his-user-sessions-duration.png)

Usuários sombra

No Director, use o recurso de usuário sombra para visualizar ou trabalhar diretamente na máquina virtual ou sessão de um usuário. Você pode usar o modo sombra em VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja usar o modo sombra. Verifique isso verificando o nome da máquina listado na barra de título do usuário.

O Director inicia o modo sombra em uma nova guia; atualize as configurações do seu navegador para permitir pop-ups do URL do Director.

Acesse o recurso de modo sombra na exibição **Detalhes do Usuário**. Selecione a sessão do usuário e clique em **Sombra** na exibição Gerenciador de Atividades ou no painel Detalhes da Sessão.

Modo sombra em VDAs Linux

O modo sombra está disponível para VDAs Linux versão 7.16 ou posterior, executando as distribuições Linux RHEL7.3 ou Ubuntu versão 16.04.

> **Observação:**
>
> - O VDA deve estar acessível a partir da interface do usuário do Director para que o modo sombra funcione. Portanto, o modo sombra é possível apenas para VDAs Linux na mesma intranet que o cliente Director.
> - O Director usa FQDN para se conectar ao VDA Linux de destino. Certifique-se de que o cliente Director possa resolver o FQDN do VDA Linux.
> - O VDA deve ter os pacotes python websockify e x11vnc instalados.
> - A conexão noVNC com o VDA usa o protocolo WebSocket. Por padrão, o protocolo WebSocket **ws://** é usado. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro **wss://**. Instale certificados SSL em cada cliente Director e VDA Linux.

> Siga as instruções em Modo Sombra de Sessão para configurar seu VDA para o modo sombra.

1. Depois de clicar em **Sombra**, a conexão do modo sombra é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou sessão.
3. O administrador pode apenas visualizar a sessão em modo sombra.

Modo sombra em VDAs Windows

As sessões VDA do Windows são sombreadas usando o Assistência Remota do Windows. Habilite o recurso **Assistência Remota do Windows do Usuário** durante a instalação do VDA. Para obter mais informações, consulte Habilitar ou desabilitar recursos.

1. Depois de clicar em **Sombra**, 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. Uma solicitação de confirmação aparece no dispositivo do usuário.
3. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou da sessão.
4. Para ter mais controle, peça ao usuário para compartilhar o controle do teclado e do mouse.

OTIMIZAR NAVEGADORES MICROSOFT INTERNET EXPLORER PARA SOMBREAMENTO

Configure seu navegador Microsoft Internet Explorer para abrir automaticamente o arquivo Microsoft Remote Assistance (.msra) baixado com o cliente de Assistência Remota.

Para fazer isso, você deve habilitar a configuração de Solicitação automática para downloads de arquivos no editor de Política de Grupo:

Configuração do Computador \> Modelos Administrativos \> Componentes do Windows \> Internet Explorer \> Painel de Controle da Internet \> Página de Segurança \> Zona da Internet \> Solicitação automática para downloads de arquivos.

Por padrão, esta opção está habilitada para sites na zona da intranet local. Se o site do Director não estiver na zona da intranet local, considere adicionar o site manualmente a esta zona.

Enviar mensagens para usuários

No Director, envie uma mensagem para um usuário que esteja conectado a uma ou mais máquinas. Use este recurso para enviar avisos imediatos sobre ações administrativas, como manutenção iminente da área de trabalho, logoffs e reinícios de máquinas e redefinições de perfil.

1. Na exibição do Gerenciador de Atividades, selecione o usuário e clique em Detalhes.
2. Na exibição Detalhes do Usuário, localize o painel Detalhes da Sessão e clique em Enviar Mensagem.
3. Digite as informações da sua mensagem nos campos Assunto e Mensagem e clique em Enviar.

Se a mensagem for enviada com sucesso, uma mensagem de confirmação aparecerá no Director. A mensagem aparecerá na máquina do usuário.

Se a mensagem não for enviada com sucesso, uma mensagem de erro aparecerá no Director. Solucione o problema de acordo com a mensagem de erro. Quando terminar, digite o assunto e o texto da mensagem novamente e clique em **Tentar** novamente.

Resolver falhas de aplicativo

Na exibição **Gerenciador de Atividades**, clique na guia Aplicativos. Você pode visualizar todos os aplicativos em todas as máquinas às quais este usuário tem acesso, incluindo aplicativos locais e hospedados para a máquina atualmente conectada, e o status de cada um.

> **Observação:**
>
> Se a guia Aplicativos estiver esmaecida, entre em contato com um administrador com permissão para habilitar a guia.
>
> A lista inclui apenas os aplicativos que foram iniciados na sessão.

Para máquinas de SO de várias sessões e máquinas de SO de sessão única, os aplicativos são listados para cada sessão desconectada. Se o usuário não estiver conectado, nenhum aplicativo será exibido.

AÇÃO	DESCRIÇÃO
Encerrar o aplicativo que não está respondendo	Escolha o aplicativo que não está respondendo e clique em Encerrar Aplicativo. Assim que o aplicativo for encerrado, peça ao usuário para iniciá-lo novamente.
Encerrar processos que não estão respondendo	Se você tiver a permissão necessária, clique na guia Processos. Selecione um processo que esteja relacionado ao aplicativo ou que esteja usando uma grande quantidade de recursos de CPU ou memória, e clique em Encerrar Processo. No entanto, se você não tiver a permissão necessária para encerrar o processo, a tentativa de encerrar um processo falhará.
Reiniciar a máquina do usuário	Apenas para máquinas de SO de sessão única, para a sessão selecionada, clique em Reiniciar. Alternativamente, na exibição Detalhes da Máquina, use os controles de energia para reiniciar ou desligar a máquina. Instrua o usuário a fazer logon novamente para que você possa verificar o aplicativo

AÇÃO	DESCRIÇÃO
	novamente. Para máquinas de SO de várias sessões, a opção de reinicialização não está disponível. Em vez disso, faça logoff do usuário e permita que o usuário faça logon novamente.
Colocar a máquina em modo de manutenção	Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina em modo de manutenção. Na exibição Detalhes da Máquina, clique em Detalhes e ative a opção de modo de manutenção. Encaminhe para o administrador apropriado.

Restaurar conexões de desktop

No Director, verifique o status da conexão do usuário para a máquina atual na barra de título do usuário.

Se a conexão da área de trabalho falhou, o erro que causou a falha é exibido e pode ajudar você a decidir como solucionar o problema.

AÇÃO	DESCRIÇÃO
Certifique-se de que a máquina não esteja em modo de manutenção	Na página Detalhes do Usuário, certifique-se de que o modo de manutenção esteja desativado.
Reiniciar a máquina do usuário	Selecione a máquina e clique em **Reiniciar**. Use esta opção se a máquina do usuário não estiver respondendo ou não conseguir se conectar. Por exemplo, quando a máquina está usando uma quantidade incomumente alta de recursos da CPU, o que pode tornar a CPU inutilizável.

Restaurar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

Na exibição Detalhes do Usuário, solucione falhas de sessão no painel **Detalhes da Sessão**. Você pode visualizar os detalhes da sessão atual, indicados pelo ID da sessão.

AÇÃO	DESCRIÇÃO
Encerrar aplicativos ou processos que não estão respondendo	Clique na guia **Aplicativos**. Selecione qualquer aplicativo que não esteja respondendo e clique em **Encerrar Aplicativo**. Da mesma forma, selecione qualquer processo correspondente que não esteja respondendo e clique em **Encerrar Processo**. Além disso, encerre processos que estão consumindo uma quantidade incomumente alta de memória ou recursos da CPU, o que pode tornar a CPU inutilizável.
Desconectar a sessão do Windows	Clique em **Controle de Sessão** e selecione **Desconectar**. Esta opção está disponível apenas para máquinas de SO de múltiplas sessões intermediadas. Para sessões não intermediadas, a opção é desabilitada.
Fazer logoff da sessão do usuário	Clique em **Controle de Sessão** e selecione **Logoff**.

Para testar a sessão, o usuário pode tentar fazer logon novamente nela. Você também pode acompanhar o usuário para monitorar mais de perto esta sessão.

Redefinir um perfil de usuário

> **CUIDADO:**

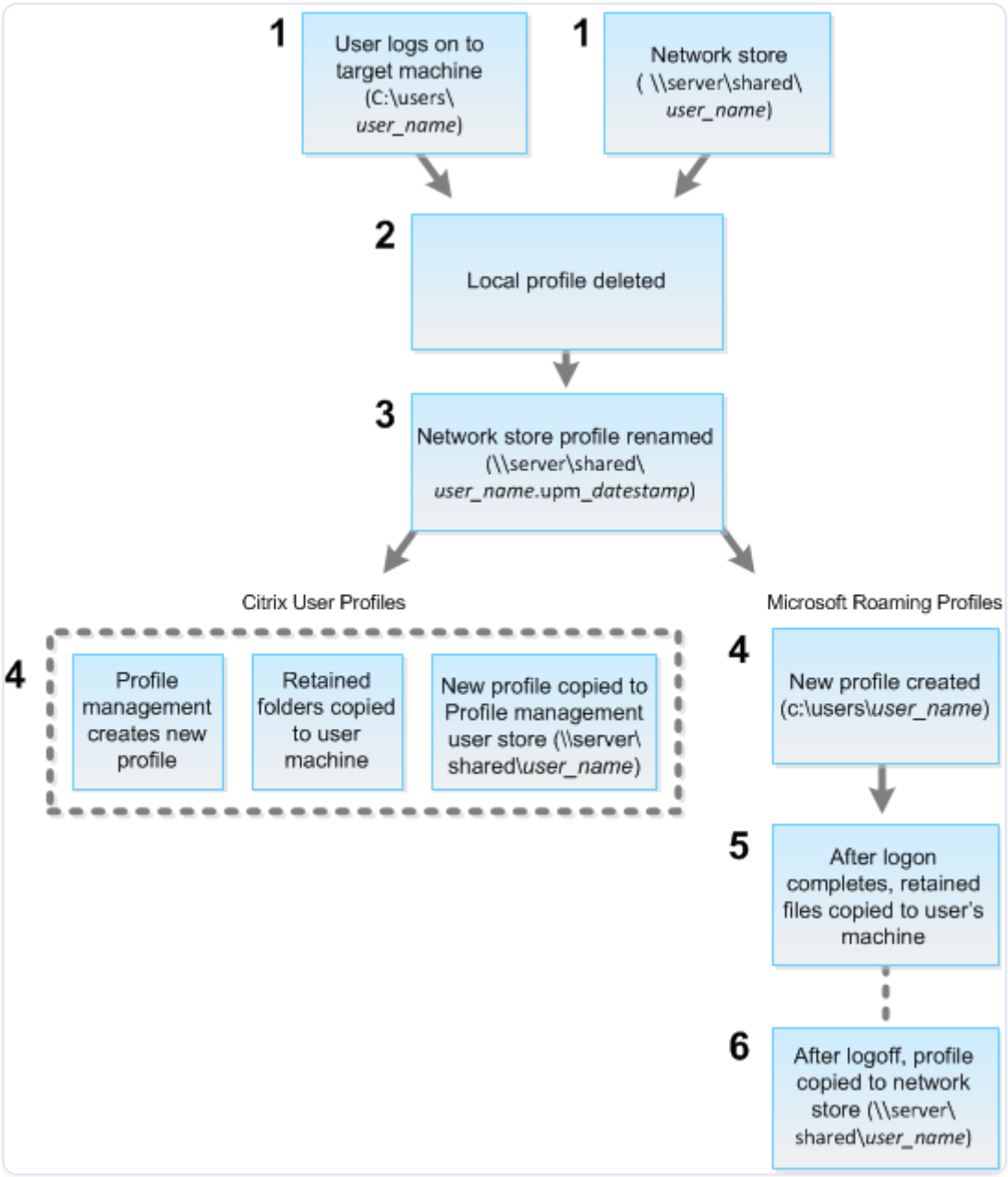
> Quando um perfil é redefinido, as pastas e arquivos do usuário são salvos e copiados para o novo perfil. No entanto, a maioria dos dados do perfil do usuário está ausente (por exemplo, o registro é redefinido e as configurações do aplicativo podem ser excluídas).

> A função de redefinição se aplica a soluções de perfil baseadas em arquivo e baseadas em contêiner.

Como os perfis redefinidos são processados

Qualquer perfil de usuário Citrix® ou perfil móvel da Microsoft pode ser redefinido. Depois que o usuário faz logoff e você seleciona o comando de redefinição (seja no Director ou usando o SDK do PowerShell), o Director primeiro identifica o perfil de usuário em uso e emite um comando de redefinição apropriado. O Director recebe as informações através do Profile Management, incluindo informações sobre o tamanho, tipo e tempos de logon do perfil.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.



O comando de redefinição emitido pelo Director especifica o tipo de perfil. O serviço Profile Management então tenta redefinir um perfil desse tipo e procura o compartilhamento de rede

apropriado (repositório de usuário). Se o usuário for processado pelo Profile Management, mas receber um comando de perfil móvel, 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 Citrix ou um perfil móvel da Microsoft.

   Para perfis de usuário Citrix, o novo perfil é criado usando as regras de importação do Profile Management. As pastas são copiadas de volta para o perfil de rede, e o usuário pode fazer logon normalmente. Se um perfil móvel for usado para a redefinição, quaisquer configurações de registro no perfil móvel serão preservadas no perfil redefinido. Você pode configurar o Profile Management para que um perfil de modelo substitua o perfil móvel, se necessário.

   Para perfis móveis da Microsoft, o Windows cria um 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 redefinir um perfil de usuário no Director

Se você estiver usando o Citrix Virtual Desktops™ (Desktop VDA), faça o seguinte:

1. No **Director**, procure o usuário cujo perfil você deseja redefinir e, em seguida, selecione a sessão desse usuário.
2. Clique em **Redefinir Perfil**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente. As pastas e arquivos que foram salvos do perfil do usuário são copiados para o novo perfil.

Se você estiver usando o Citrix Virtual Desktops (Server VDA), precisará estar logado para realizar a redefinição do perfil. O usuário precisará então fazer logoff e logon novamente para concluir a redefinição do perfil.

> **Importante:**

> Se o usuário tiver perfis em várias plataformas (como Windows 8 e Windows 7), instrua-o a fazer logon novamente primeiro na mesma área de trabalho ou aplicativo que ele relatou como problema. Essa ação de logon garante que o perfil correto seja redefinido. Se o perfil for um perfil de usuário Citrix, ele já estará redefinido quando a área de trabalho do usuário

> aparecer. Se o perfil for um perfil móvel da Microsoft, a restauração da pasta ainda poderá estar em andamento por um breve período. O usuário deve permanecer logado até que a restauração seja concluída.

> Se o perfil não for redefinido com êxito (por exemplo, o usuário não conseguir fazer logon novamente na máquina ou alguns arquivos estiverem faltando), você deverá restaurar manualmente o perfil original.

Observe o seguinte:

- Se o armazenamento de usuário estiver habilitado como a solução de perfil de usuário, o novo perfil conterá as seguintes pastas pessoais do perfil de usuário original:
  - Área de trabalho
  - Cookies
  - Favoritos
  - Documentos
  - Imagens
  - Música
  - Vídeos
- A partir do Citrix Profile Management versão 2407, se o contêiner de perfil estiver habilitado como a solução completa de perfil de usuário, o novo perfil reterá as pastas pessoais anteriores.
- No Windows 8 e posterior, os cookies não são copiados para o novo perfil quando os perfis são redefinidos.

Para restaurar manualmente um perfil após uma redefinição falha

1. Instrua o usuário a fazer logoff de todas as sessões.
2. Exclua o perfil local, se existir.
3. Localize a pasta arquivada no compartilhamento de rede que contém a data e a hora anexadas ao nome da pasta, a pasta com uma extensão .upm_datestamp.
4. Exclua o nome do perfil atual. Ou seja, aquele sem a extensão upm_datestamp.
5. Renomeie a pasta arquivada usando o nome do perfil original. Ou seja, remova a extensão de data e hora. Você retornou o perfil ao seu estado original, antes da redefinição.

Para redefinir um perfil usando o PowerShell SDK

Você pode redefinir um perfil usando o Broker PowerShell SDK.

NEW-BROKERMACHINECOMMAND

Cria um comando enfileirado para entrega a um usuário, sessão ou máquina específica. Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`.

EXEMPLOS

Consulte os exemplos a seguir para obter detalhes sobre como usar os cmdlets do PowerShell para redefinir um perfil:

Redefinir um perfil do Profile Management

- Suponha que você queira redefinir o perfil para user1. Use o comando PowerShell New-BrokerMachineCommand. Por exemplo:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **Importante:**
>
> O `CommandData $byteArray` deve estar no seguinte formato: `<SID>[,<backup path>]`. Se você não fornecer o caminho de backup, o Profile Management gerará uma pasta de backup nomeada pela data e hora atuais.

Redefinir um perfil de roaming do Windows

- Suponha que você queira redefinir o perfil de roaming para user1. Use o comando PowerShell New-BrokerMachineCommand. Por exemplo:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

Gravar sessões

Você pode gravar sessões ICA® usando os controles de Gravação de Sessão nas telas **Detalhes do Usuário** e **Detalhes da Máquina** no Director. Este recurso está disponível para clientes em sites **Premium**.

Gravação Dinâmica de Sessão

Você pode gravar a sessão ativa atual usando os controles de Gravação de Sessão na tela **Detalhes do Usuário**. Para obter mais informações sobre a Gravação Dinâmica de Sessão, consulte o artigo serviço de Gravação de Sessão.

Gravação de Sessão baseada em política

Para configurar a Gravação de Sessão baseada em política no Director usando a ferramenta DirectorConfig, consulte a seção **Configurar o Director para usar o Servidor de Gravação de Sessão** em Configurar políticas de gravação de sessão. Os controles de Gravação de Sessão estão disponíveis no Director somente se o usuário logado tiver permissão para modificar as políticas de Gravação de Sessão. Essa permissão pode ser definida no console de Autorização de Gravação de Sessão, conforme descrito em Autorizar usuários.

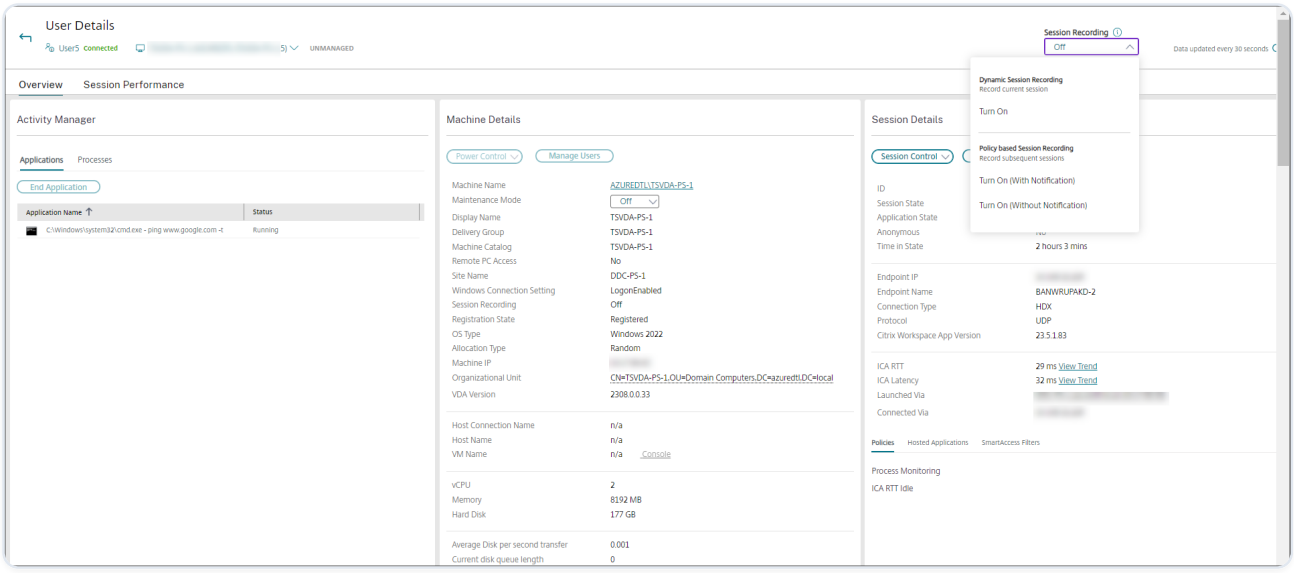
> **Nota:** As alterações feitas nas configurações de Gravação de Sessão através do Director ou do console de Política de Gravação de Sessão entram em vigor a partir da sessão ICA subsequente.

Controles de Gravação de Sessão no Director

Você pode usar as ações **Detalhes do Usuário** > **Gravação de Sessão** para gravar as sessões atuais ou subsequentes.

- Ativar Gravação Dinâmica de Sessão - a sessão atual é gravada.
- Ativar (com notificação) - as sessões subsequentes são gravadas e o usuário é notificado sobre a gravação da sessão ao fazer logon na sessão ICA.
- Ativar (sem notificação) - as sessões subsequentes são gravadas e a sessão é gravada silenciosamente sem notificar o usuário.
- Desativar - desabilitar a gravação de sessões para o usuário.

O painel **Políticas** exibe o nome da política de Gravação de Sessão ativa.



O painel **Detalhes da Máquina** exibe o status da política de Gravação de Sessão para a máquina.

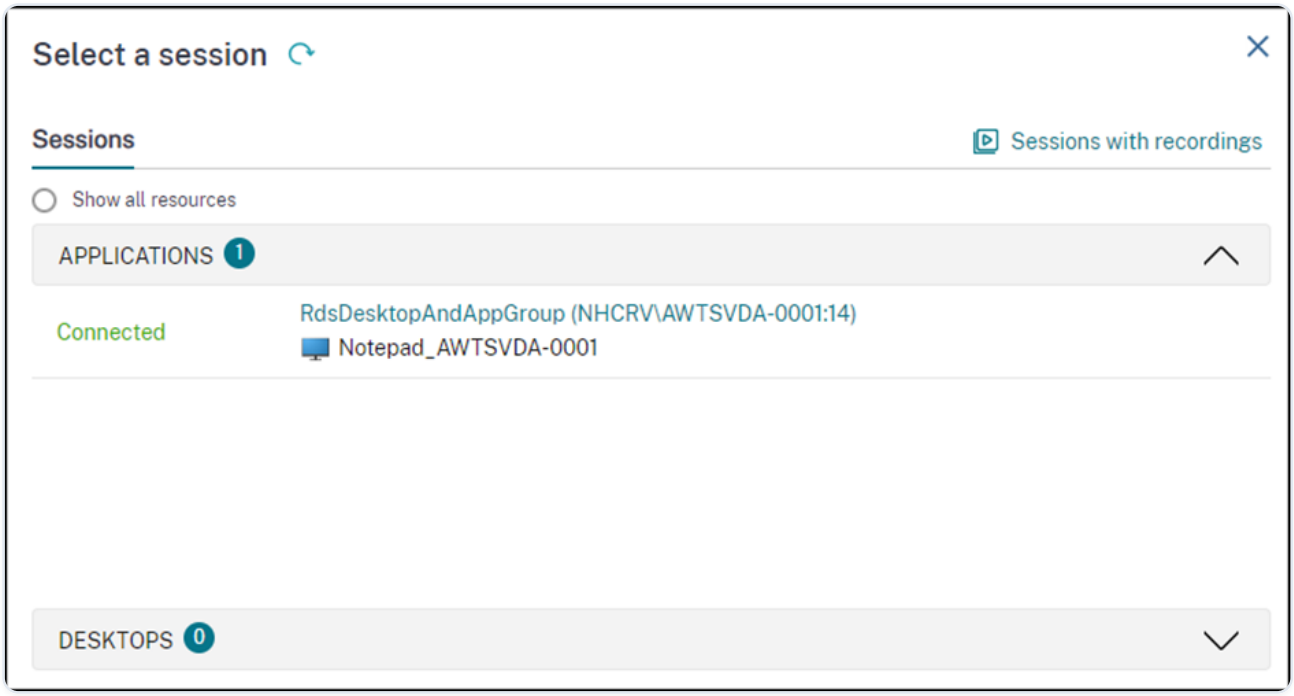
REPRODUZIR SESSÕES AO VIVO E GRAVADAS

Você pode reproduzir sessões de usuário gravadas e ao vivo para entender os problemas encontrados pelo usuário. O acesso fácil a gravações e métricas relacionadas à sessão dentro do console do Director elimina a necessidade de procurar as gravações em vários servidores de gravação de sessão ou de procurar aplicativos de terceiros para visualizar as gravações. Isso ajuda a correlacionar os problemas descobertos nas gravações com as métricas de desempenho.

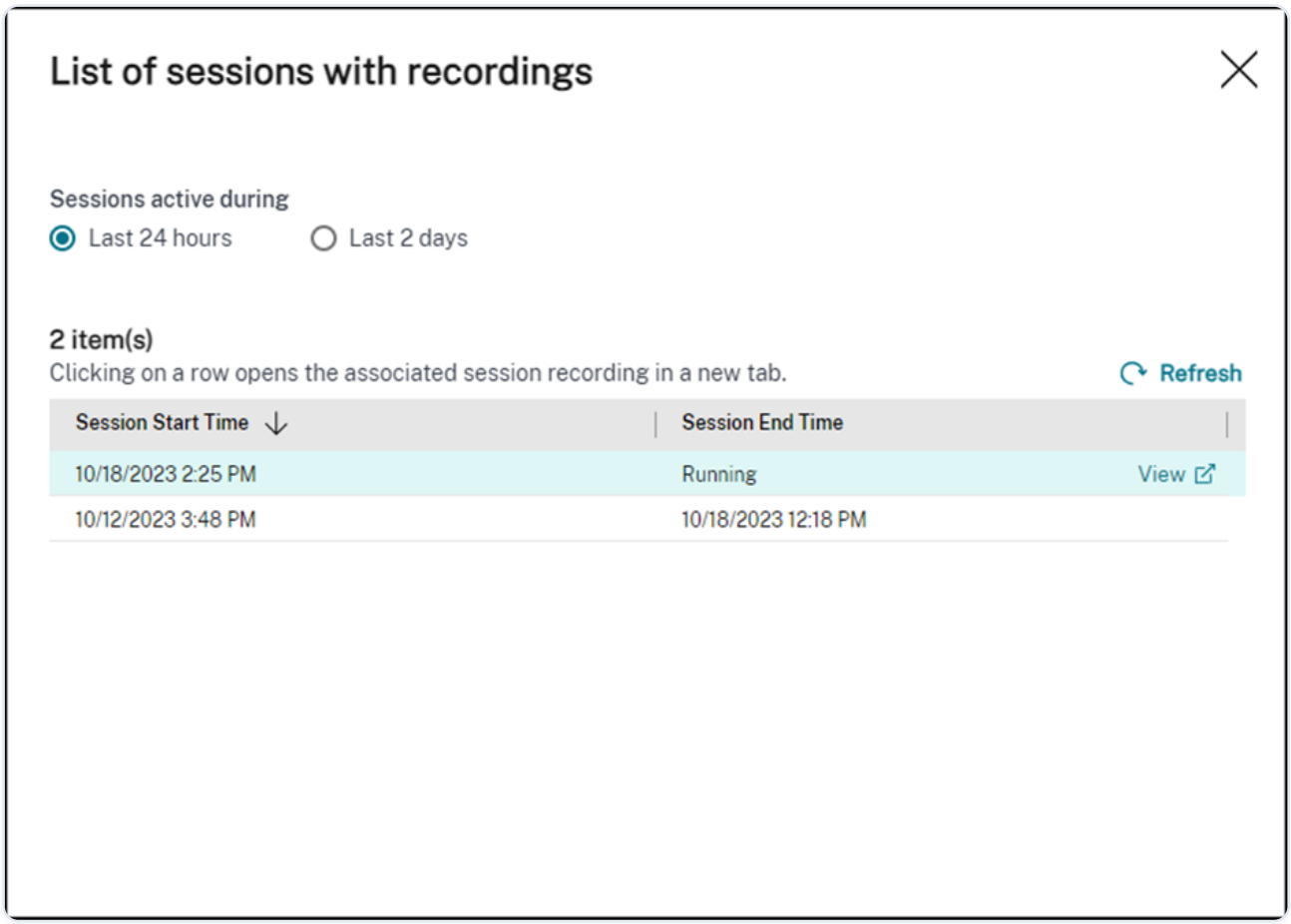
Este recurso requer o seguinte:

- O VDA e os servidores de Gravação de Sessão estão na versão 2308 ou posterior.
- O Delivery Controller™ e o Director estão na versão 2311 ou posterior.

O Director armazena as gravações de sessão em um repositório centralizado. A lista de gravações pertencentes ao usuário é exibida ao clicar no link **Seletor de Sessão** modal > **Sessões com gravações**.



Você pode optar por visualizar gravações de sessões que estiveram ativas nas últimas 24 horas ou nos últimos 2 dias. As gravações ao vivo de sessões atualmente ativas são marcadas com **Hora de Término da Sessão** como **Em Execução**.



Clique no link **Exibir** para reproduzir a gravação em uma nova guia usando o servidor de reprodução do Citrix Session Recording.

Pesquisa unificada para implantações híbridas multi-nuvem

Anteriormente, durante a triagem, ao pesquisar um usuário no Director, você obtinha os detalhes do usuário apenas se ele fosse de um site local. Se o usuário fosse de um site na nuvem, você precisava ir para o Monitor e pesquisar novamente.

Com esta funcionalidade de pesquisa aprimorada, você pode pesquisar usuários de sites na nuvem ou sites locais usando a opção **Pesquisar** no Director. Você pode usar este recurso ao empregar implantações híbridas (sites na nuvem e locais) e ao usar o Director para fins de triagem. Você pode obter os detalhes dos usuários independentemente de serem de sites locais ou na nuvem. Se o site estiver presente no Director, você pode navegar diretamente para o Gerenciador de Atividades da sessão selecionada no Director. Se o site não estiver presente no Director, você pode navegar diretamente para o Gerenciador de Atividades da sessão selecionada no Monitor. E, então, continuar com a triagem.

Observação:

Você pode usar o console de pesquisa unificada através do Citrix Director.

Este recurso reduz o tempo médio para resolver problemas e oferece uma experiência perfeita com um único console para usuários da nuvem e locais. O benefício adicional é que não há um crescimento rápido no tamanho do banco de dados, pois apenas os detalhes do site na nuvem são adicionados ao Director. Os detalhes do usuário são salvos na própria nuvem.

Observação:

Você pode obter resultados de pesquisa em até três segundos para até seis ou menos sites na nuvem.

Para habilitar este recurso, você precisa conectar o site na nuvem ao Director.

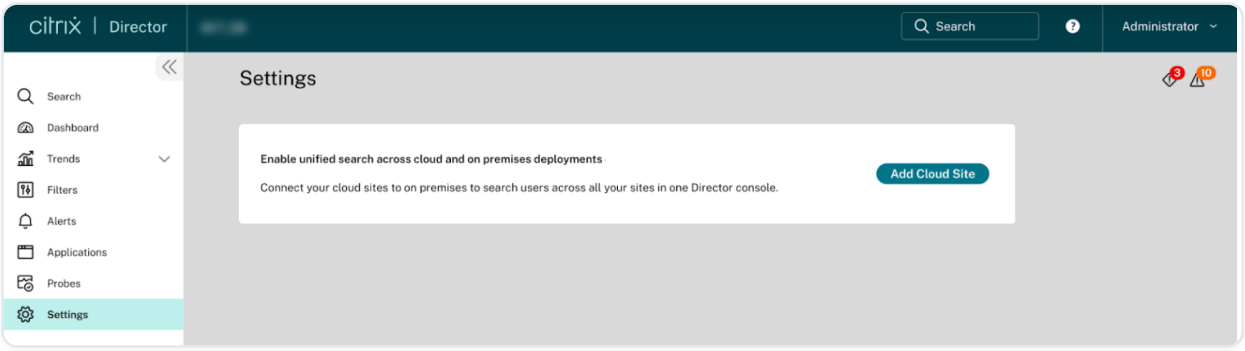
Conectando o site na nuvem ao Director

Pré-requisitos

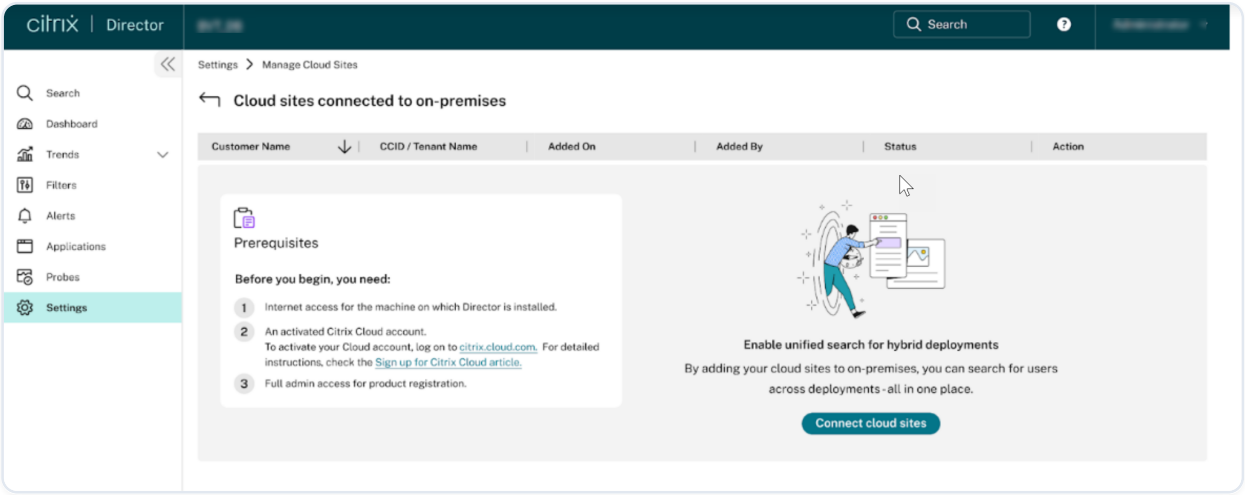
- Certifique-se de que há acesso à internet para a máquina na qual o Citrix Director está instalado.
- Para usar os serviços do Citrix Cloud, você deve ser capaz de se conectar aos endereços Citrix necessários através da porta HTTPS 443. Para mais informações, consulte Requisitos de conectividade com a Internet.
- Certifique-se de ter acesso de administrador completo para realizar o registro do produto.

Etapas de configuração

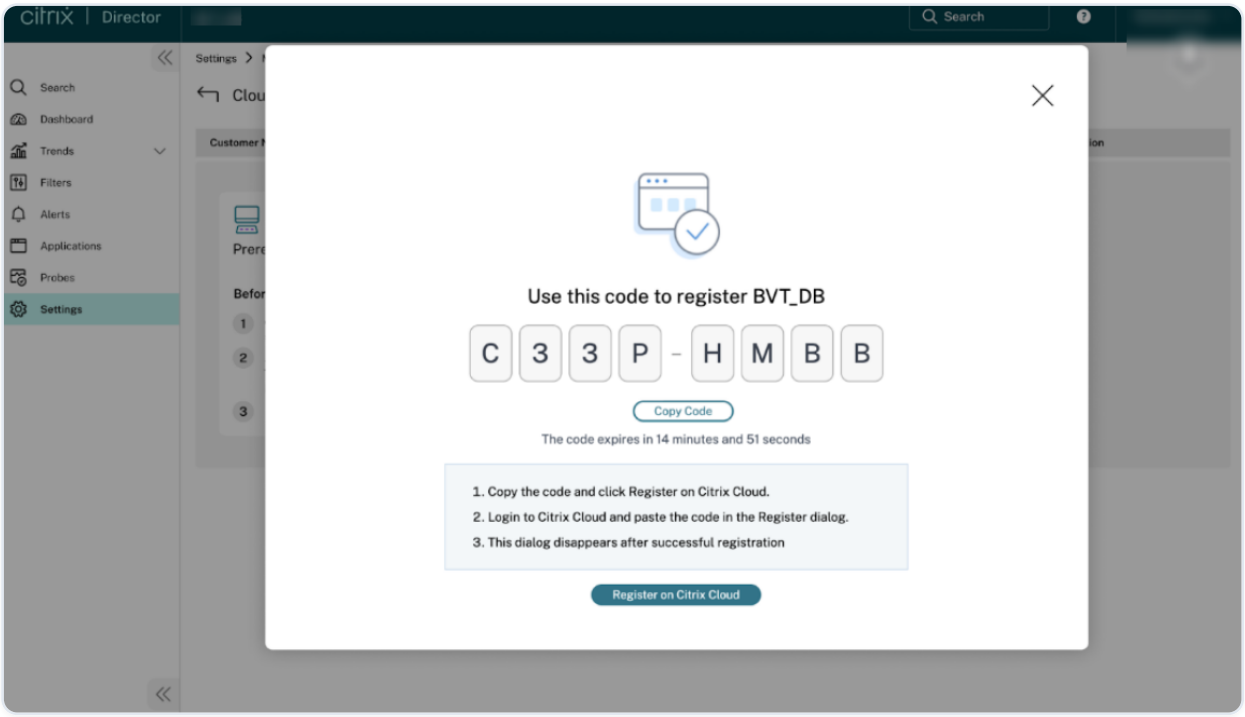
1. Faça login no Director como administrador completo. A página do Painel do Director é exibida.
2. Clique na guia **Configurações**. A página **Configurações** é exibida.



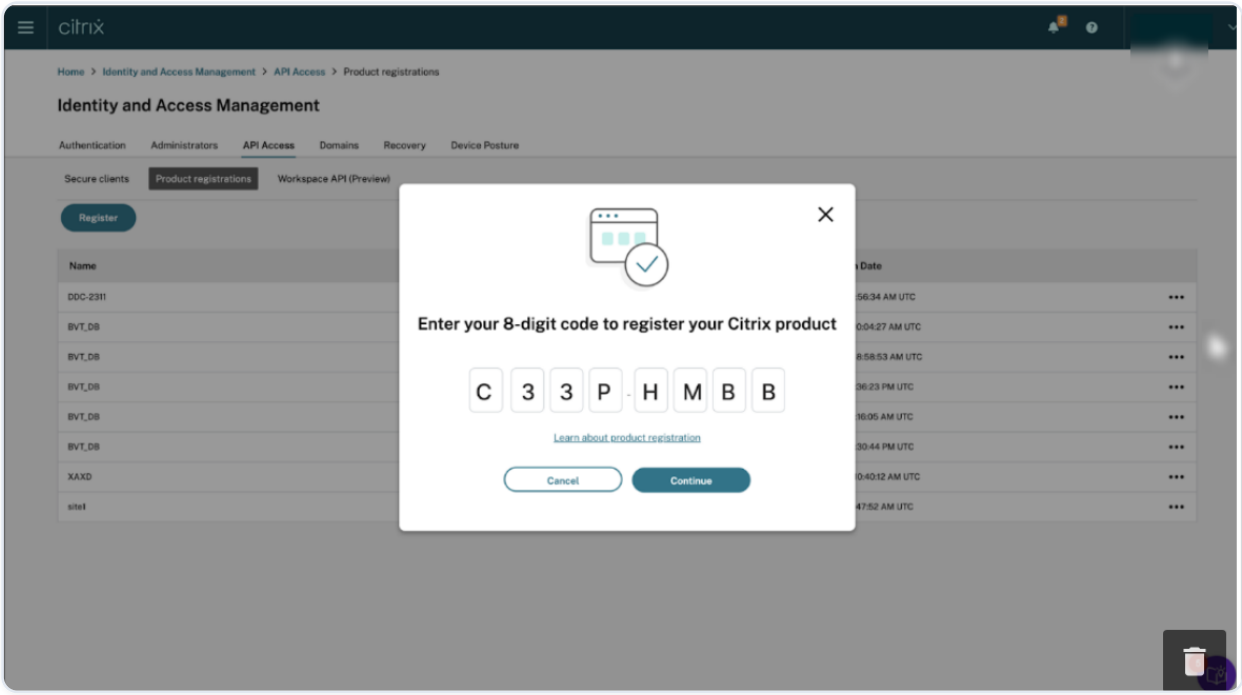
3. Clique em **Adicionar Site na Nuvem**. A seguinte página é exibida:



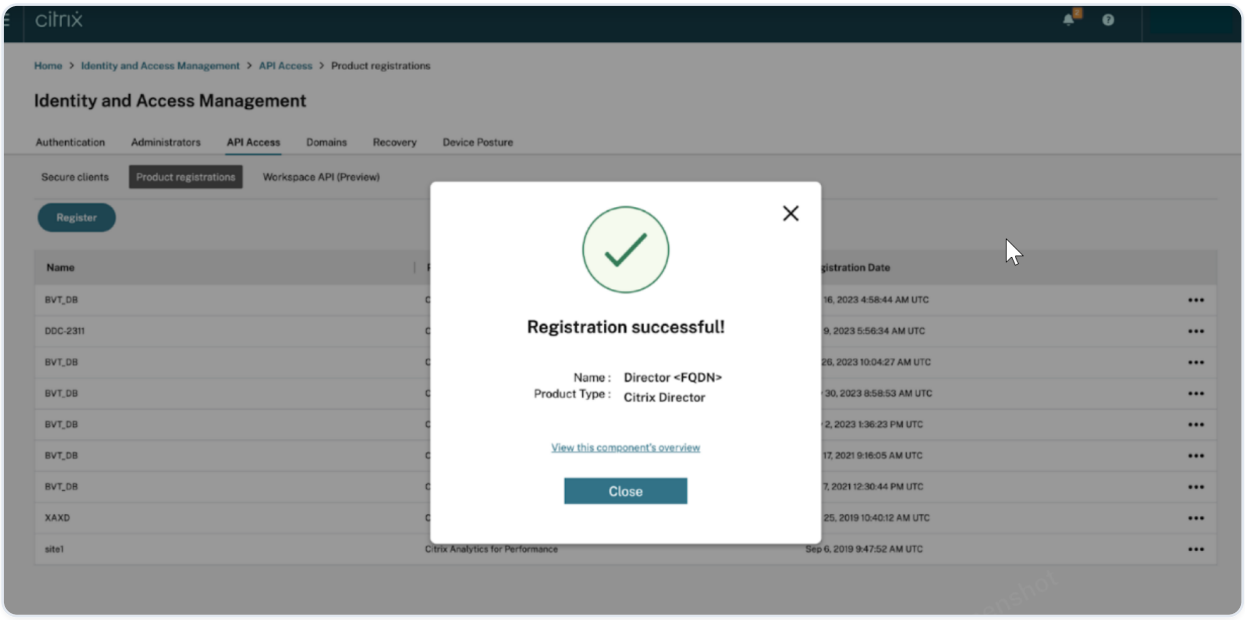
4. Revise os pré-requisitos e então clique em **Conectar sites de nuvem** para iniciar o processo de configuração. Um código de registro exclusivo de 8 dígitos é gerado para ser usado para registrar este site no Citrix Cloud.



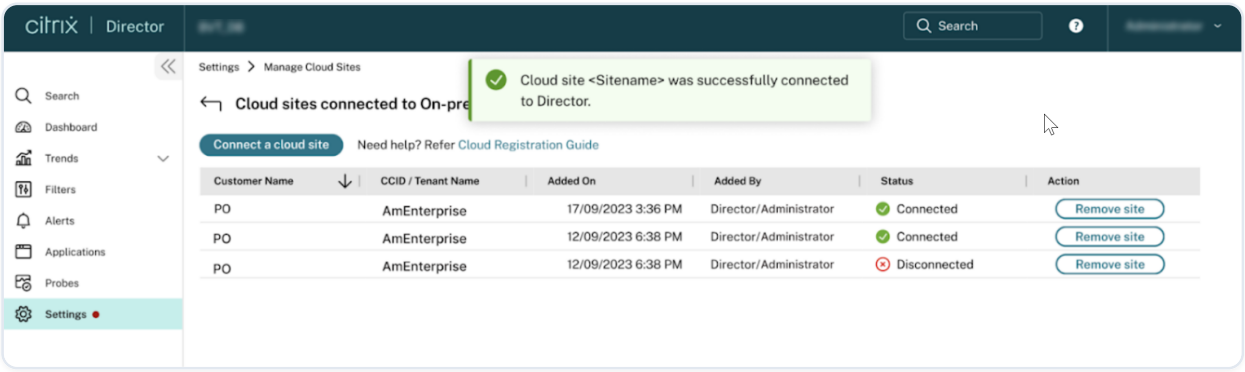
5. Clique em **Copiar Código** para copiar o código e então clique em **Registrar no Citrix Cloud**. Você será redirecionado para a URL de registro no Citrix Cloud.
6. Faça login com suas credenciais do Citrix Cloud e selecione seu cliente.
7. Cole o código de registro copiado na página **Registros de Produtos** no Citrix Cloud. Clique em **Continuar** para registrar o site.



8. Clique em **Continuar**. Seu site de nuvem é registrado no Citrix Director e você recebe a seguinte mensagem:



9. Clique em **Fechar**. A seguinte tela aparece:



10. Para configurar vários sites de nuvem com o Director, repita as etapas de configuração anteriores para cada site a partir do Director.

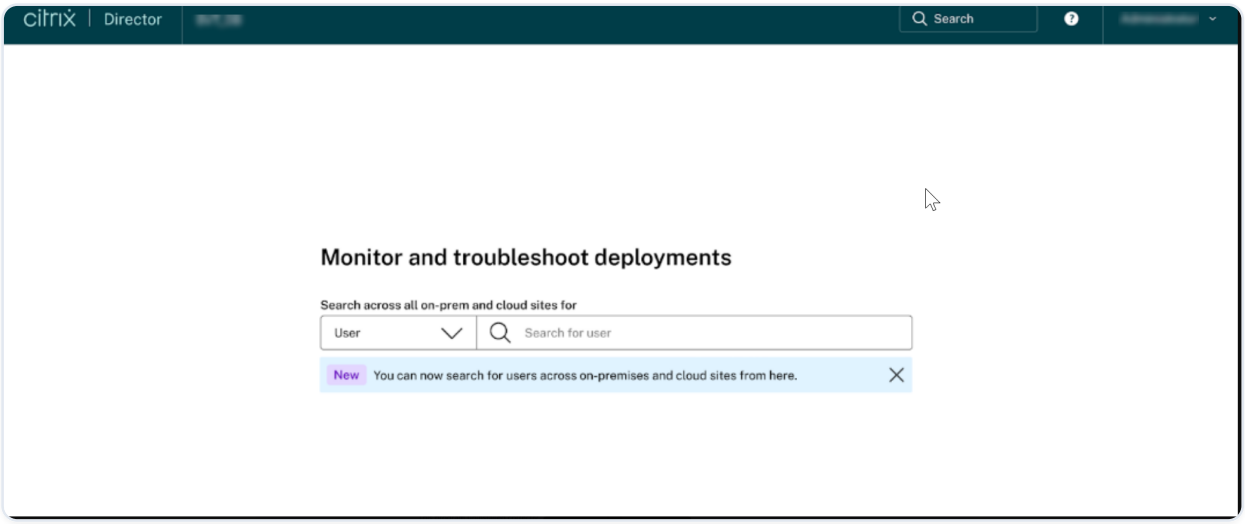
    Caso você tenha mais de uma instância do Director em execução por site, configure a partir de qualquer instância do Director. Todas as outras instâncias do Director conectadas ao site são atualizadas na próxima atualização após o processo de configuração.

> **Observação:**
>
> Para desconectar seu site do Citrix Director, clique em **Remover site**. Esta opção exclui a configuração existente.

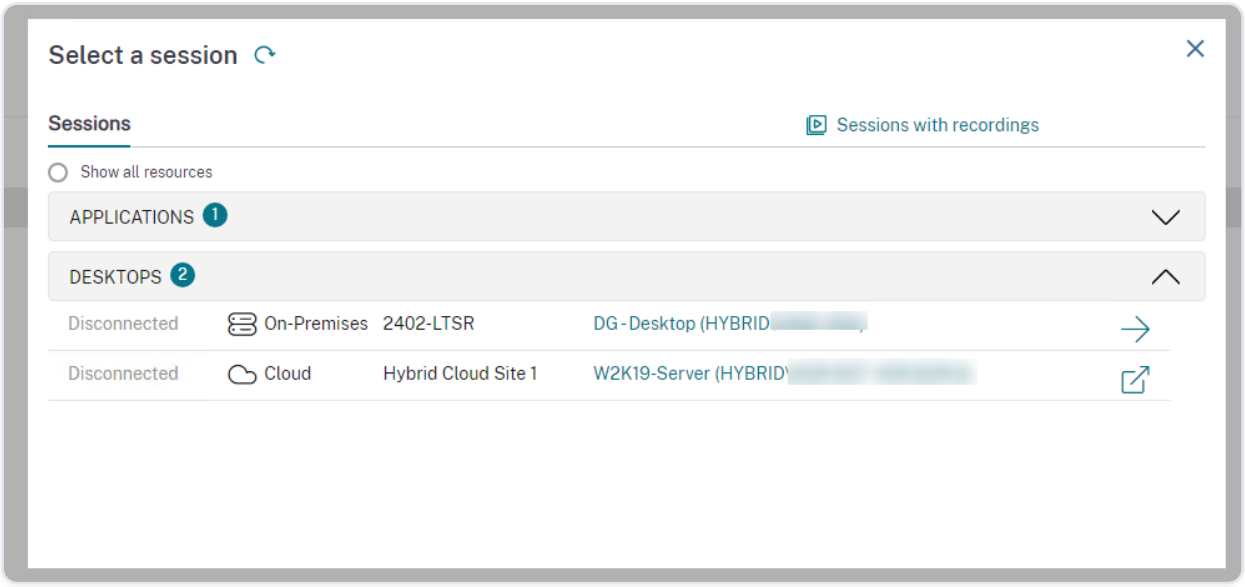
Pesquisando por um usuário de implantações híbridas

Para pesquisar um usuário, faça o seguinte:

1. Clique em **Pesquisar** na barra de navegação superior. A página **Monitorar e solucionar problemas de implantações** é exibida:



2. Selecione **Usuário** na lista suspensa e insira o nome de usuário. Uma lista de sessões ativas e com falha de implantações locais e na nuvem é exibida:



3. Selecione uma sessão para inspecionar:

- Se for uma sessão usando implantação na nuvem, a URL relevante do DaaS Monitor com o contexto do usuário é aberta na página **Gerenciador de Atividades** para iniciar rapidamente a solução de problemas.
- Se for uma sessão usando implantação local, a página Gerenciador de Atividades é aberta rapidamente para iniciar a solução de problemas.

Monitoramento de infraestrutura

O Director agora oferece visibilidade sobre a saúde operacional dos componentes do Citrix Virtual Apps and Desktops™. Este recurso ajuda você a identificar, solucionar e resolver facilmente problemas relacionados à sua infraestrutura. Atualmente, a saúde dos componentes Citrix Provisioning (PVS) e StoreFront é monitorada.

Para suportar este recurso, um novo executável do Windows chamado Citrix Infrastructure Monitor é introduzido para componentes Citrix. Isso ajuda na coleta e transmissão de métricas de saúde relevantes de servidores PVS ou StoreFront™ para o Director.

Este recurso ajuda você a obter conjuntos de dados de monitoramento críticos e alertas proativos sobre as métricas do sistema dos servidores PVS e StoreFront em um único console no Director. Os dados são coletados a cada cinco minutos dos componentes de monitoramento para garantir as informações mais recentes.

Este recurso visa aprimorar a eficiência operacional, oferecendo monitoramento proativo, métricas detalhadas e alertas automatizados, garantindo que sua infraestrutura Citrix funcione de forma suave e eficiente.

Principais recursos

Monitoramento em tempo real:

- Monitoramento contínuo de componentes da infraestrutura Citrix, como servidores Citrix Provisioning™ (PVS) e StoreFront.
- Visualizações de painel apresentando a saúde do sistema, utilização de recursos e métricas de desempenho relevantes.

Análise detalhada:

- Fornece análise detalhada sobre as métricas de saúde do sistema, como status de conectividade e status de serviço ou processo para cada componente.
- Detalhes sobre as métricas de utilização de recursos, como CPU, memória e utilização de disco.

Alertas e notificações automatizados:

- Limites de alerta personalizáveis para várias métricas e estados com escopos granulares.
- Notificações em tempo real por e-mail e webhooks.

Casos de uso

Eficiência operacional:

Garante que as equipes de administração da Citrix possam manter alta disponibilidade e desempenho de seus servidores e serviços Citrix. Esse recurso também ajuda a minimizar o tempo de inatividade, identificando proativamente e alertando os administradores sobre problemas antes que eles afetem grupos de usuários significativos.

Resolução mais rápida de tickets:

Monitora as principais métricas de integridade e desempenho do servidor para avaliar a entrega ideal de aplicativos e desktops virtuais aos usuários. Use essas métricas para diagnosticar e resolver reclamações de usuários relacionadas ao desempenho, analisando os componentes associados.

Pré-requisitos

- Citrix Virtual Apps and Desktops versão 2407 ou posterior
- Configure HTTPS para o Citrix Infrastructure Monitor com DDC. Este pré-requisito é opcional, mas recomendado. Para mais informações, consulte Configurar HTTPS para o Citrix Infrastructure Monitor.
- Contas de usuário ou permissões necessárias para executar o Citrix Infrastructure Monitor:
    - Contas de usuário com permissões de administrador do Windows para instalar o Citrix Infrastructure Monitor nas máquinas de endpoint.
    - Uma conta de usuário administrador completa ou uma função personalizada com as seguintes permissões do Director:
        - Criar\Editar\Habilitar\Excluir Políticas de Alerta
        - Criar\Editar\Remover Configuração do Servidor de E-mail de Alerta
        - Descartar Alertas
        - Visualizar Políticas de Alerta
        - Visualizar Alertas
        - Visualizar página do Painel
        - Visualizar página do Monitor de Infraestrutura

> **Observação:**

> Se você não tiver permissão para acessar a página de **Alertas**, a opção **Gerenciar Alertas** será desabilitada na página de **Monitoramento de Infraestrutura**.

Introdução ao Monitoramento de Infraestrutura

Etapa 1: Instalação do Citrix Infrastructure Monitor

Execute os passos a seguir para concluir a instalação no componente de destino e estabelecer a conexão para coleta segura de dados.

Etapa 1.1: Identificar os componentes de destino

Identifique os componentes de destino, como servidores PVS ou StoreFront, que precisam ser monitorados.

Etapa 1.2 Baixar o Citrix Infrastructure Monitor

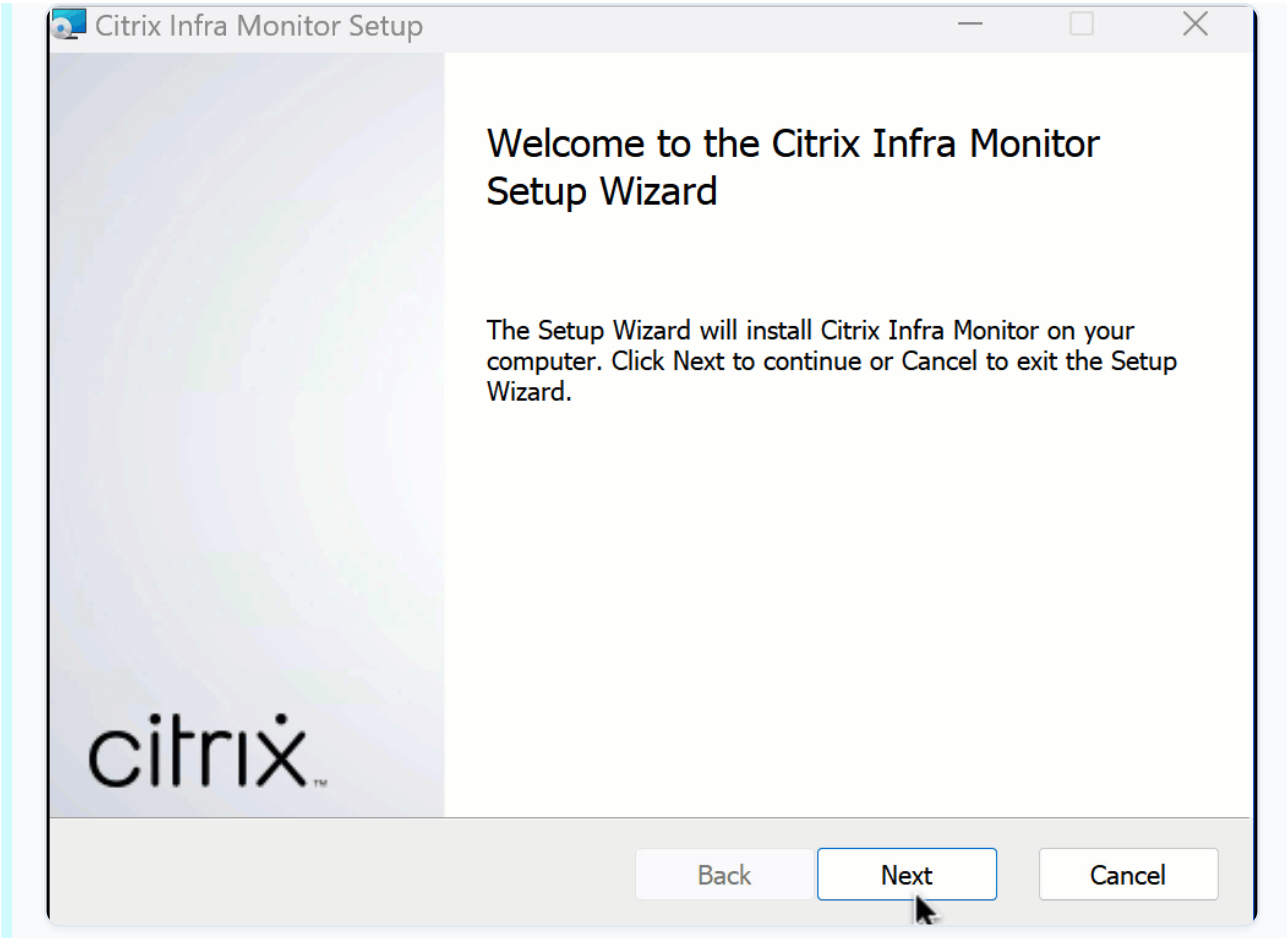
Você pode baixar `CitrixInfraMonitor.msi` na página downloads da Citrix no servidor de destino identificado na Etapa 1.1.

Etapa 1.3: Executar o Citrix Infrastructure Monitor

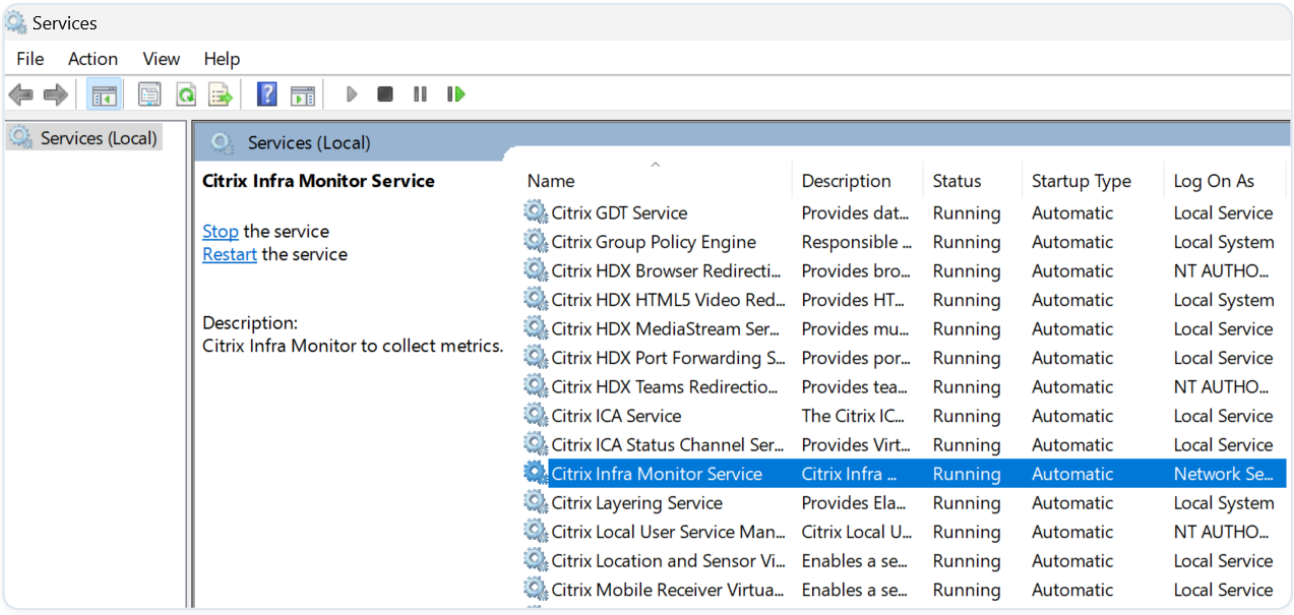
Execute o instalador `CitrixInfraMonitor.msi` no componente de destino seguindo as instruções do assistente de instalação.

> **Observação:**

> Usuários com privilégios administrativos podem instalar e configurar o Citrix Infrastructure Monitor no componente de destino.



Após a instalação ser bem-sucedida, você pode visualizar o Serviço de Monitoramento de Infraestrutura Citrix na seção **Serviços**:



Etapa 1.4: Obtenha o token de registro

Obtenha o token fornecido no arquivo `RegistrationToken.txt` em `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` no sistema onde o Citrix

Infrastructure Monitor está instalado e mantenha-o pronto para uso na Etapa 3: Registrar o Citrix Infrastructure Monitor.

> **Observação:**
>
> Após instalar com sucesso `CitrixInfraMonitor.msi`, o instalador cria uma exceção para a porta 9595. Se você estiver usando um firewall de terceiros, talvez seja necessário permitir a comunicação TCP para esta porta manualmente para usar o serviço Citrix Infrastructure Monitoring.

Etapa 2: Configurar HTTPS para o Citrix Infrastructure Monitor

> **Observação:**
>
> O serviço Citrix Infrastructure Monitor também funciona no modo HTTP e, neste caso, a seguinte configuração não é necessária. No entanto, recomendamos que você o use no modo HTTPS. Execute as seguintes etapas somente se precisar configurar HTTPS para o Citrix Infrastructure Monitor.

Etapa 2.1: Carregar o certificado para a máquina

1. Obtenha um certificado PFX para sua máquina onde o Citrix Infrastructure Monitor está instalado. Para obter mais informações sobre a geração de arquivos PFX, consulte Como criar um arquivo PFX.

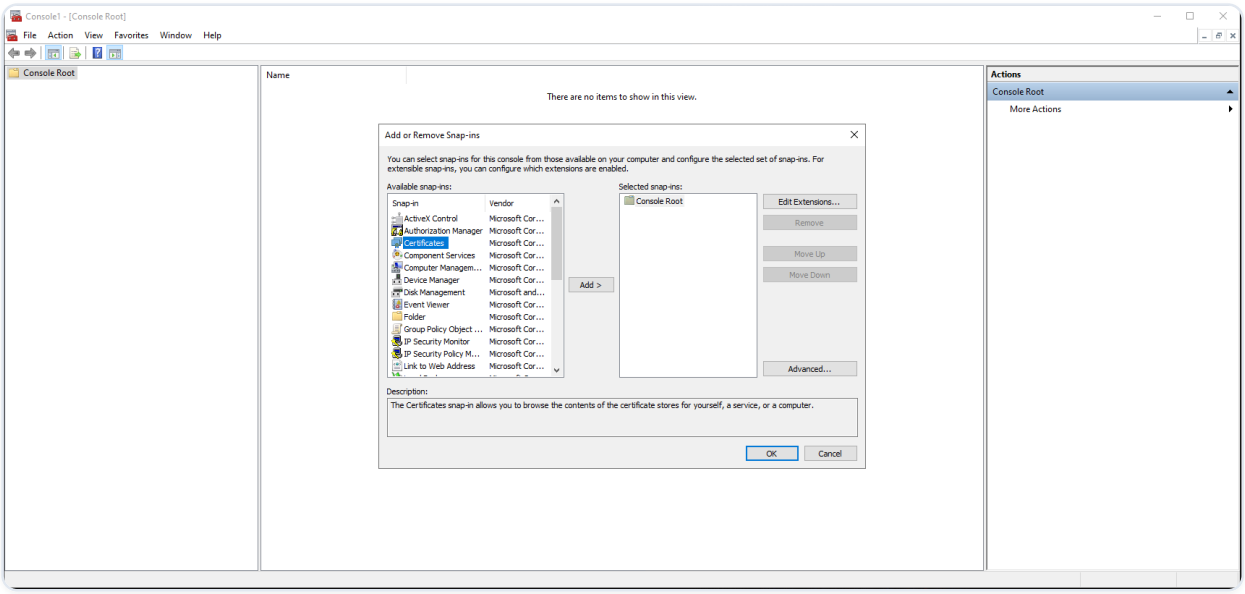
   > **Observação:**
   >
   > Você também pode usar arquivos PFX protegidos por senha.

2. Carregue o certificado para a máquina em qualquer local.

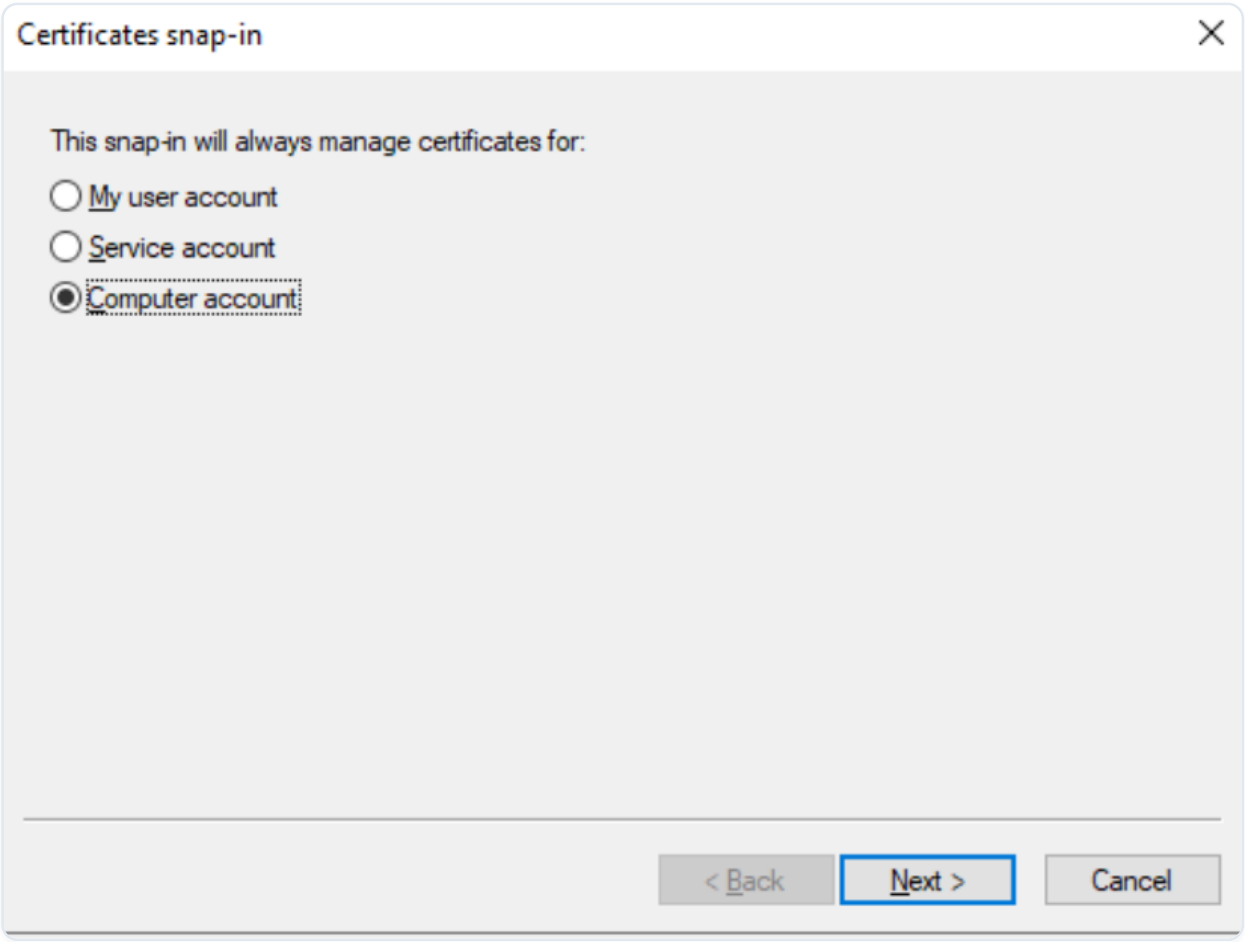
Passo 2.2: Importar o certificado para certificados de computador

1. Clique em **Iniciar** > **Executar** > digite `mmc` e, em seguida, clique em **OK**. A janela **Console 1 -** é exibida.

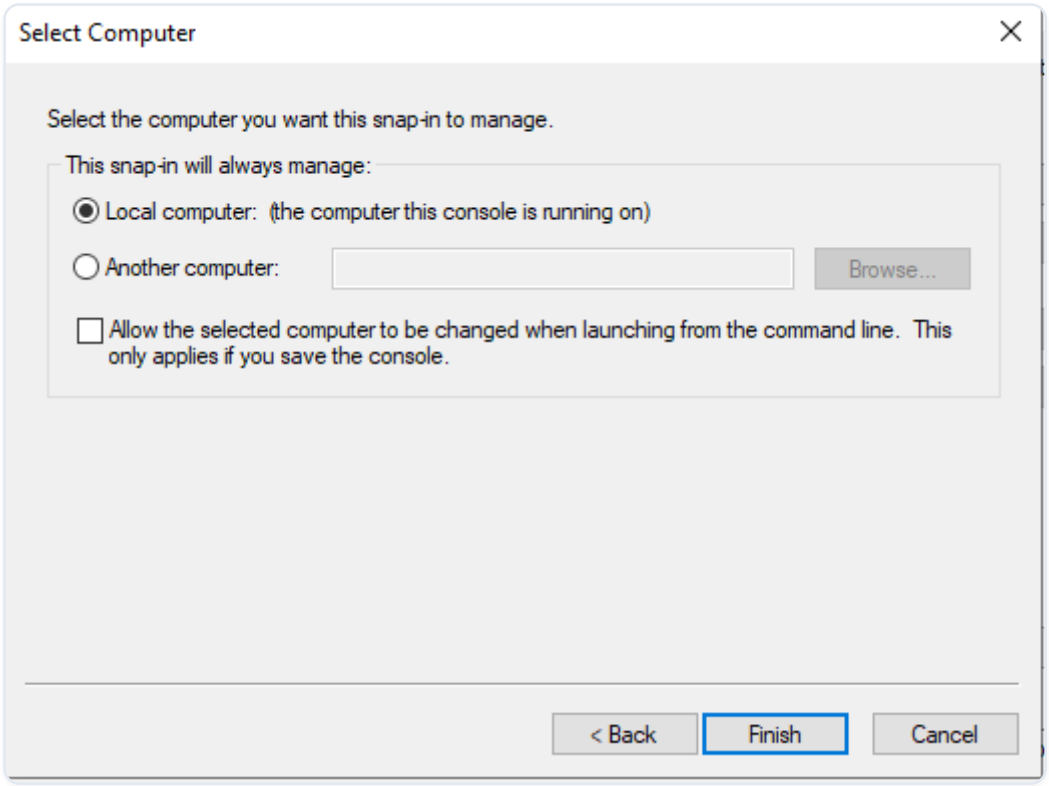
2. No menu **Arquivo**, clique em **Adicionar/Remover Snap-in**. A janela **Adicionar ou Remover Snap-ins** é exibida.



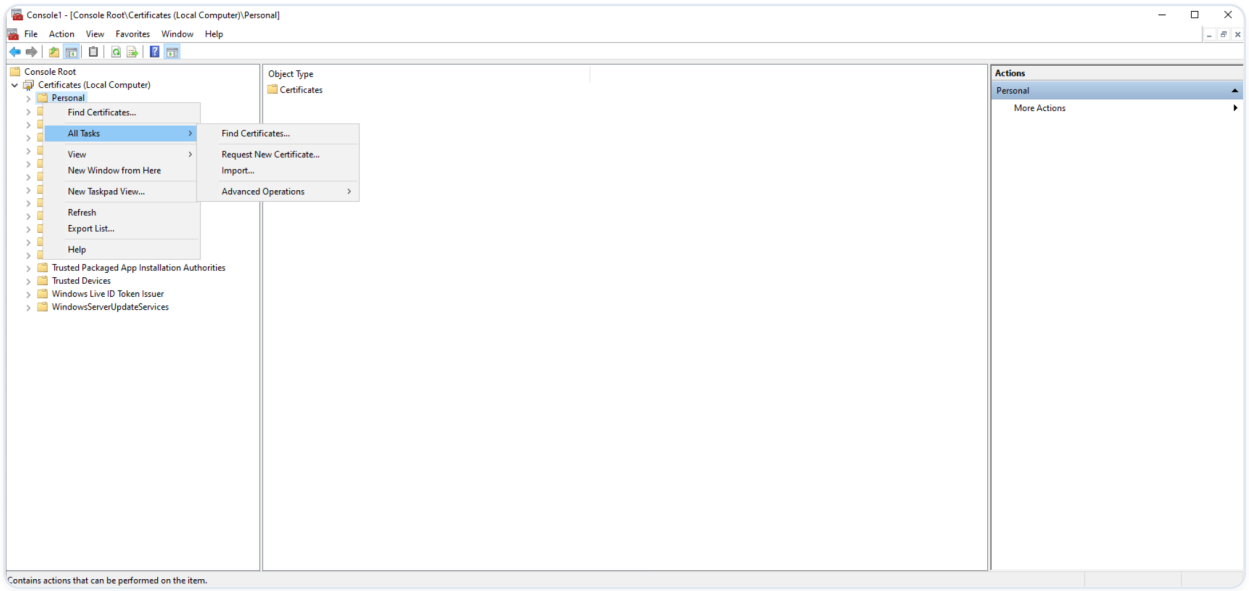
3. Em **Snap-in**, clique duas vezes em **Certificados**. A janela **Snap-in de Certificados** é exibida.



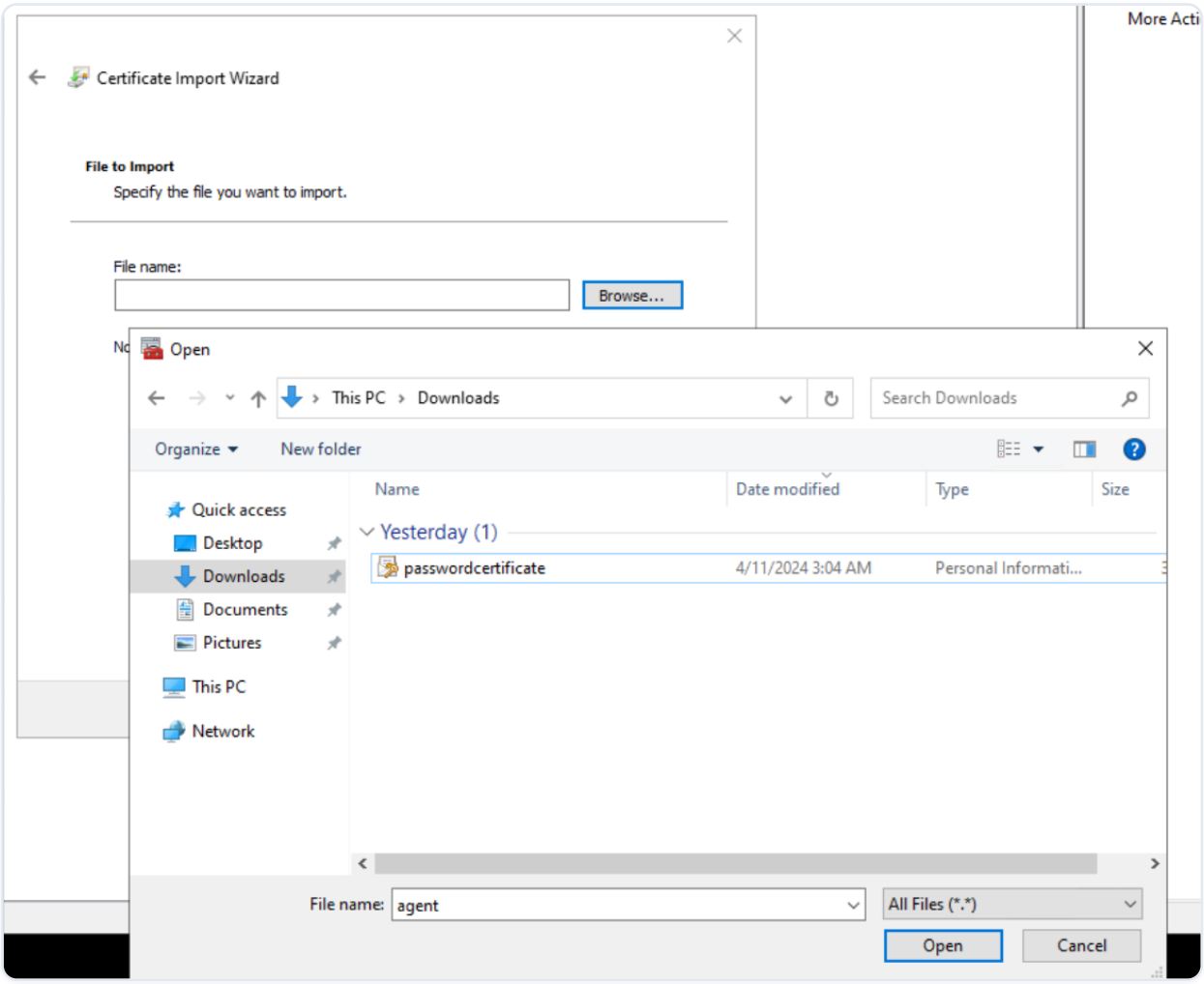
4. Selecione **Conta de computador** e clique em **Avançar**. A janela **Selecionar Computador** é exibida.



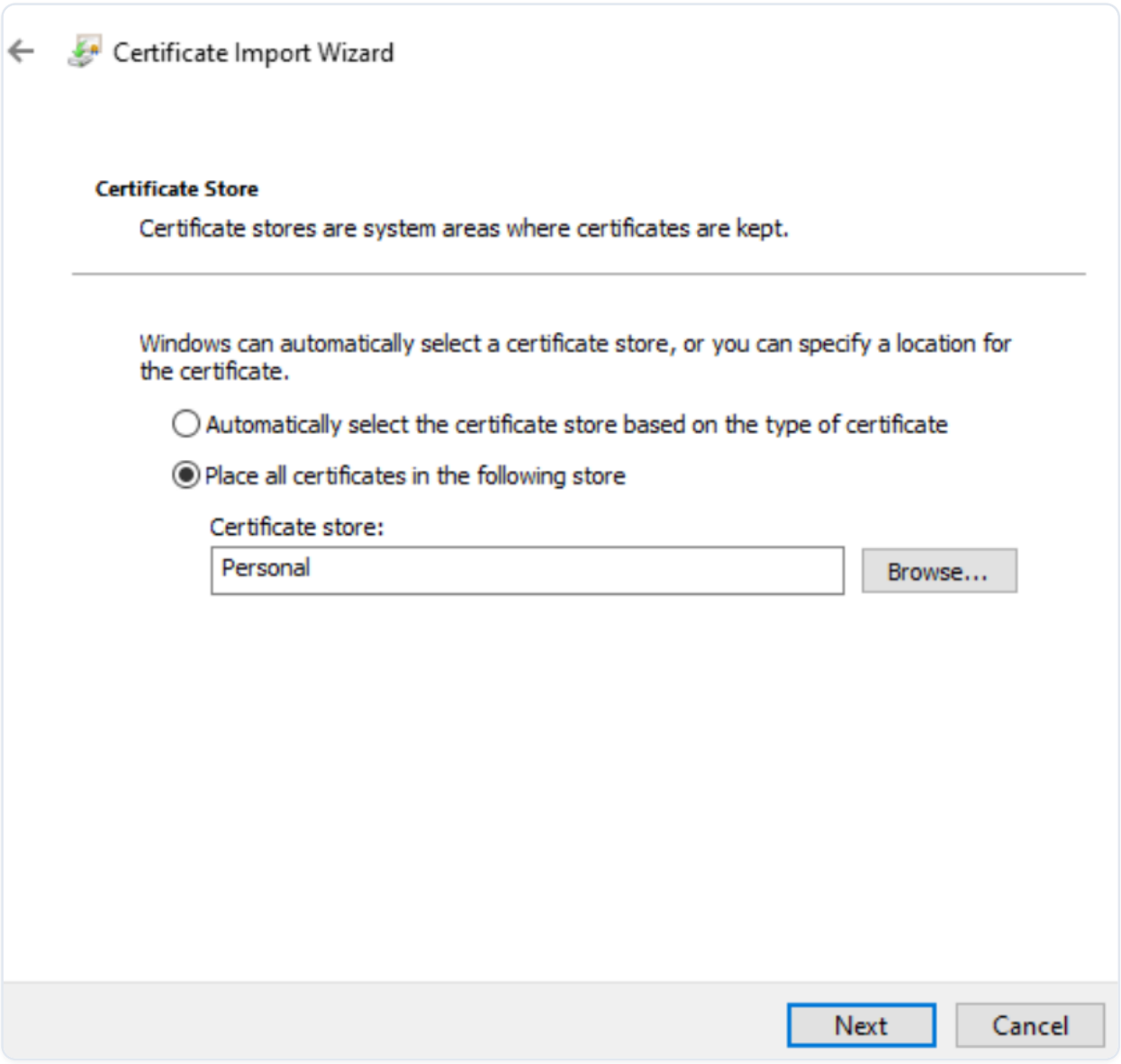
5. Selecione **Computador local**.
6. Clique em **Concluir**. A seção **Certificados (Computador Local)** aparece na lista de snap-ins selecionados para o novo console.
7. Clique em **OK**.
8. Expanda **Certificados**, clique com o botão direito em **Pessoal** > **Todas as Tarefas** > **Importar**. O **Assistente para Importação de Certificados** é exibido.



9. Selecione **Avançar** > **Procurar Arquivos**. navegar até o local onde você carregou o arquivo PFX, altere o tipo de arquivo para **Todos os arquivos** e, em seguida, selecione o certificado PFX respectivo.



10. Insira a senha PFX. Você pode deixá-lo em branco se não houver senha.
11. Clique em **Avançar**.
12. Para o Repositório de Certificados, certifique-se de que a opção **Colocar todos os certificados no seguinte repositório** esteja selecionada e que o **Repositório de certificados** esteja selecionado como **Pessoal**.



13. Clique em **Avançar**.
14. Revise os detalhes e clique em **Concluir**.
15. Aguarde a confirmação. A mensagem *A importação foi bem-sucedida* é exibida.
16. navegar para **Certificados** > **Pessoal** e certifique-se de que o certificado esteja presente.
17. Exclua o arquivo de certificado PFX da máquina.

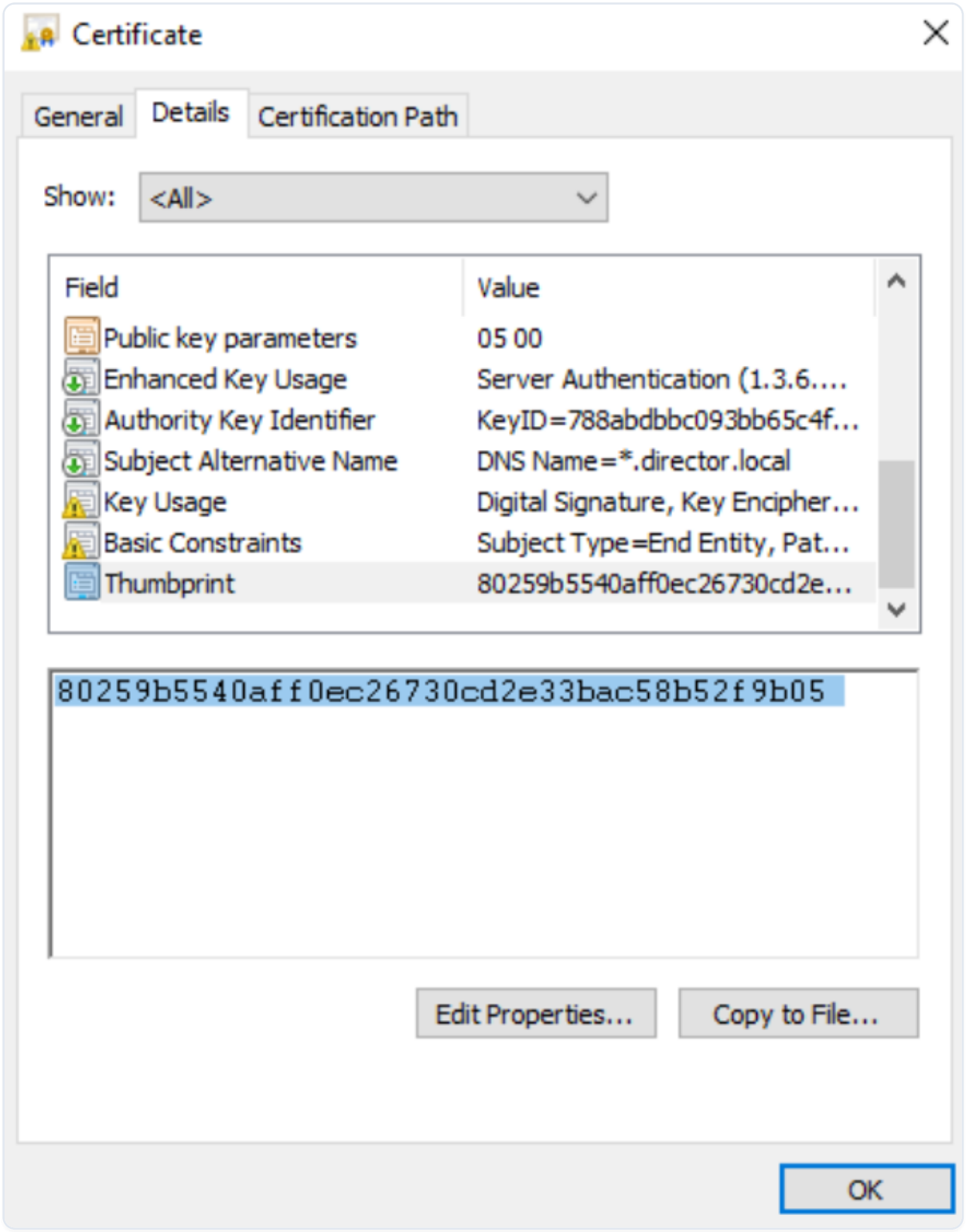
Passo 2.3: Fornecer acesso de leitura ao certificado

1. Clique com o botão direito do mouse no certificado importado > **Todas as Tarefas** > **Gerenciar Chaves Privadas**.
2. Na caixa de diálogo que se abre, selecione **Adicionar** e, em seguida, procure por **Serviço de Rede**. Clique em **OK**.
3. Selecione **NETWORK SERVICE** em **Grupo** ou **nomes de usuário**.

4. Permita o acesso de *Leitura* em **Permissões para NETWORK SERVICE**.
5. Clique em **OK**.

Passo 2.4: Obter o Thumbprint

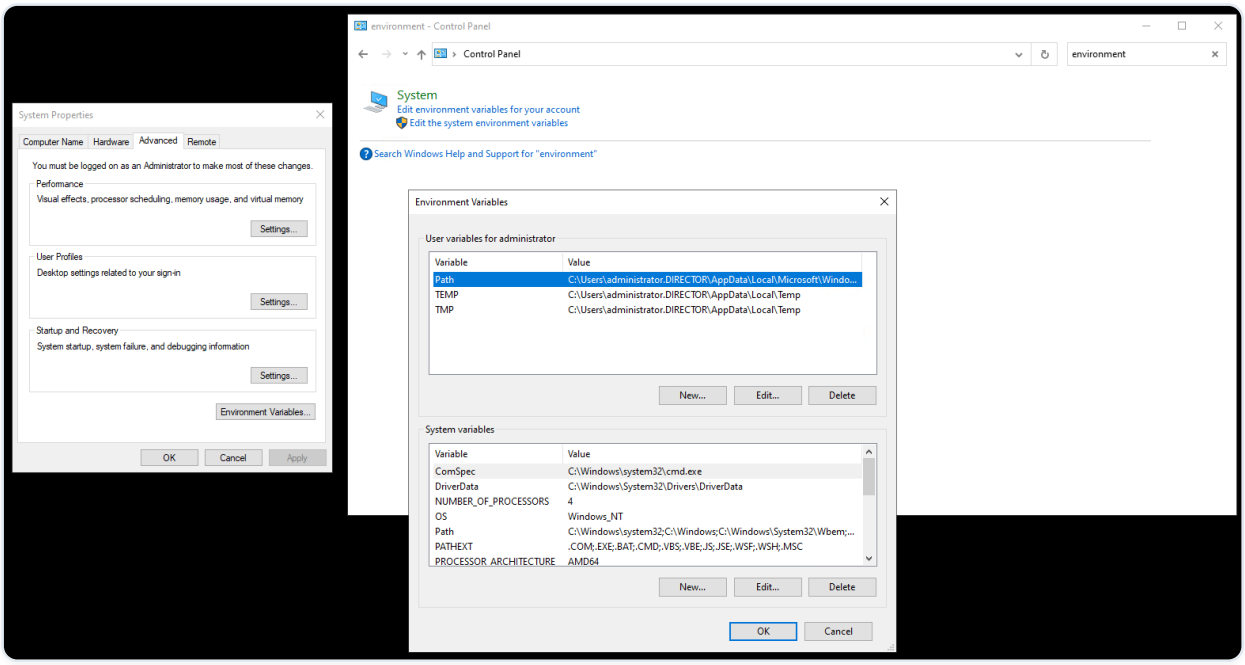
1. Clique duas vezes no certificado importado.
2. Na caixa de diálogo que se abre, navegar para a guia **Detalhes** e role até o final.
3. Clique em **Impressão digital**.



4. Copie o valor e o mantenha pronto para a próxima etapa.

Passo 2.5: Definir a variável de ambiente

1. Abra o Painel de Controle.
2. Pesquise por ambiente e selecione **Editar as variáveis de ambiente do sistema**.
3. Em **Variáveis do Sistema (para todos os usuários)**, clique em **Novo**.



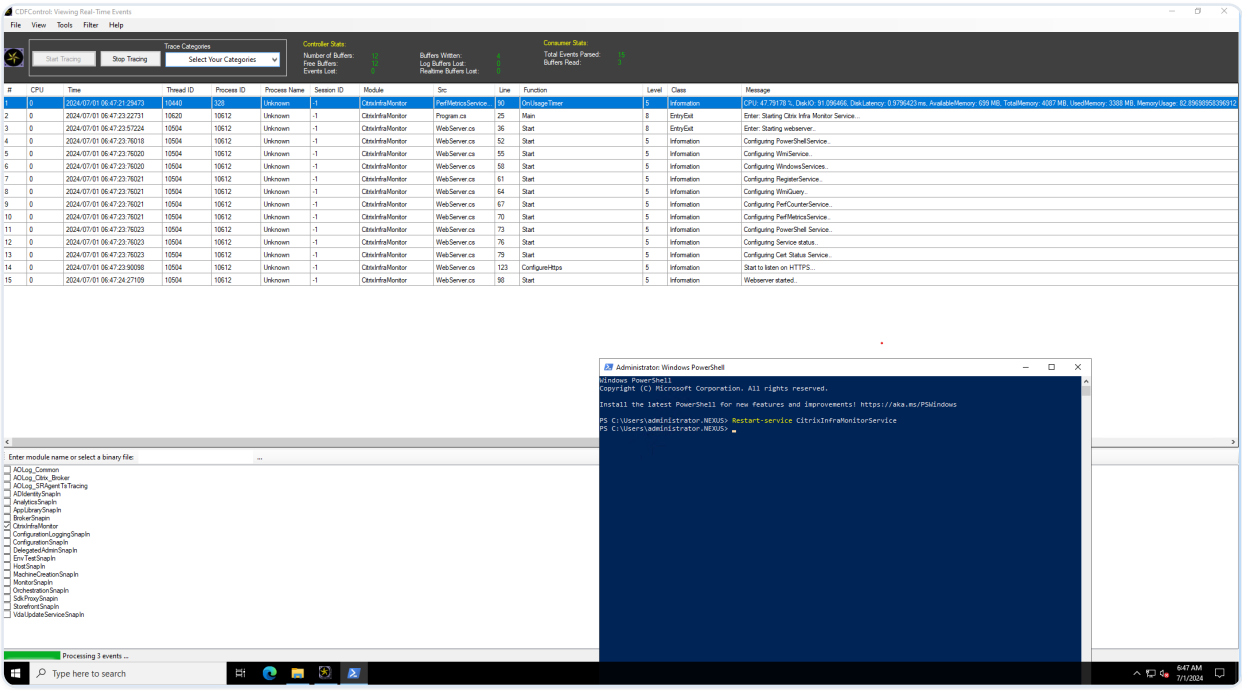
4. Especifique o nome da **Variável** como *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*.
5. Especifique a impressão digital da etapa anterior em valor da **Variável**.
6. Clique em **OK**.

Passo 2.6: Reiniciar o CitrixInfraMonitorService

1. Abra o PowerShell e execute o seguinte comando:

```
Restart-Service CitrixInfraMonitorService
```

2. Certifique-se de que o HTTPS esteja habilitado capturando o módulo **CitrixInfraMonitorService** e procurando pela linha de log **Start to listen on HTTPS...**.



Passo 2.7: Habilitar HTTPs na configuração do Monitor

Execute o seguinte comando em uma máquina DDC:

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

Passo 3: Registrar o Citrix Infrastructure Monitor

Pré-requisito:

- Certifique-se de que o Citrix Infrastructure Monitor esteja instalado na máquina StoreFront ou PVS.

Registre o Citrix Infrastructure Monitor no DDC para se comunicar com a máquina PVS ou StoreFront. Este registro serve para enviar as métricas de saúde da infraestrutura coletadas na máquina PVS ou StoreFront para o DDC.

Execute o seguinte comando PowerShell no Delivery Controller™ para registrar o Citrix Infrastructure Monitor:

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

Observação:

O nome de usuário e a senha são parâmetros opcionais. No entanto, se você não fornecer esses parâmetros, algumas das métricas não estarão disponíveis para você.

Os parâmetros do comando anterior são os seguintes:

PARÂMETRO	DESCRIÇÃO
`Fqdn`	FQDN do servidor PVS ou StoreFront.
`Component`	O componente que você está integrando. Por exemplo: PVS ou SF. PVS significa Citrix Provisioning e SF significa StoreFront.
`Domain`	O domínio do qual todos os componentes fazem parte.
`Username`	Nome de usuário do administrador.
`Password`	Senha do usuário administrador.
`Token`	Obtenha o token do Citrix Infrastructure Monitor do arquivo `RegistrationToken.txt` em `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` no sistema onde o Citrix Infrastructure Monitor está instalado.

Observação:

- O texto do token presente no arquivo `RegistrationToken.txt` é regenerado quando você reinicia o serviço Citrix Infrastructure Monitor. Após o registro ser bem-sucedido, o arquivo de token é excluído da máquina. Se você precisar registrar novamente, reinicie o serviço Citrix Infrastructure Monitor.
- Por motivos de segurança, o arquivo de token é removido após três tentativas de registro falhas com um token inválido.

Depois de registrar com sucesso a máquina PVS ou StoreFront, os detalhes do nome da máquina aparecem na guia **Director** > **Infraestrutura**.

Um exemplo de comando para se registrar no Citrix Infrastructure Monitor é o seguinte:

```
Add-MonitorDirectorAgent -Component PVS -Fqdn NX-PVS-
-Domain  -Username  -Password  -Token
```

Cancelar o registro de um componente

Caso precise cancelar o registro de um determinado componente, execute o seguinte comando PowerShell no Delivery Controller:

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Um exemplo de comando para remover o registro do Citrix Infrastructure Monitor é o seguinte:

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn
```

Observação:

O cancelamento do registro de um componente apenas interrompe o fluxo de dados do componente específico para o Director. Se precisar desinstalar o Citrix Infrastructure Monitor, desinstale-o do Painel de Controle.

Painel de Infraestrutura

Você pode ver os valores de integridade dos seus componentes na página **Monitoramento de Infraestrutura**. Esses resultados ajudam a analisar e solucionar problemas proativamente relacionados à sua infraestrutura.

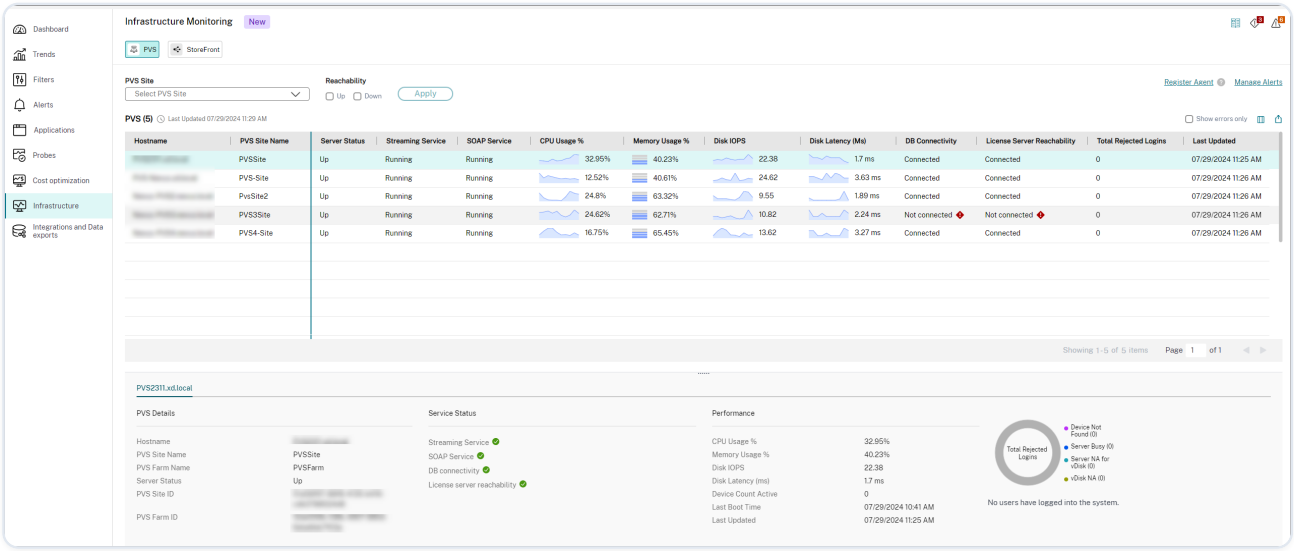
Você pode filtrar a página **Monitoramento de Infraestrutura** por:

- Nome do host - Selecione o nome do host
- Acessibilidade - Selecione a caixa de seleção **Ativo** (servidor acessível) ou **Inativo** (servidor não acessível)
- Erros - Selecione a caixa de seleção Mostrar linhas com erros apenas.

Use a opção **Gerenciar colunas** para escolher os dados a serem exibidos no seu painel.

Métricas de saúde do PVS

Clique na guia **Infraestrutura** e selecione **PVS**. O painel de Infraestrutura para PVS é exibido:



Os seguintes detalhes são monitorados para servidores PVS:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Nome do host	O nome da máquina PVS onde o Citrix Infrastructure Monitor está instalado. Esta métrica é um valor de string.
	Nome do Site PVS	O nome do site PVS. Esta métrica é um valor de string.
	Nome da Farm PVS	O nome da farm PVS. Esta métrica é um valor de string.
	ID do Site PVS	Exibe o ID do site do servidor PVS. Esta métrica é um valor de string.
	ID da Farm PVS	Exibe o ID do farm do servidor PVS. Esta métrica é um valor de string.
	Status do Servidor	Mostra o estado de acessibilidade do servidor fornecido. Os valores

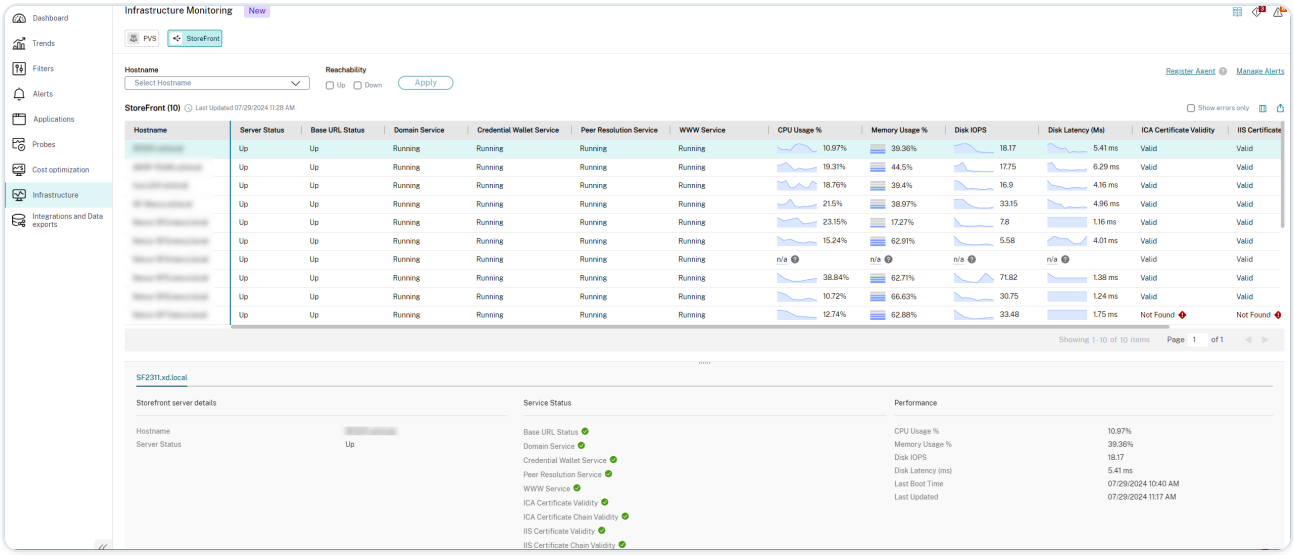
CATEGORIA	MÉTRICAS	DESCRIÇÃO
		possíveis são *Up*, *Down* e *Unknown*.
	Última Inicialização	Exibe a hora em que o servidor PVS foi inicializado pela última vez.
	Última atualização	Exibe a hora em que os dados foram coletados do servidor PVS.
Serviços Dependentes	Serviço de Streaming	Exibe o status do serviço de streaming. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Not running*, *Running*, *Not Installed* e *n/a* (com ícone de ajuda).
	Serviço SOAP	Exibe o status do serviço Simple Object Access Protocol (SOAP). Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Not running*, *Running*, *Not Installed* e *n/a* (com ícone de ajuda).
	Conectividade do BD	Exibe o status da conectividade do banco de dados. Se você estiver usando um servidor Citrix Provisioning versão 2402 ou anterior, poderá receber um erro desconhecido. Os valores possíveis são *Não Conectado*, *Conectado*, *Desconhecido* e *n/a* (com ícone de ajuda).

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Acessibilidade do Servidor de Licenças	Exibe se o servidor de licenças está acessível ou não. Se você estiver usando o servidor Citrix Provisioning versão 2402 ou anterior, poderá receber um erro desconhecido. Os valores possíveis são *Não Conectado*, *Conectado*, *Desconhecido* e *n/a* (com ícone de ajuda).
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	CPU Média %	Exibe a porcentagem média de CPU do servidor PVS agregada nos últimos 10 minutos.
	Pico de CPU %	Exibe a porcentagem máxima de CPU do servidor PVS nos últimos 5 minutos.
	Uso de Memória %	Exibe o uso de memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Memória %	Exibe a porcentagem média de memória do servidor PVS agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem máxima de memória do servidor PVS nos últimos 5 minutos.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	IOPS de Disco	Exibe o valor de entrada e saída do disco usando um gráfico de linha.
	Média de IOPS de Disco %	Exibe o IOPS médio do disco do servidor PVS agregado nos últimos 10 minutos.
	Pico de IOPS de Disco %	Exibe a porcentagem máxima de IOPS do disco do servidor PVS nos últimos 10 minutos.
	Latência do Disco (Ms)	Exibe o valor da latência do disco usando um gráfico de linha.
	Latência Média do Disco %	Exibe a latência média do disco do servidor PVS agregada nos últimos 10 minutos.
	Pico de Latência do Disco %	Exibe a porcentagem máxima de latência do disco do servidor PVS nos últimos 5 minutos.
Impacto	Total de Logins Rejeitados	Número total de falhas de login dividido pelo número total de tentativas de login.
	Contagem de Dispositivos Ativos	Exibe o número total de dispositivos ativos no servidor PVS. Esta métrica é um valor inteiro.

Métricas de saúde do StoreFront

Clique na guia **Infraestrutura** e selecione **StoreFront**. O painel de Infraestrutura para StoreFront é exibido:



Os seguintes detalhes são monitorados para servidores StoreFront:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Nome do host	Exibe o nome do servidor StoreFront. Esta métrica é um valor de string.
	Status do Servidor	Exibe o status do servidor StoreFront. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/d* (com ícone de ajuda).
	Status da URL Base	Exibe a integridade da URL base. Se o código de status HTTP for 200, o status é UP. Caso contrário, o valor é Down.
	Última Inicialização	Exibe a hora em que o servidor StoreFront foi inicializado pela última vez.
	Última atualização	Exibe a hora em que os dados foram coletados do servidor StoreFront.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Serviços Dependentes	Serviço de Domínio	Integridade do serviço do Windows denominado serviço de domínio. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/a* (com ícone de ajuda).
	Serviço de Carteira de Credenciais	Este serviço é um serviço do Windows usado para armazenar senhas criptografadas. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/a* (com ícone de ajuda).
	Serviço de Resolução de Pares	Este serviço é um serviço do Windows responsável pela comunicação de rede entre grupos de servidores, formando uma malha de pares de servidores StoreFront. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/d* (com ícone de ajuda).
	Serviço WWW	Esta métrica é o serviço web do servidor StoreFront. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/d* (com ícone de ajuda).

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos cinco minutos.
	CPU Média %	Exibe a porcentagem média da CPU do servidor StoreFront agregada nos últimos 10 minutos.
	Pico de CPU %	Exibe a porcentagem de pico da CPU do servidor StoreFront nos últimos cinco minutos. Este valor ajuda a decidir a capacidade máxima necessária para uma CPU.
	Uso de Memória %	Exibe o uso de memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Memória %	Exibe a porcentagem média de memória do servidor StoreFront agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem de pico de memória do servidor StoreFront nos últimos 5 minutos.
	IOPS de Disco	Exibe o valor de entrada e saída do disco usando um gráfico de linha.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Média de IOPS de Disco %	Exibe a média de IOPS de disco do servidor StoreFront usando um valor flutuante.
	Pico de IOPS de Disco %	Exibe a porcentagem de pico de IOPS de disco do servidor StoreFront agregada nos últimos 10 minutos.
	Latência do Disco (Ms)	Exibe o valor da latência do disco usando um gráfico de linha.
	Latência Média do Disco %	Exibe a latência média do disco do servidor StoreFront agregada nos últimos 10 minutos.
	Pico de Latência do Disco %	Exibe a porcentagem de pico de latência do disco do servidor StoreFront nos últimos cinco minutos.
Impacto	Validade do Certificado ICA®	Exibe a validade do certificado ICA. Os valores possíveis são *Expirado*, *Expirando*, *Válido* e *Não Encontrado*.
	Validade da Cadeia de Certificados ICA	Exibe se a Cadeia de Certificados ICA do StoreFront é válida ou não. O valor possível é *Sim* ou *Não*.
	Validade do Certificado IIS	Exibe a validade do certificado IIS. Os valores possíveis são *Expirado*, *Expirando*, *Válido* e *Não Encontrado*.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Validade da Cadeia de Certificados IIS	Exibe se a Cadeia de Certificados IIS do StoreFront é válida ou não. O valor possível é *Sim* ou *Não*.

Criar e gerenciar alertas

Você pode configurar alertas para monitorar proativamente condições e escopos de seu interesse e reduzir a fadiga de alertas. Os alertas podem ser configurados com severidade, intervalos de re-alerta, meios de notificação e seguem o ciclo de vida do alerta suportado no produto.

Para obter mais informações, consulte a página Alertas.

Sondagem de Aplicativos e Desktops

A sondagem de aplicativos e desktops automatiza o processo de verificação da integridade dos aplicativos e desktops publicados em um site, iniciando-os sequencialmente usando o StoreFront. Os resultados da sondagem estão disponíveis no Director.

Requisitos

- O Delivery Controller executa a versão 7.18 ou posterior para sondagem de aplicativos e a versão 1906 ou posterior para sondagem de desktops.
- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com o aplicativo Citrix Workspace™ para Windows versão 1808 ou posterior para sondagem de aplicativos e versão 1906 ou posterior para sondagem de desktops. O aplicativo Workspace para Unified Windows Platform (UWP) não é compatível.
- O Citrix Probe Agent oferece suporte à autenticação via StoreFront e Citrix Workspace usando credenciais do Active Directory. Nos casos em que o dispositivo de endpoint está conectado ao StoreFront / Workspace via Citrix Gateway, você pode autenticar usando as credenciais de domínio do Citrix Gateway ou autenticação multifator (MFA). O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como Single Sign-On (SSO).

> **Nota:**

    - Se o usuário ativou a política de logon ou a autenticação condicional no Citrix Cloud™, o agente de sondagem falha ao fazer logon no Storefront ou no aplicativo Citrix Workspace.
    - O Probe Agent oferece suporte apenas à autenticação do Active Directory para autenticar no aplicativo Citrix Workspace.

- Certifique-se de que o Microsoft .NET Framework versão 4.7.2 ou posterior esteja instalado na máquina de endpoint onde você deseja instalar o Probe Agent.

Contas de usuário/permissões necessárias para executar a Sondagem:

- Um usuário StoreFront exclusivo para sondar em cada máquina de endpoint. O usuário StoreFront não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint
- Reutilizar contas de usuário existentes para sondagem pode desconectar os usuários de suas sessões ativas. Uma conta de usuário administrador completa ou uma função personalizada com as seguintes permissões:
    - Permissões de grupo de entrega:
        - Somente leitura
    - Permissões do Director:
        - Criar\\Editar\\Remover Configuração do Servidor de E-mail de Alerta - se o servidor de e-mail ainda não estiver configurado
        - Criar\\Editar\\Remover Configurações de Sondagem
        - Visualizar página de Configurações
        - Visualizar página de Tendências

Configuração

Você pode agendar suas sondagens para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados aos aplicativos, máquina de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 e posterior oferece suporte a agregação de sites. Ao configurar o Citrix Probe Agent, selecione a opção Workspace (StoreFront) Site Aggregation Enabled para habilitar a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

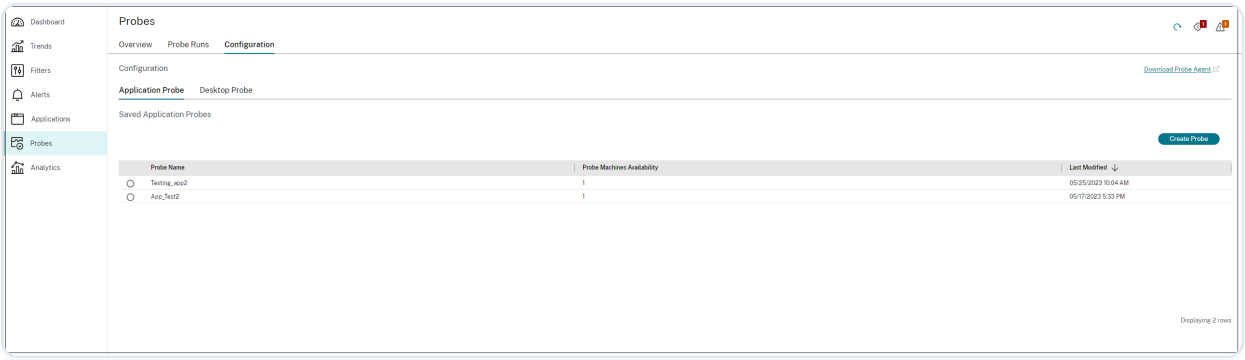
- Vários sites locais com uma URL do StoreFront.
- Sites locais e na nuvem com uma URL do StoreFront ou Workspace.
- Vários sites na nuvem com uma URL do Workspace.
- Sites locais conectados ao StoreFront ou Workspace via Citrix Gateway.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar sondas que tenham acesso a apenas um site.

Etapa 1: Instalar e configurar o Citrix Probe Agent

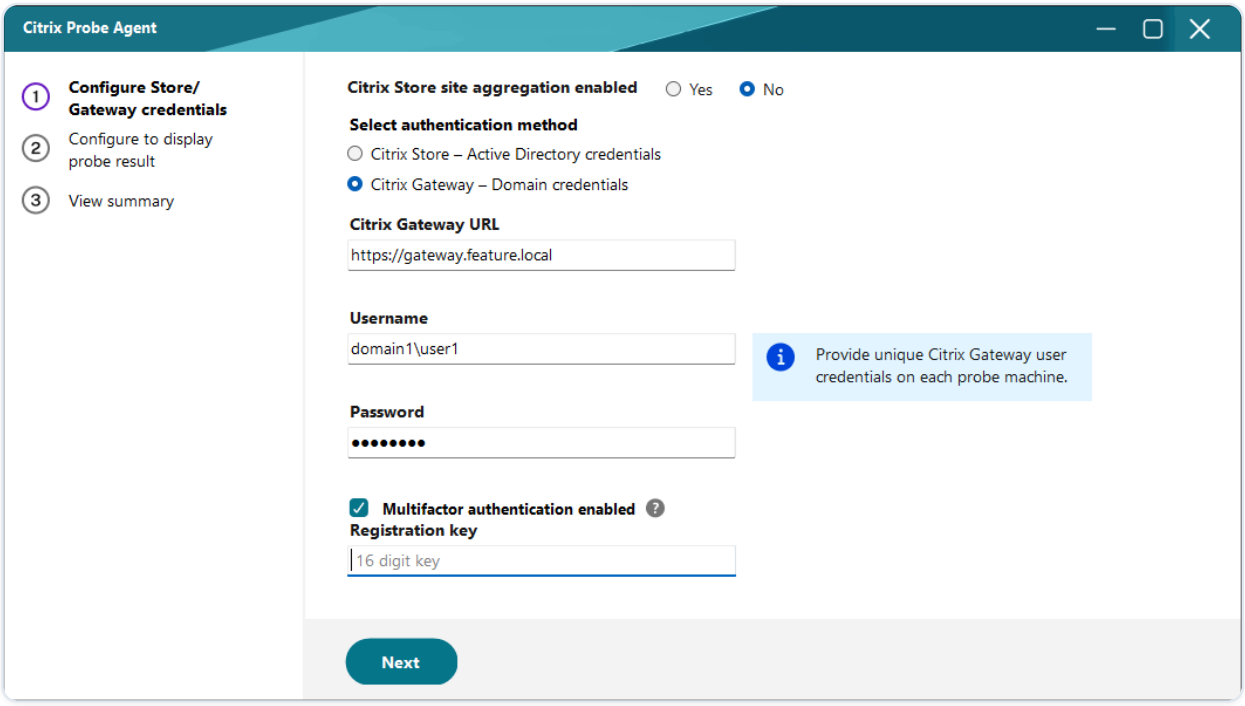
O Citrix Probe Agent é um executável do Windows que simula o lançamento real de um aplicativo ou desktop pelo usuário através do StoreFront. Ele testa os lançamentos conforme configurado no Director e reporta os resultados de volta ao Director.

1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`. O link para download também está disponível na guia **Probes** no Director.

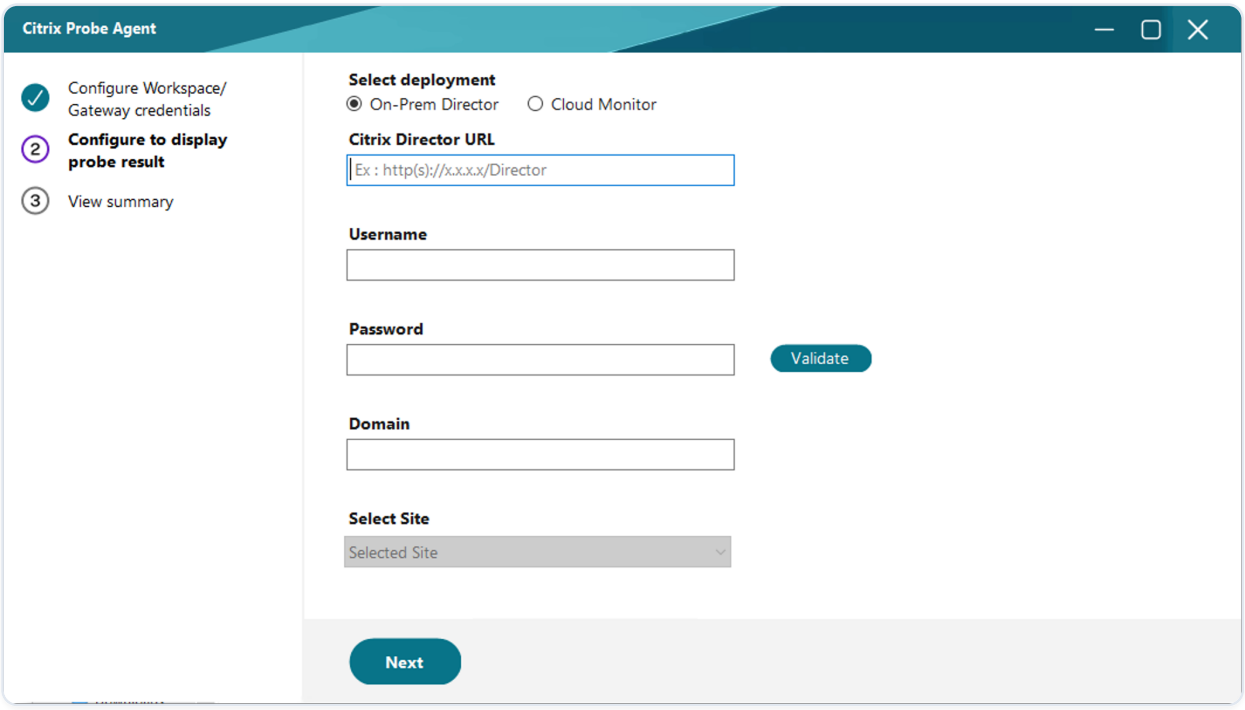


.

3. Se você tiver sites agregados, selecione a opção Workspace (StoreFront) Site Aggregation Enabled para habilitar a enumeração de aplicativos e desktops de sites agregados.
4. Selecione um método de autenticação e insira as credenciais relevantes. As credenciais são criptografadas e armazenadas com segurança.
5. Configure com suas credenciais do Active Directory do StoreFront. Configure um usuário exclusivo do Workspace (StoreFront) em cada máquina de endpoint.
6. Escolha a opção Citrix Gateway se seu endpoint estiver conectado ao StoreFront via Citrix Gateway e configure com suas credenciais de Domínio do Citrix Gateway.



7. Escolha a opção de Autenticação Multifator se o seu Gateway a suportar e insira a chave de autenticação de 16 dígitos. Isso está disponível apenas para o Citrix Gateway configurado com LDAP e OTP Nativo usando o Esquema de Login Único.
8. Na guia **Configurar para Exibir Resultado da Sondagem**, insira suas credenciais do Director e clique em **Validar**.



9. Selecione seu site e clique em **Avançar**.
10. Na guia **Visualizar Resumo**, certifique-se de que os detalhes configurados estejam precisos. Se precisar fazer alterações, vá para a guia respectiva e faça as atualizações.

> **Observação:**

> Você pode usar o script PowerShell contido em Automatizando a Instalação e Configuração do Agente de Sondagem Citrix para automatizar a instalação e configuração do Agente de Sondagem Citrix.

Etapa 2: Configurar a Sondagem no Director

> **Limitação:**

> A sondagem falha se aplicativos ou desktops forem iniciados para teste a partir de VDAs Windows que têm o banner de mensagem de logon interativo ativado. Isso ocorre porque um tempo limite é atingido devido à espera para aceitar a mensagem de logon interativo. Para desativar a mensagem de logon em um VDA de Servidor. Vá para Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança.

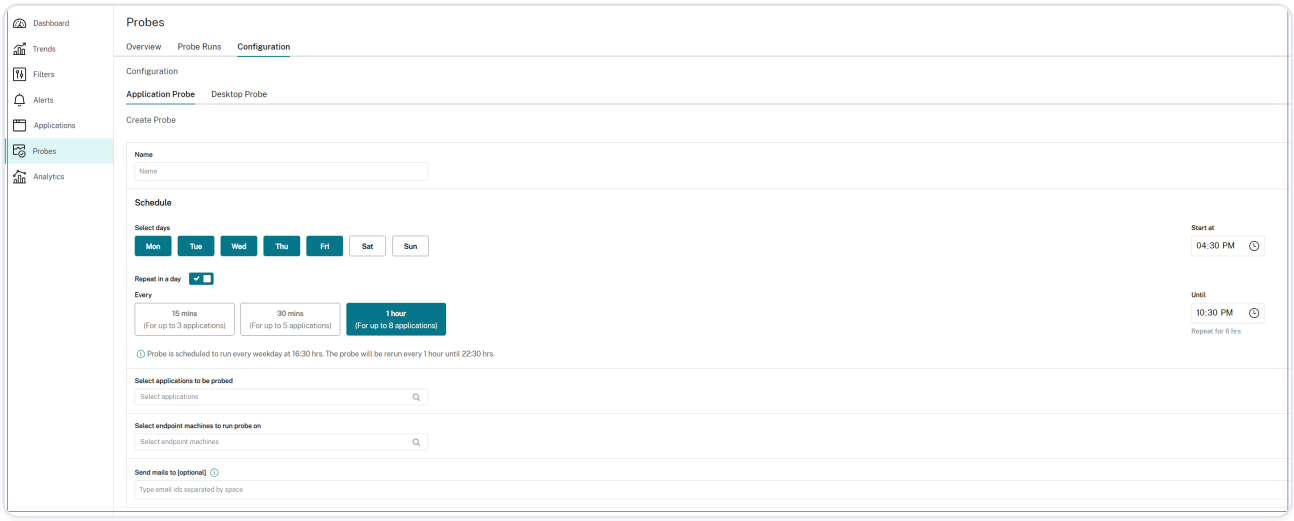
Remova o texto nos seguintes campos e atualize a política da Microsoft.

- Logon Interativo: Texto da Mensagem para usuários tentando fazer logon
- Logon Interativo: Título da Mensagem para usuários tentando fazer logon

Atribua o usuário da sondagem a este VDA de Servidor específico com o banner de mensagem de logon interativo desabilitado para garantir que a sondagem possa passar do estado de Inicialização de Aplicativo ou Área de Trabalho.

Para obter mais informações, consulte `<https://learn.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`.

1. Vá para **Sondagens** \> **Sondagem de Aplicativo** ou **Sondagem de Área de Trabalho** e clique em **Criar Sondagem**.
2. Na página **Criar Sondagem**, insira o nome da sondagem.
3. Selecione o agendamento:
    a. Escolha os dias da semana em que você deseja que a sondagem seja executada.
    b. Insira a hora de início em que você deseja que a sondagem seja executada.
    c. Além disso, você pode escolher a opção **Repetir em um dia**. Insira a hora de término e o intervalo em que você deseja que a sondagem se repita dentro de um dia. Por exemplo, a configuração abaixo ajuda a executar sondagens de aplicativos das 12:08 horas até as 16:34 horas, repetindo a cada 30 minutos todas as segundas, quartas, quintas e domingos.
4. Selecione o número recomendado de aplicativos ou desktops a serem sondados, dependendo do intervalo.
5. Selecione as máquinas de endpoint nas quais a sondagem deve ser executada.
6. Insira os endereços de e-mail dos administradores para enviar os resultados das sondagens com falha. Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.



Nesta configuração, as sessões do aplicativo são iniciadas às 12:08, 12:38, 13:08 e assim por diante até as 16:08, todas as segundas, quartas, quintas e domingos.

Observação:

- Após a configuração, o agente executa as sondagens configuradas a partir da próxima hora.
- As sondagens que foram configuradas antes da introdução da opção **Repetir em um dia** continuam a ser executadas no horário agendado. Elas têm a opção **Repetir em um dia** desativada por padrão.
- Recomenda-se que você configure as sondagens de forma que cada execução tenha um período de 5 minutos para evitar sobreposições.

Etapa 3: Execução da sondagem

O agente executa a sondagem de acordo com a configuração de sondagem que ele busca do Director periodicamente.

Ele inicia os aplicativos selecionados serialmente usando o StoreFront. O agente reporta os resultados de volta ao Director via banco de dados do Monitor. As falhas são reportadas em cinco estágios específicos:

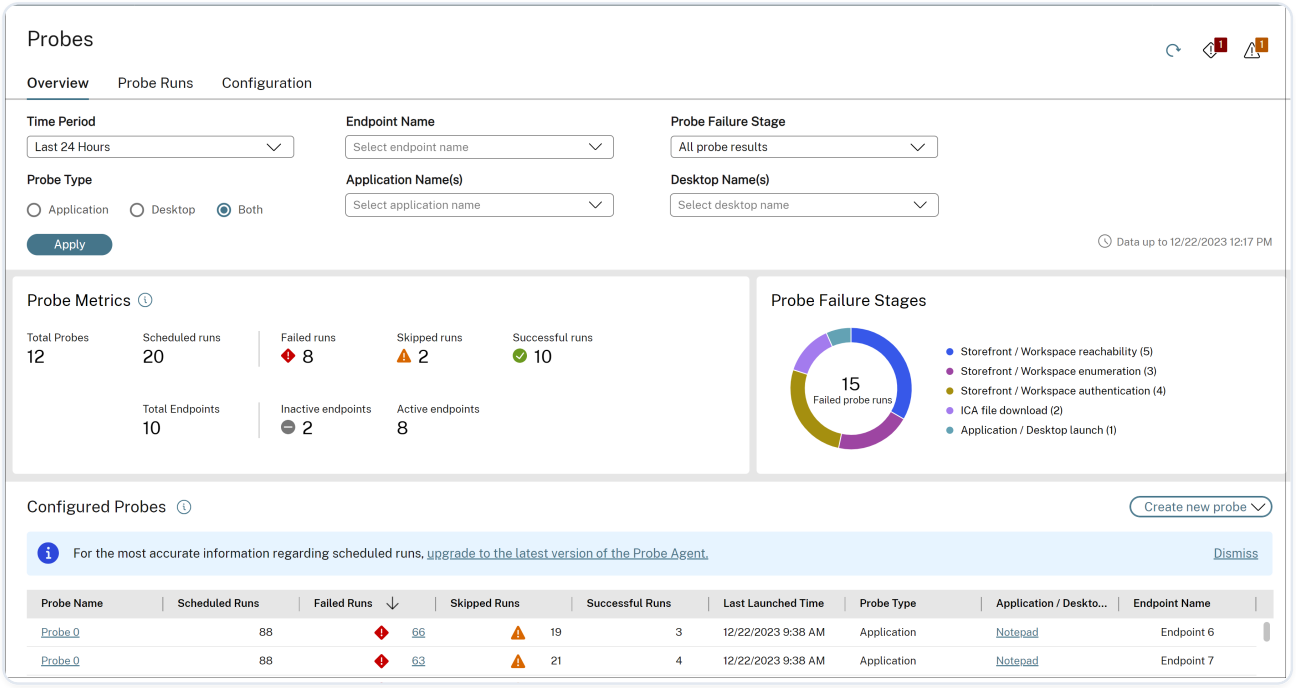
- **Acessibilidade do StoreFront** - a URL do StoreFront configurada não está acessível.
- **Autenticação do StoreFront** - as credenciais do StoreFront configuradas são inválidas.
- **Enumeração do StoreFront** - a lista de aplicativos enumerados do StoreFront não contém o aplicativo ou área de trabalho a ser sondado.

- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização de Aplicativo / Desktop** – o aplicativo ou desktop não pôde ser iniciado.

Etapa 4: Visualizar resultados da sonda

Você pode ver os resultados da sonda em **Sondas**. A visualização Sondas oferece uma visão abrangente dos resultados da sonda. Esses resultados ajudam a analisar e solucionar problemas proativamente, permitindo uma experiência de inicialização de sessão mais suave para os usuários.

A guia **Visão Geral** fornece um resumo de todas as sondas configuradas em uma única visualização.



Você pode filtrar sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Tipo de Resultado da Sonda. As sondas que correspondem aos critérios de filtro são mostradas com os seguintes detalhes por sonda, aplicativo/desktop e endpoint.

Métricas da Sonda mostra a contagem de execuções Agendadas, Planejadas, Ignoradas, Bem-sucedidas e Falhas.

- Execuções Concluídas – o número de execuções da sonda que foram concluídas.
- Execuções com Falha – o número de execuções da sonda que falharam.
- Execuções Ignoradas – o número de execuções que não foram concluídas devido ao endpoint estar inativo ou aos serviços estarem indisponíveis.

- Execuções Bem-sucedidas – o número de sondas que foram concluídas com sucesso, sem falhas em nenhuma etapa durante o lançamento do aplicativo/desktop.

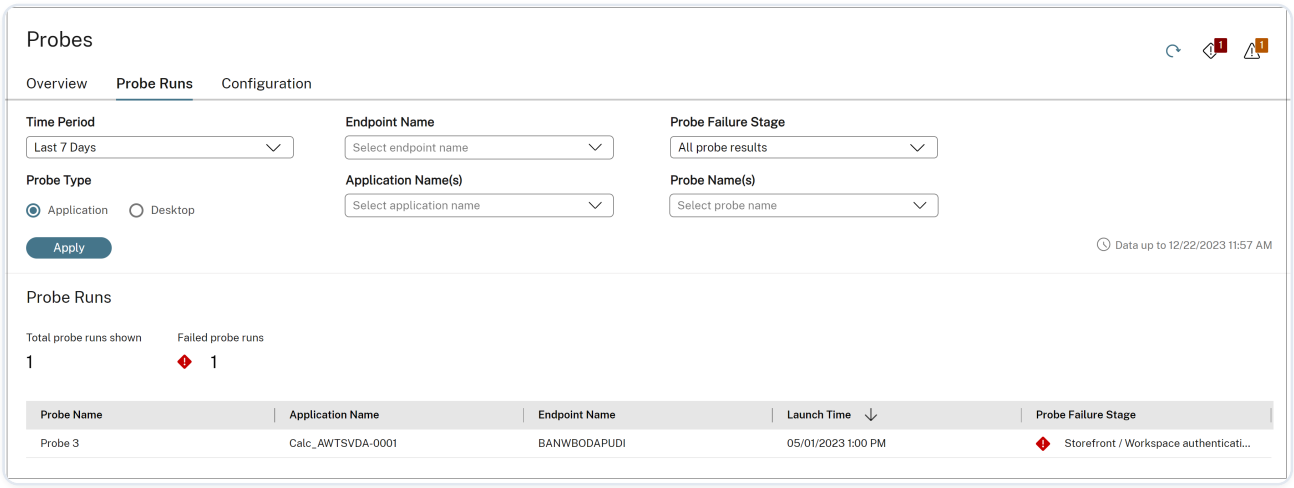
O número total de máquinas de endpoint também é exibido, com a contagem de máquinas ativas e inativas.

Estágios de Falha da Sonda apresenta uma análise visual da distribuição de falhas para cada grupo de falhas. Ao analisar os estágios em que a maioria das falhas ocorreu, torna-se mais fácil interpretar os resultados da sonda e solucionar problemas. A representação gráfica mostra o número de execuções de sonda com falha para o lançamento de aplicativo/desktop, downloads de arquivos ICA, enumeração do Storefront/Workspace, acessibilidade do Storefront/Workspace e autenticação do Storefront/Workspace.

Ajuda a analisar os estágios em que a maioria das falhas ocorreu. Essas informações ajudam a entender rapidamente os resultados da sonda e a solucionar problemas.

Algumas execuções de sonda podem não ser concluídas devido ao endpoint estar inativo ou aos serviços estarem indisponíveis.

A guia **Execuções de Sonda** fornece os resultados das execuções de sonda concluídas em detalhes. Você pode detalhar para ver os detalhes de cada execução individual de uma sonda selecionada. Você pode filtrar e analisar ainda mais com base em pontos de pivô importantes.



Você pode filtrar as execuções de sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Estágio de Falha da Sonda. O Estágio de Falha da Sonda exibe o estágio em que a sonda falhou. Clicar nos links Nome da Sonda, Execuções Agendadas, Execuções com Falha, Nome do Aplicativo/Desktop também o leva à página Execuções de Sonda com a lista de execuções de sonda que correspondem aos critérios de filtro.

Otimização de custos

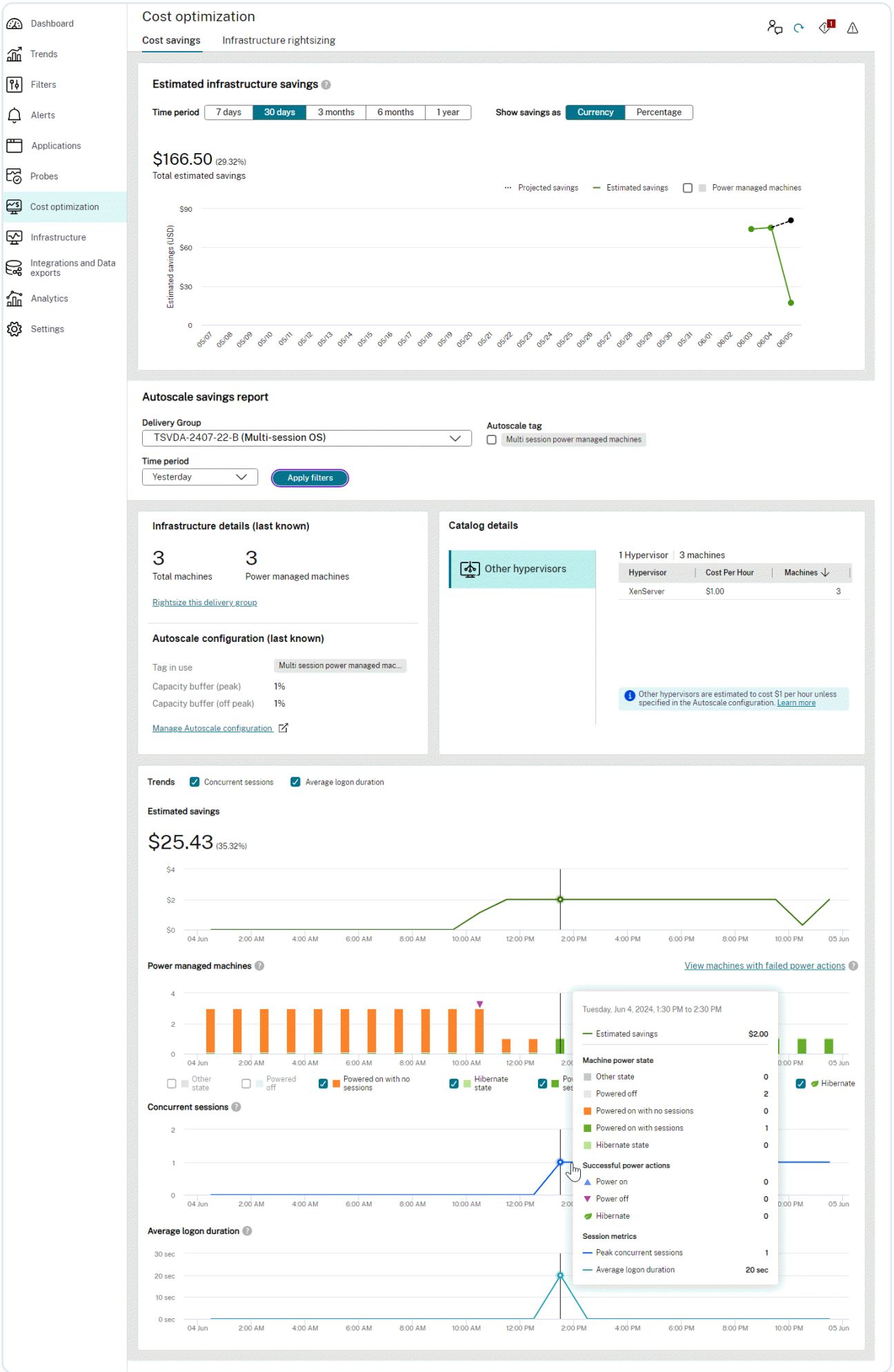
O Citrix Director agora apresenta um novo recurso chamado Otimização de Custos, que ajuda a analisar o uso de máquinas virtuais e sessões de forma eficaz. Este recurso fornece representações visuais perspicazes sobre como otimizar o custo. Também ajuda a eliminar máquinas desnecessárias e, assim, reduzir custos.

Para apoiar a otimização de custos, os seguintes alertas também foram introduzidos:

- Ação de ligar falhou e Ação de desligar falhou
- Alerta de tempo de atividade da máquina

Você também pode inspecionar máquinas com ações de energia recentes para analisar falhas de inicialização que causam problemas aos usuários e falhas de desligamento que aumentam os custos. Para obter mais informações, consulte a seção Inspecionar máquinas com ações de energia recentes.

Clique na guia **Otimização de Custos** no menu esquerdo da página **Início** para acessar a página **Otimização de Custos**.


Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and Data exports
Analytics
Settings
Cost optimization
Cost savings
Infrastructure rightsizing
Estimated infrastructure savings
Time period
7 days
30 days
3 months
6 months
1 year
Show savings as
Currency
Percentage
$166.50 (29.32%)
Total estimated savings
Projected savings
Estimated savings
Power managed machines
Estimated savings (USD)
$90
$60
$30
0
05/07
05/08
05/09
05/10
05/11
05/12
05/13
05/14
05/15
05/16
05/17
05/18
05/19
05/20
05/21
05/22
05/23
05/24
05/25
05/26
05/27
05/28
05/29
05/30
05/31
06/01
06/02
06/03
06/04
06/05
Autoscale savings report
Delivery Group
TSVDA-2407-22-B (Multi-session OS)
Autoscale tag
Multi session power managed machines
Time period
Yesterday
Apply filters
Infrastructure details (last known)
3
Total machines
3
Power managed machines
Rightsize this delivery group
Autoscale configuration (last known)
Tag in use
Multi session power managed mac...
Capacity buffer (peak)
1%
Capacity buffer (off peak)
1%
Manage Autoscale configuration
Catalog details
Other hypervisors
1 Hypervisor | 3 machines
Hypervisor
Cost Per Hour
Machines
XenServer
$1.00
3
Other hypervisors are estimated to cost $1 per hour unless specified in the Autoscale configuration. Learn more
Trends
Concurrent sessions
Average logon duration
Estimated savings
$25.43 (35.32%)
$4
$2
$0
04 Jun
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
05 Jun
Power managed machines
View machines with failed power actions
Other state
Powered off
Powered on with no sessions
Hibernate state
Hibernate
Tuesday, Jun 4, 2024, 1:30 PM to 2:30 PM
Estimated savings
$2.00
Machine power state
Other state
0
Powered off
2
Powered on with no sessions
0
Powered on with sessions
1
Hibernate state
0
Successful power actions
Power on
0
Power off
0
Hibernate
0
Session metrics
Peak concurrent sessions
1
Average logon duration
20 sec
Concurrent sessions
Average logon duration
30 sec
20 sec
10 sec
0 sec

Na página inicial de **Otimização de Custos**, você pode fazer o seguinte:

- Link de introdução - Acesse este link para saber mais sobre o recurso de otimização de custos.
- Revisar a página de otimização de custos - Você pode fornecer feedback sobre a página **Otimização de Custos**
- Atualizar os dados.
- Visualizar os alertas - Você pode visualizar alertas críticos e de aviso.

A página **Otimização de Custos** inclui os seguintes recursos:

- Economia de custos
- Dimensionamento correto da infraestrutura

Como o custo é calculado para otimizar o custo?

O custo por máquina por hora é exibido na moeda que o hipervisor suporta. Esta seção descreve como o custo é calculado para máquinas Azure e para outras máquinas.

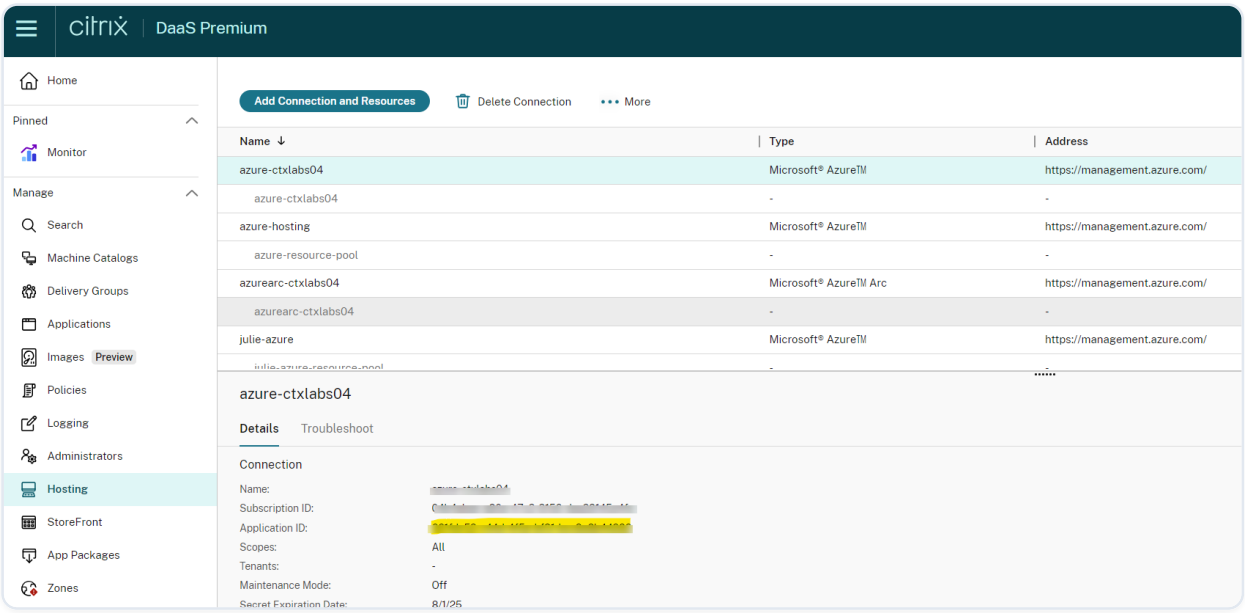
Custo para máquinas Azure

A ordem de prioridade para calcular o custo é a seguinte:

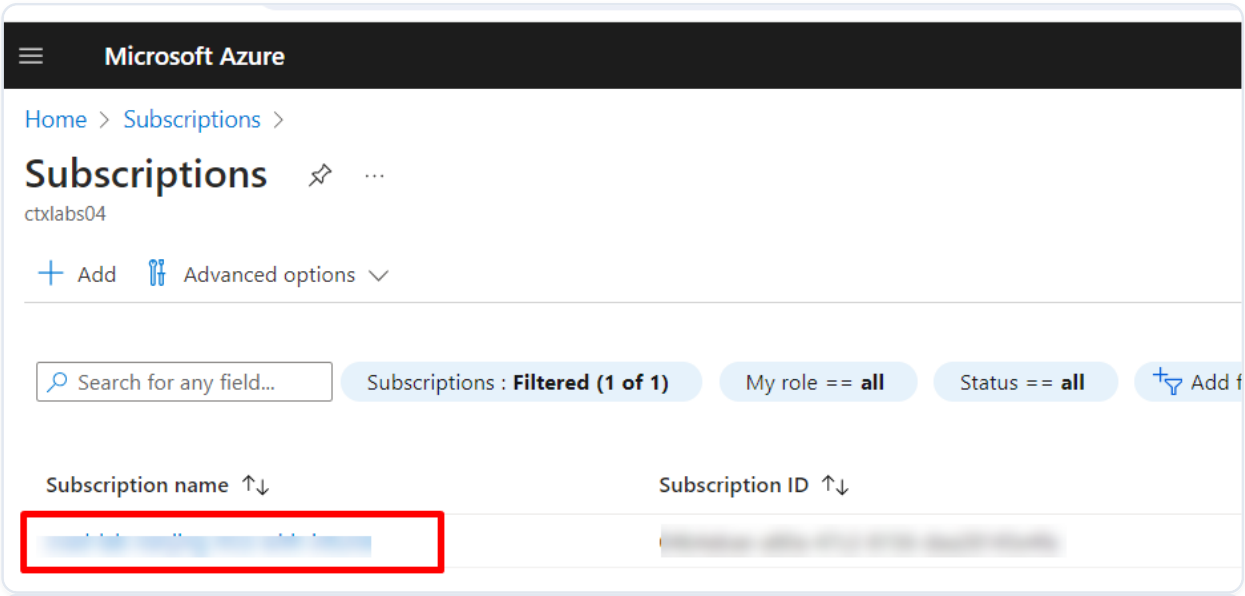
1. Quando a permissão 'Microsoft.Consumption/pricesheets/read estiver disponível, o preço efetivo é exibido na moeda configurada na assinatura do Azure.
2. Se as permissões não estiverem disponíveis, o preço de varejo do Azure será exibido. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure.
3. Quando o preço efetivo ou o preço de varejo não estiver disponível, o custo é exibido com base no custo inserido pelos administradores no Web Studio.
4. Se nenhum custo for mencionado no Web Studio, o custo padrão de $1 é considerado.

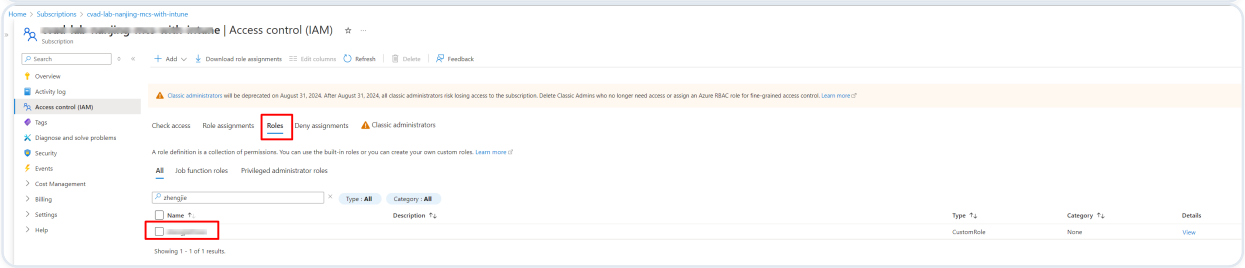
Para encontrar os detalhes da conta do Azure e adicionar a permissão necessária para encontrar o preço efetivo, faça o seguinte:

1. navegar para o Citrix DaaS.
2. Clique na guia **Hospedagem** para encontrar a conta de conexão de hospedagem.
3. Procure o **ID do Aplicativo** mencionado na guia **Hospedagem**.



4. Vá para o Azure AD e procure o **ID do Aplicativo** anotado na etapa 3.
5. Vá para **Assinatura** > **Controle de acesso (IAM)** > escolha uma função personalizada configurada para o SPN de conexão de hospedagem.





6. Adicione a permissão *Microsoft.Consumption/pricesheets/read* à função.

Como verificar o preço de varejo do Azure?

Se o `Microsoft.Consumption/pricesheets/read` não estiver disponível, o preço de varejo do Azure será exibido. Agora você pode usar a API de Preços de Varejo para obter preços de varejo

para todos os serviços do Azure. Anteriormente, a única maneira de recuperar preços para serviços do Azure era usar a Calculadora de Preços do Azure ou o portal do Azure. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure.

Calculando custos para máquinas que não sejam do Azure

Para outras máquinas, o custo é exibido com base no custo inserido pelos administradores no Web Studio. Se nenhum custo for mencionado no Web Studio, o custo padrão de $1 será considerado.

Economia de custos

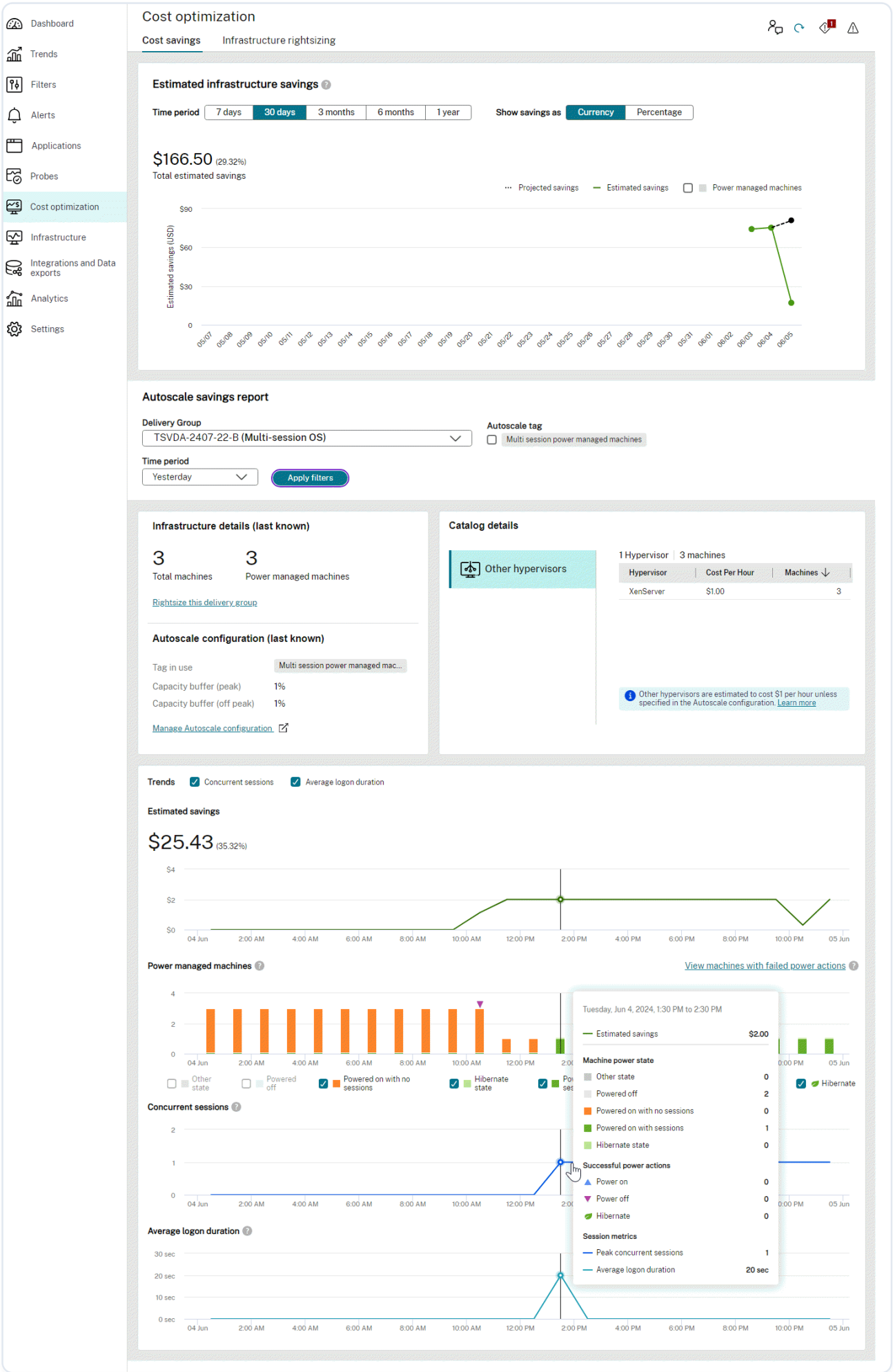
A página Economia de custos fornece uma representação visual da economia de infraestrutura acumulada durante um período selecionado e prevê a economia esperada para os dias restantes. Ao analisar o uso e as sessões das máquinas, esta página ajuda a identificar a economia alcançada e as oportunidades de redução de custos. Esta página oferece:

- Visão sobre a otimização dos custos de infraestrutura
- O valor economizado
- Informações sobre uma série de cenários que podem resultar na superação dos custos projetados
- Oportunidades potenciais para identificação e planejamento estratégico para realizar economia de custos de infraestrutura

O uso da máquina geralmente aumenta durante os horários de pico, exigindo mais recursos. O recurso Autoscale™ ajuda a reduzir custos desligando automaticamente as máquinas não utilizadas durante o período de baixa demanda. A economia projetada depende desse padrão de uso. No entanto, os custos podem exceder as expectativas em circunstâncias específicas, como quando há máquinas não utilizadas ou quando há falhas nas ações de energia do Autoscale. Identificar as razões por trás dessas ocorrências era anteriormente um desafio.

A página **Otimização de Custos** fornece informações detalhadas sobre diferentes cenários que podem fazer com que você exceda o custo esperado. Da mesma forma, por exemplo, se houver máquinas sem sessões, ela mostra mais oportunidades de economia de custos.

Clique na guia **Otimização de Custos** no menu esquerdo da página **Início** para acessar a página **Otimização de Custos**.


Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and Data exports
Analytics
Settings
Cost optimization
Cost savings
Infrastructure rightsizing
Estimated infrastructure savings
Time period
7 days
30 days
3 months
6 months
1 year
Show savings as
Currency
Percentage
$166.50 (29.32%)
Total estimated savings
Projected savings
Estimated savings
Power managed machines
Estimated savings (USD)
$90
$60
$30
0
05/07
05/08
05/09
05/10
05/11
05/12
05/13
05/14
05/15
05/16
05/17
05/18
05/19
05/20
05/21
05/22
05/23
05/24
05/25
05/26
05/27
05/28
05/29
05/30
05/31
06/01
06/02
06/03
06/04
06/05
Autoscale savings report
Delivery Group
TSVDA-2407-22-B (Multi-session OS)
Autoscale tag
Multi session power managed machines
Time period
Yesterday
Apply filters
Infrastructure details (last known)
3
Total machines
3
Power managed machines
Rightsize this delivery group
Autoscale configuration (last known)
Tag in use
Multi session power managed mac...
Capacity buffer (peak)
1%
Capacity buffer (off peak)
1%
Manage Autoscale configuration
Catalog details
Other hypervisors
1 Hypervisor | 3 machines
Hypervisor
Cost Per Hour
Machines
XenServer
$1.00
3
Other hypervisors are estimated to cost $1 per hour unless specified in the Autoscale configuration. Learn more
Trends
Concurrent sessions
Average logon duration
Estimated savings
$25.43 (35.32%)
$4
$2
$0
04 Jun
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
05 Jun
Power managed machines
View machines with failed power actions
Tuesday, Jun 4, 2024, 1:30 PM to 2:30 PM
Estimated savings
$2.00
Machine power state
Other state
0
Powered off
2
Powered on with no sessions
0
Powered on with sessions
1
Hibernate state
0
Successful power actions
Power on
0
Power off
0
Hibernate
0
Session metrics
Peak concurrent sessions
1
Average logon duration
20 sec
Other state
Powered off
Powered on with no sessions
Hibernate state
Hibernate
Concurrent sessions
Average logon duration
30 sec
20 sec
10 sec
0 sec

A página **Otimização de Custos** inclui **Economia estimada** e **Relatório de economia do Autoscale**.

Economia estimada: Esta representação gráfica ajuda a avaliar a utilização eficiente dos recursos de infraestrutura. A economia de custos é exibida na moeda do hipervisor ou como uma porcentagem do custo incorrido. Você pode visualizar os resultados para o último:

- Sete dias
- Trinta dias
- Três meses
- Seis meses
- Doze meses

O gráfico de Economia estimada exibe o seguinte:

- Economias estimadas - Exibe o valor das economias alcançadas na infraestrutura para a duração selecionada
- Máquinas com gerenciamento de energia - Exibe o número total de máquinas com gerenciamento de energia
- Economia projetada - Exibe quanta economia de infraestrutura pode ser feita para a duração restante
- Duração média de logon - Exibe o tempo médio para um usuário fazer logon durante a duração de tempo selecionada.

Relatório de Economia do Autoscale: Esta representação gráfica fornece o relatório de economia para os grupos de entrega para os quais o recurso Autoscale está configurado e habilitado. Este relatório é aplicável apenas para máquinas com gerenciamento de energia. Você pode selecionar um grupo de entrega e, em seguida, selecionar dados para hoje, ontem, semana passada, próxima semana, este mês ou próximo mês. Você pode passar o mouse sobre qualquer gráfico para recuperar valores específicos do gráfico.

> **Observação:**

> Se o grupo de entrega for excluído, você não poderá obter nenhum dado no relatório de economia do Autoscale.

> Você pode detalhar as seguintes opções na lista suspensa de grupos de entrega:

- **Todos**: Os detalhes da infraestrutura exibem todas as informações do grupo de entrega.
- **Sessões únicas**: Detalhes da infraestrutura para todos os grupos de entrega que são máquinas de sessão única, juntamente com a representação gráfica do estado de energia da máquina, ações de energia bem-sucedidas do Autoscale e sessões ao passar o mouse sobre o gráfico.
- **Múltiplas sessões**: Detalhes da infraestrutura para todos os grupos de entrega que são máquinas de múltiplas sessões, juntamente com a representação gráfica.

Os dados são exibidos para a duração selecionada. A representação gráfica das **Economias estimadas** são as economias reais da seleção feita no menu suspenso. Ao passar o mouse sobre os pontos de pico, são exibidas informações sobre o estado de energia da máquina, ações de energia bem-sucedidas do Autoscale e sessões.

Com base no grupo de entrega selecionado, você pode visualizar os seguintes detalhes:

- **Detalhes da infraestrutura**
  - Total de máquinas e máquinas gerenciadas por energia - Exibe o número total de máquinas e, destas, quantas são gerenciadas por energia. Esses dados oferecem uma oportunidade adicional para considerar a conversão das máquinas restantes não gerenciadas por energia em máquinas gerenciadas por energia, habilitando assim o recurso Autoscale para uma cobertura mais abrangente. Os dados na seção Detalhes da infraestrutura mostram as últimas informações conhecidas, atualizadas a cada hora.
- **Detalhes do catálogo**

  Exibe o nome dos hipervisores (provedores de serviço). Para obter mais informações, consulte Plataformas de hospedagem VDA compatíveis. Os dados nos Detalhes do catálogo mostram os dados mais recentes (dados em tempo real) disponíveis no momento atual.

  Você pode obter os seguintes detalhes:

  - **Nome do hipervisor** - Exibe o nome do hipervisor ao qual o site está conectado. Exibe todos os hipervisores disponíveis quando vários hipervisores estão presentes.
  - **Instância** - Exibe o nome da instância.
  - **Custo por hora** - Exibe o custo por máquina por hora na moeda que o hipervisor suporta. Para máquinas Azure, quando a permissão Microsoft.Consumption/pricesheets/read está disponível, o preço efetivo é exibido na moeda configurada na assinatura do Azure. Se as permissões não estiverem disponíveis, o preço de varejo do Azure será exibido. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure. Para outras

máquinas, o custo é exibido com base no custo inserido pelos administradores no Web Studio. O custo padrão é de US$ 1 se o custo não for mencionado no Web Studio. Para obter mais informações, consulte Como o custo é calculado para otimizar o custo?.

- **Máquinas** - Exibe a contagem de máquinas para a instância selecionada.

- **Configuração do Autoscale (última conhecida)**

  Tag em uso - Exibe a tag das máquinas configuradas nas configurações do Autoscale em um WebStudio. Você também pode filtrar os dados com base nas máquinas marcadas. Neste caso, você obtém apenas o resumo das máquinas marcadas.

  Buffer de capacidade (pico) e **Buffer de capacidade (fora de pico)**

  Exibe a porcentagem de buffer para máquinas ligadas com base no requisito máximo do grupo de entrega durante os horários de pico e fora de pico.

- **Economia estimada**

  Exibe o valor da economia alcançada na infraestrutura para a duração selecionada.

- **Máquinas com gerenciamento de energia**

  Com o Autoscale ativado, as máquinas com gerenciamento de energia são desligadas quando não estão em uso para otimizar custos. Você pode obter os seguintes detalhes:

  - Número de máquinas desligadas - Esses dados ajudam você a analisar o número de máquinas que foram desligadas e, assim, ajudaram a reduzir custos.
  - Estado de hibernação - Esses dados ajudam você a analisar quantas máquinas estão no estado de hibernação.
  - Máquinas ligadas sem sessões - Esses dados fornecem a você a oportunidade de analisar por que as máquinas estavam ativas sem nenhuma sessão. Esses dados fornecem a você a oportunidade de planejar uma estratégia de economia de infraestrutura mais eficaz.
  - Máquinas ligadas com sessões - Esses dados ajudam você a analisar o número de máquinas que foram ligadas e com sessões ativas.
  - Desligar - Esses dados ajudam você a analisar o número de máquinas que foram desligadas ou suspensas e quando essa ação foi realizada. Você pode verificar esses dados e fazer modificações adicionais, contribuindo para a redução de custos.
  - Ligar - Esses dados ajudam você a analisar quantas máquinas foram ligadas e quando essa ação foi realizada. Você pode verificar esses dados e fazer modificações adicionais e, assim, ajudar a reduzir custos.

- **Sessões simultâneas**

  Exibe o número total de sessões no horário selecionado. Esses dados ajudam você a determinar quando desligar máquinas para otimização de custos.

- **Duração média do logon**

  Exibe o tempo médio para um usuário fazer logon durante a duração de tempo selecionada.

Dimensionamento da infraestrutura

A página **Dimensionamento da Infraestrutura** ajuda você a analisar os aspectos de provisionamento e dimensionamento do seu grupo de entrega com base na utilização dos recursos. Com base nesta análise, você pode:

- Reduzir os gastos com recursos não utilizados
- Identificar se as máquinas para o consumo do grupo de entrega fornecido estão superdimensionadas, subdimensionadas ou dimensionadas corretamente
- Identificar se a utilização é impulsionada principalmente por usuários avançados (indicado por maior utilização pelas máquinas do percentil superior de 5% em comparação com o restante do grupo)

Você pode filtrar o dimensionamento da infraestrutura usando o seguinte:

- Grupo de Entrega - Você pode filtrar por grupos de entrega de SO de sessão única ou SO de múltiplas sessões
- Tags - Tags são os nomes de tags aplicados à máquina. Assim, você pode filtrar máquinas com as mesmas tags. Você pode selecionar várias tags, até cinco tags. Ao selecionar várias tags, você pode filtrar todas as máquinas que possuem pelo menos uma das tags de máquina selecionadas aplicadas.
- Período de tempo - Você pode filtrar os dados para as últimas 24 horas, 7 dias e 30 dias.

A página de dimensionamento da infraestrutura oferece:

- Visão detalhada dos detalhes de utilização
- Resumo da utilização dos recursos
- Tendências na utilização de recursos

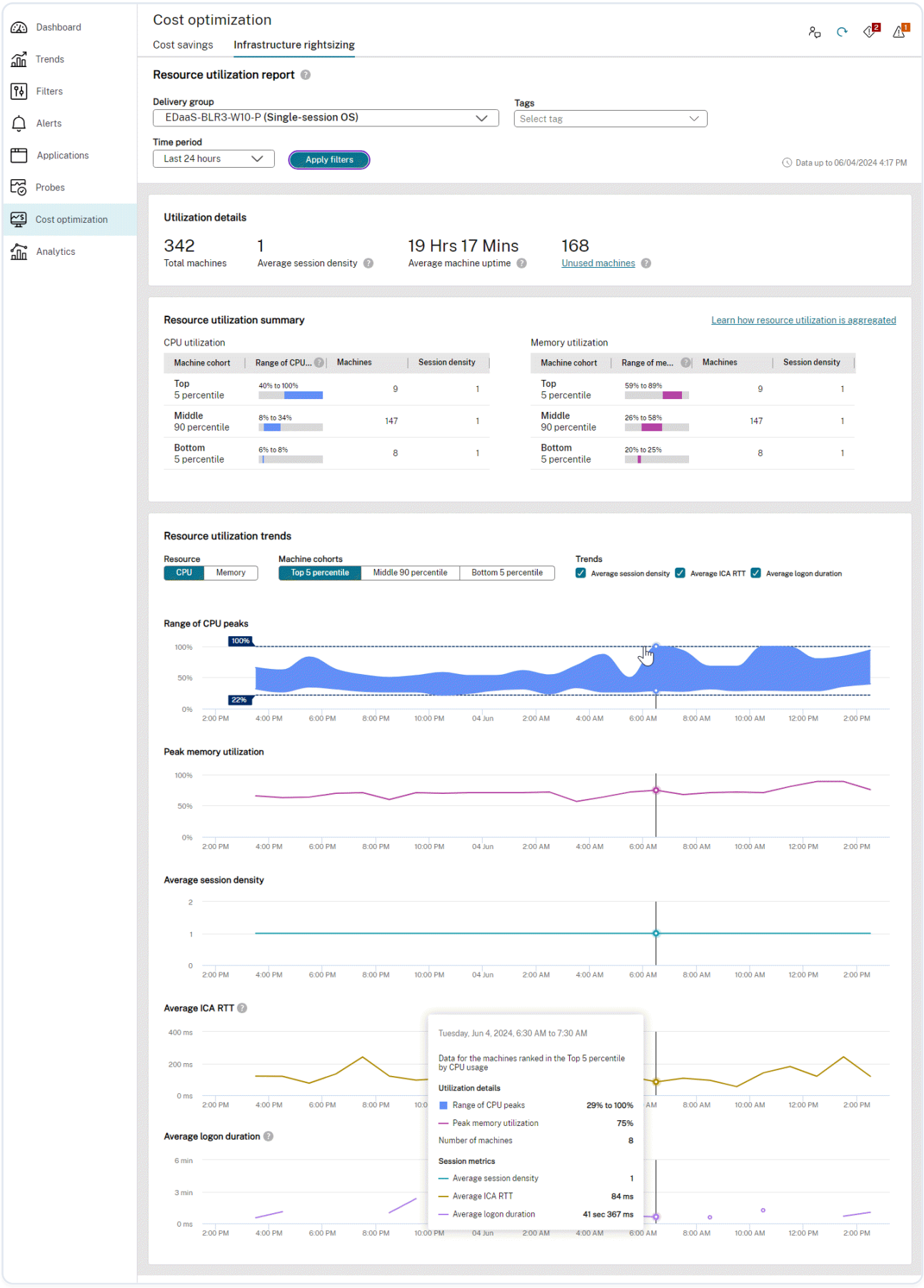
Os dados agregados exibidos nesta página são atualizados da seguinte forma:

- Uma hora para o filtro Últimas 24 horas e Últimos 7 dias

- Um dia para o filtro Últimos 30 dias

Clique na guia **Otimização de Custos** no menu esquerdo da página inicial. Em seguida, clique na guia **Dimensionamento de infraestrutura** para acessar a página **Dimensionamento de infraestrutura**.

Você também pode clicar no link **Dimensionar este grupo de entrega** na seção **Detalhes da infraestrutura** na guia **Otimização de Custos** > **Economia de custos** para acessar a página **Dimensionamento de infraestrutura**.



A página **Dimensionamento da infraestrutura** inclui:

- Detalhes de utilização

- Resumo da utilização de recursos
- Tendências de utilização de recursos

Detalhes de utilização: Esta seção fornece detalhes sobre a utilização do grupo de entrega selecionado e para as tags selecionadas. Você pode visualizar os detalhes das últimas 24 horas, 7 dias e 30 dias. A seção Detalhes de utilização fornece detalhes para toda a duração do filtro de tempo selecionado. Por exemplo, se 7 dias for selecionado, a contagem total de máquinas é o número total de máquinas que estavam ligadas em qualquer ponto durante os 7 dias. A seção Detalhes de utilização fornece o seguinte:

- **Total de máquinas** - Exibe o número total de máquinas. Isso inclui todas as máquinas que foram ligadas durante o período selecionado. Por exemplo, se 7 dias for selecionado, a contagem total de máquinas é o número total de máquinas que estavam ligadas em qualquer ponto durante os 7 dias.
- **Densidade média de sessão** - Esta é uma média entre o número de máquinas e o período de tempo selecionado. Refere-se à quantidade de carga de sessão em uma máquina que afeta o recurso disponível para as sessões.
- **Tempo médio de atividade da máquina** - É a proporção do tempo total de atividade das máquinas gerenciadas por energia para o período de tempo selecionado. Quanto tempo a máquina esteve ativa, por dia por máquina. Suponha que existam duas máquinas em um grupo de entrega ou na tag selecionada, e uma máquina foi usada por 24 horas e a outra máquina foi usada por 1 hora, o tempo médio de atividade da máquina é de 12 horas e 30 minutos. Neste exemplo, o valor do filtro selecionado é Últimas 24 horas.
- **Máquinas não utilizadas** - Exibe o número de máquinas que não tiveram sessões durante o período de tempo selecionado, mas que ainda estavam ligadas. Clique no link **Máquinas não utilizadas** para abrir a guia **Filtros**, onde você pode visualizar todas as máquinas nesse mesmo grupo de entrega que estão atualmente ligadas e não têm sessões.

Resumo de utilização de recursos: Esta seção fornece um resumo de como os recursos foram utilizados para o grupo de entrega selecionado e para as tags selecionadas. Você pode selecionar várias tags, até cinco tags. Você pode visualizar os detalhes para as últimas 24 horas, 7 dias e 30 dias. As máquinas são classificadas com base na utilização. A seção Resumo de utilização de recursos fornece detalhes sobre a utilização da CPU e da memória para as máquinas com sessões ativas.

- **Utilização da CPU**:
  - Coorte de máquinas - Fornece informações sobre os grupos de máquinas categorizados em superior, médio e inferior com base na utilização da CPU. 5% das máquinas mais

utilizadas são categorizadas em **Percentil superior de 5%**, 5% das máquinas menos utilizadas são categorizadas em **Percentil inferior de 5%**, e os 90% restantes são categorizados em **Percentil médio de 90%**.

- Intervalo de picos de CPU - Exibe o intervalo de picos de CPU com base na sua utilização correspondente à coorte de máquinas.
- Máquinas - Exibe o número de máquinas correspondentes à coorte de máquinas.
- Densidade da sessão - Exibe a densidade da sessão correspondente à coorte de máquinas.

- **Utilização da memória**:
  - Coorte de máquinas - Fornece informações sobre os grupos de máquinas categorizados em superior, médio e inferior com base na utilização da memória. 5% das máquinas mais utilizadas são categorizadas em **Percentil superior de 5%**, 5% das máquinas menos utilizadas são categorizadas em **Percentil inferior de 5%**, e os 90% restantes são categorizados em **Percentil médio de 90%**.
  - Intervalo de picos de memória - Exibe o intervalo de picos de memória com base na sua utilização correspondente à coorte de máquinas.
  - Máquinas - Exibe o número de máquinas correspondentes à coorte de máquinas.
  - Densidade da sessão - Exibe a densidade da sessão correspondente à coorte de máquinas.

A tabela a seguir fornece informações sobre os possíveis itens de ação que você pode realizar com base nos valores presentes na seção Resumo de Utilização de Recursos:

CENÁRIO	ITEM DE AÇÃO
A utilização da CPU é maior	Aumente as especificações da CPU do grupo de entrega. Ou, identifique os usuários com maior uso e mova-os para um grupo de entrega diferente com melhores especificações.
A utilização da CPU é menor	Diminua a especificação da CPU do grupo de entrega.
A utilização da memória é maior	Aumente as especificações de memória do grupo de entrega.

CENÁRIO	ITEM DE AÇÃO
A utilização da memória é menor	Diminua a especificação de memória do grupo de entrega.

Como os dados são preenchidos na seção de resumo de utilização de recursos?

Os dados na seção de resumo de utilização de recursos são preenchidos com base nos dados das **tendências de utilização de recursos**. O resumo fornece detalhes apenas para as máquinas com sessões ativas. O resumo oferece melhores resultados quando há mais de cinco máquinas.

Com base no número de máquinas no grupo de entrega selecionado, o valor máximo e mínimo de utilização é calculado.

Por exemplo, considere que você selecionou Últimos 7 dias como período de tempo e tem 20 máquinas no grupo de entrega selecionado. Essas 20 máquinas são categorizadas em **percentil superior de 5%**, **percentil médio de 90%** e **percentil inferior de 5%**. A utilização da CPU e da memória é calculada quando há sessões ativas. Por exemplo, neste caso, a primeira e a última máquina nos 5% superiores e 5% inferiores. As 18 máquinas restantes são categorizadas no percentil médio de 90%. Neste caso, como há apenas uma máquina no **percentil superior de 5%**, o valor máximo e mínimo é o mesmo. Quando há mais de uma máquina na coorte, o valor mais alto e mais baixo da coorte é baseado no valor máximo da máquina de classificação mais alta nesse grupo e no valor máximo da máquina de classificação mais baixa nesse grupo, respectivamente.

Quando você seleciona **CPU** como tipo de **Recurso**, o **Intervalo de picos de CPU** e a **Utilização máxima de memória** para as máquinas selecionadas são exibidos.

Quando você seleciona Memória como tipo de Recurso, o Intervalo de picos de memória e a Utilização máxima de CPU para as máquinas selecionadas são exibidos.

Tendências de utilização de recursos: Esta seção fornece uma representação gráfica para o Intervalo de picos de CPU, utilização máxima de memória, densidade média de sessão, RTT médio de ICA® e duração média de logon.

Você pode filtrar os detalhes para os seguintes itens:

- Recurso - CPU e Memória
- Coortes de máquina - 5º percentil superior, 90º percentil médio e 5º percentil inferior
- Tendências - Sessão média, RTT ICA médio, Duração média do logon.

Você pode visualizar os seguintes gráficos:

- **Intervalo de picos de CPU** - Exibe o intervalo de picos de CPU em uma faixa. Quando você passa o mouse sobre qualquer ponto na faixa, o valor superior e inferior da faixa é exibido.
- **Utilização máxima de memória** - Exibe a maior utilização de memória para as máquinas selecionadas e para o tempo selecionado em um gráfico.
- **Densidade média da sessão** - Exibe a densidade média da sessão para as máquinas selecionadas e para o tempo selecionado em um gráfico.
- **RTT ICA médio** - Exibe o tempo médio de ida e volta para a sessão. Este gráfico mostra interrupções quando não há sessões ativas ou quando as sessões são desconectadas.
- **Duração média do logon** - Exibe a duração média do logon para as máquinas selecionadas e para o período de tempo selecionado em um gráfico. Este gráfico mostra dados quando um novo logon é iniciado durante o tempo selecionado.

Matriz de compatibilidade de recursos

O Citrix Director 7 2407 é compatível com:

- Citrix Virtual Apps and Desktops™ 7 2112 e posterior
- Citrix Aplicativos Virtuais e Desktops 7 1912 LTSR

Em cada site, embora você possa usar o Director com versões anteriores do Delivery Controller™, nem todos os recursos da versão mais recente do Director podem estar disponíveis. A Citrix recomenda que o Director, o Delivery Controller e os VDAs estejam na mesma versão.

> **Observação:**
>
> Depois de atualizar um Delivery Controller, você será solicitado a atualizar o site ao abrir o Studio. Para obter mais informações, consulte a seção **Sequência de atualização** em Atualizar uma implantação.
>
> Na primeira vez que você fizer login após uma atualização do Director, uma verificação de versão será realizada nos sites configurados. Se algum site estiver executando uma versão do Controller anterior à do Director, uma mensagem aparecerá no console do Director, recomendando uma atualização do site. Além disso, enquanto a versão do site for mais

antiga que a do Director, uma nota permanecerá exibida no Painel do Director indicando essa incompatibilidade.

Observação:

Versões anteriores do Citrix Director não exibem políticas aplicadas a sessões de usuário executadas em versões recentes do VDA. O Citrix Director 1912 e versões anteriores não exibem políticas aplicadas a sessões de usuário executadas em versões do VDA 2003 e posteriores. Use as versões 2003 e posteriores do Citrix Director para visualizar essas políticas.

Os recursos específicos do Director com a versão mínima do Delivery Controller (DC), VDA e outros componentes dependentes necessários, juntamente com a Edição da Licença, estão listados abaixo.

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
2407	Otimização de custos	Nenhum	Todas
2407	Integrações e exportações de dados	VDA 2407	Todas
2407	Diagnosticar sessões de usuário históricas (Pré-visualização)	VDA 2407	Todos
2407	Gerenciador de Atividades para sessão de Acesso Privado Seguro (Pré-visualização)	VDA 2407	Todos
2407	Integração de Acesso Privado	VDA 2407	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
	Seguro para aplicativos TCP e UDP com o Director (Pré-visualização)		
2407	Monitoramento de infraestrutura (Pré-visualização)	VDA 2407	Todos
2407	Alerta de máquinas não registradas(/pt-br/citrix-virtual-apps-desktops/2407/director/site-analytics/alerts-notifications.html#unregistered-machines-in-)	VDA 2407 e DDC 2407	Todos
2407	Alerta de tempo de atividade da máquina	VDA 2407 e DDC 2407	Todos
2407	Alerta de ação de ligar falha e ação de desligar falha	VDA 2407 e DDC 2407	Todos
2407	Capacidade de incluir anexo CSV em e-mails de alerta e payload JSON em Webhook de alerta	VDA 2407 e DDC 2407	Todos
2407	Inspecionar máquinas com ações de energia recentes	VDA 2407	Todos
2407	Políticas de alerta avançadas	VDA 2407 e DDC 2407	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
2407	Pesquisa unificada para usuários em nuvem e locais	VDA 2407	Todos
2407	Gráficos de monitoramento de uso de aplicativos publicados no Dashboard	VDA 2407 e DDC 2407	Sites com licença Platinum
2402 LTSR	Integração do Secure Private Access para aplicativos web e SaaS com o Director (Pré-visualização)	VDA 2402 LTSR	Todos
2402 LTSR	Suporte para Microsoft Teams versão 2.1 ou anterior	VDA 2402 LTSR	Todos
2311	Reproduzir sessões ao vivo e gravadas	VDA 2308 e DDC 2311	Todos
2311	Topologia da Sessão	Nenhum	Todos
2311	Resolução de tela ideal	Nenhum	Todos
2311	Otimização do MS Teams	VDA 2311 e DDC mais recente	Todos
2311	Aprimoramentos da Visão Geral de Probes	Nenhum	Todos
2311	Visualização de Duração de Logon	Nenhum	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
	de Sessão Reformulada		
2308	Resumo e detalhamento de Probes	Nenhum	Todos
2308	Suporte do Agente de Probes Citrix para autenticação multifator do Citrix Gateway	Citrix Gateway	Todos
2308	Desativar Alertas de Hipervisor	Nenhum	Todos
2308	Tendências para métricas de Experiência de Sessão	Nenhum	Todos
2305	Suporte à autenticação via Citrix Gateway	Nenhum	Todos
2305	Gerenciamento de Autoscale no Director	Nenhum	Todos
2303	Alerta de Máquinas com Falha	DC 7 2303	Premium
2203	Suporte a TLS 1.3	-	Todos
2212	Utilização de GPU em tempo real disponível para GPUs AMD	DC 7.14 e VDA 7.14 executando Windows de 64 bits e HDX 3D Pro ativado	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
2212	Agendamento Avançado de Sondas	DC 7 1906 e Citrix Probe Agent 2209	Premium
1909	Configurar sites locais com o Citrix Analytics for Performance	DC 7 1906 e VDA 1906	Todos
1906	Reconexão Automática de Sessão	DC 7 1906 e VDA 1906	Todos
1906	Duração da inicialização da sessão	DC 7 1906 e VDA 1903	Todos
1906	Sondagem de desktop(/pt-br/citrix-virtual-apps-desktops/2407/director/probes.html)	DC 7 1906 e Citrix Probe Agent 1903	Premium
7.9 e posterior	Duração do Citrix Profile Management no Carregamento de Perfil	VDA 1903	Todos
1811	Detalhamento de Perfil	DC 7 1811 e VDA 1811	Todos
1811	Monitoramento de Alertas do Hypervisor	DC 7 1811	Premium
1811	Sondagem de aplicativo(/pt-br/citrix-virtual-apps-	DC 7 1811 e Citrix Application Probe Agent 1811	Premium

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
	desktops/2407/director/probes.html)		
1811	Integridade da licença RDS da Microsoft	DC 7 1811 e VDA 7.16	Todos
1811	Exibição de dados RTOP principais	DC 7 1811 e VDA 1808	Premium
1808	Exportação de dados de filtros	DC 7 1808	Todos
1808	Detalhamento da sessão interativa	DC 7 1808 e VDA 1808	Todos
1808	Detalhamento de GPO	DC 7 1808 e VDA 1808	Todos
1808	Dados históricos da máquina disponíveis usando a API OData	DC 7 1808	Todos
7.18	Sondagem de aplicativos	DC 7.18	Premium (anteriormente Platinum)
7.18	Políticas de alerta inteligente	DC 7.18	Premium (anteriormente Platinum)
7.18	Link do Assistente de Saúde	Nenhum	Todos
7.18	Detalhamento da Sessão Interativa	Nenhum	Todos
7.17	Autenticação de cartão inteligente PIV	Nenhum	Todos

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
7.16	Análise de Aplicativos	DC 7.16 e VDA 7.15	Todos
7.16	API OData V.4	DC 7.16	Todos
7.16	Usuários do VDA Linux em modo sombra	VDA 7.16	Todos
7.16	Suporte a grupos locais de domínio	Nenhum	Todos
7.16	Acesso ao console da máquina	DC 7.16	Todos
7.15	Monitoramento de falhas de aplicativos	DC 7.15 e VDA 7.15	Todos
7.14	Solução de problemas centrada em aplicativos	DC 7.13 e VDA 7.13	Todos
7.14	Monitoramento de Disco	DC 7.14 e VDA 7.14	Todos
7.14	Monitoramento de GPU	DC 7.14 e VDA 7.14	Todos
7.13	Protocolo de transporte no painel Detalhes da sessão	DC 7.x e VDA 7.13	Todos
7.12	Descrições de falha de conexão e máquina amigáveis ao usuário	DC 7.12 e VDA 7.x	Todos
7.12	Disponibilidade de dados históricos	DC 7.12 e VDA 7.x	Enterprise

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
	aumentada na edição Enterprise		
7.12	Relatórios Personalizados	DC 7.12 e VDA 7.x	Premium (anteriormente Platinum)
7.11	Relatórios de utilização de recursos	DC 7.11 e VDA 7.11	Todos
7.11	Alertas estendidos para condições de CPU, memória e RTT ICA	DC 7.11 e VDA 7.11	Premium (anteriormente Platinum)
7.11	Melhorias no relatório de exportação	DC 7.11 e VDA 7.x	Todos
7.11	Integração com Citrix ADM	DC 7.11, VDA 7.x e MAS versão 11.1 Build 49.16	Premium (anteriormente Platinum)
7.9	Detalhamento da duração do logon	DC 7.9 e VDA 7.x	Todos
7.7	Monitoramento e alerta proativos	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)
7.7	Integração de Autenticação do Windows	DC 7.x e VDA 7.x	Todos
7.7	Uso de SO de Sessão Única e Múltiplas Sessões	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)

VERSÃO DO DIRECTOR	RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	EDIÇÃO
7.6.300	Suporte para canal virtual Framehawk	DC 7.6 e VDA 7.6	Todos
7.6.200	Integração de gravação de sessão(/pt-br/citrix-virtual-apps-desktops/2407/director/troubleshoot-deployments/user-issues/record-sessions.html)	DC 7.6 e VDA 7.x	Premium (anteriormente Platinum)
7	Integração do HDX Insight(/pt-br/citrix-virtual-apps-desktops/2407/director/install-and-configure/hdx-insight.html)	DC 7.6, VDA 7.x e Citrix ADM	Premium (anteriormente Platinum)

Granularidade e retenção de dados

Agregação de valores de dados

O Monitor Service coleta vários dados, incluindo uso da sessão do usuário, detalhes de desempenho de logon do usuário, detalhes de balanceamento de carga da sessão e informações de falha de conexão e máquina. Os dados são agregados de forma diferente dependendo de sua categoria. Compreender a agregação de valores de dados apresentados usando as APIs do Método OData é fundamental para interpretar os dados. Por exemplo:

- Sessões Conectadas e Falhas de Máquina ocorrem durante um período. Portanto, são expostas como máximos durante um período de tempo.
- A Duração do Logon é uma medida do período de tempo, portanto, é exposta como uma média durante um período de tempo.

- A Contagem de Logons e as Falhas de Conexão são contagens de ocorrências durante um período, portanto, são expostas como somas durante um período de tempo.

Avaliação de dados concorrentes

As sessões devem ser sobrepostas para serem consideradas concorrentes. No entanto, quando o intervalo de tempo é de 1 minuto, todas as sessões nesse minuto (independentemente de se sobreporem) são consideradas concorrentes. O tamanho do intervalo é tão pequeno que a sobrecarga de desempenho envolvida no cálculo da precisão não compensa o valor adicionado. Se as sessões ocorrerem na mesma hora, mas não no mesmo minuto, elas não são consideradas sobrepostas.

Correlação de tabelas de resumo com dados brutos

O modelo de dados representa métricas de duas maneiras diferentes:

- As tabelas de resumo representam visualizações agregadas das métricas em granularidades de tempo por minuto, hora e dia.
- Os dados brutos representam eventos individuais ou o estado atual rastreado na sessão, conexão, aplicativo e outros objetos.

Ao tentar correlacionar dados entre chamadas de API ou dentro do próprio modelo de dados, é importante entender os seguintes conceitos e limitações:

- **Nenhum dado de resumo para intervalos parciais.** Os resumos de métricas são projetados para atender às necessidades de tendências históricas em longos períodos de tempo. Essas métricas são agregadas na tabela de resumo para intervalos completos. Não há dados de resumo para um intervalo parcial no início (dados mais antigos disponíveis) da coleta de dados nem no final. Ao visualizar agregações de um dia (Intervalo=1440), isso significa que os primeiros e os mais recentes dias incompletos não possuem dados. Embora dados brutos possam existir para esses intervalos parciais, eles nunca são resumidos. Você pode determinar o intervalo agregado mais antigo e mais recente para uma granularidade de dados específica puxando o min e o max SummaryDate de uma tabela de resumo específica. A coluna SummaryDate representa o início do intervalo. A coluna Granularity representa a duração do intervalo para os dados agregados.
- **Correlação por tempo.** As métricas são agregadas na tabela de resumo para intervalos completos, conforme descrito na seção anterior. Elas podem ser usadas para tendências históricas, mas os eventos brutos podem estar mais atualizados no estado do que o que foi resumido para análise de tendências. Qualquer comparação baseada em tempo de resumo

com dados brutos deve considerar que não há dados de resumo para intervalos parciais que possam ocorrer ou para o início e o fim do período de tempo.

- **Eventos perdidos e latentes.** As métricas que são agregadas na tabela de resumo podem ser ligeiramente imprecisas se os eventos forem perdidos ou latentes para o período de agregação. Embora o Serviço de Monitoramento tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo para eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a alta disponibilidade de conexão, haverá lacunas nas contagens de dados de resumo das conexões atuais, mas as instâncias de sessão ainda estarão em execução nos dados brutos.
- **Períodos de retenção de dados.** Os dados nas tabelas de resumo são retidos em um cronograma de limpeza diferente do cronograma para dados de eventos brutos. Os dados podem estar ausentes porque foram removidos das tabelas de resumo ou brutas. Os períodos de retenção também podem diferir para diferentes granularidades de dados de resumo. Dados de granularidade mais baixa (minutos) são limpos mais rapidamente do que dados de granularidade mais alta (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles poderão ser encontrados em uma granularidade mais alta. 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 mais alta para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de data/hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não se enquadram nos limites por hora, pode haver alguma discrepância quanto ao local onde os dados são agregados.

Granularidade e retenção

A granularidade dos dados agregados recuperados pelo Director é uma função do período de tempo (T) solicitado. As regras são as seguintes:

- 0 \< T \<= 1 hora - usa granularidade por minuto
- 0 \< T \<= 30 dias - usa granularidade por hora
- T \> 31 dias - usa granularidade por dia

Os dados solicitados que não vêm de dados agregados vêm das informações brutas de Sessão e Conexão. Esses dados tendem a crescer rapidamente e, portanto, têm sua própria configuração de limpeza. A limpeza garante que apenas dados relevantes sejam mantidos a longo prazo. A

limpeza garante melhor desempenho, mantendo a granularidade necessária para relatórios. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção, caso contrário, o padrão é usado. Caso haja perda de conectividade com o banco de dados do Site, o Serviço de Monitoramento usará os dias de retenção padrão para o direito Premium, conforme especificado na tabela abaixo.

Para acessar as configurações, execute os seguintes comandos PowerShell no Delivery Controller™:

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

	NOME DA CONFIGURAÇÃO	LIMPEZA AFETADA	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
1	GroomSessions RetentionDays	Retenção de registros de Sessão e Conexão após o término da Sessão	90	31
2	GroomFailures RetentionDays	Registros de MachineFailure Log e ConnectionFail ureLog	90	31
3	GroomLoadInd exesRetentionD ays	Registros de LoadIndex	90	31
4	GroomDeleted RetentionDays	Entidades de Máquina, Catálogo, Grupo de Desktop e	90	31

	NOME DA CONFIGURAÇÃO	LIMPEZA AFETADA	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
		Hypervisor que possuem um LifecycleState de 'Excluído'. Esta configuração também exclui quaisquer registros relacionados de Sessão, Detalhe da Sessão, Resumo, Falha ou LoadIndex.		
5	GroomSummariesRetentionDays	Registros de DesktopGroupSummary, FailureLogSummary e LoadIndexSummary. Dados agregados - granularidade diária.	365	31
6	GroomMachineHotfixLogRetentionDays	Hotfixes aplicados às máquinas VDA e Controller	90	31
7	GroomMinuteRetentionDays	Dados agregados - granularidade por minuto	3	3

	NOME DA CONFIGURAÇÃO	LIMPEZA AFETADA	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
8	GroomHourlyRetentionDays	Dados agregados - granularidade horária	32	31
9	GroomApplicationInstanceRetentionDays	Histórico de instâncias de aplicativos	90	Não aplicável
10	GroomNotificationLogRetentionDays	Registros de log de notificação	90	Não aplicável
11	GroomResourceUsageRawDataRetentionDays	Dados de utilização de recursos - dados brutos	3	3
12	GroomResourceUsageMinuteDataRetentionDays	Dados de resumo de utilização de recursos - granularidade de minuto	7	7
13	GroomResourceUsageHourDataRetentionDays	Dados de resumo de utilização de recursos - granularidade de hora	30	30
14	GroomResourceUsageDayDataRetentionDays	Dados de resumo de utilização de recursos - granularidade de dia	365	31

	NOME DA CONFIGURAÇÃO	LIMPEZA AFETADA	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
15	GroomProcessUsageRawDataRetentionDays	Dados de utilização de processo - dados brutos	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Dados de utilização de processo - granularidade de minuto	3	3
17	GroomProcessUsageHourDataRetentionDays	Dados de utilização de processo - granularidade de hora	7	7
18	GroomProcessUsageDayDataRetentionDays	Dados de utilização de processo - granularidade de dia	30	30
19	GroomSessionMetricsDataRetentionDays	Dados de métricas de sessão	1	1
20	GroomMachineMetricDataRetentionDays	Dados de métricas da máquina	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	Dados de resumo de métricas da máquina	365	31

	NOME DA CONFIGURAÇÃO	LIMPEZA AFETADA	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
22	GroomApplicationErrorsRetentionDays	Dados de erro do aplicativo	1	1
23	GroomApplicationFaultsRetentionDays	Dados de falha do aplicativo	1	1

Cuidado:

A modificação de valores no banco de dados do Monitor Service exige a reinicialização do serviço para que os novos valores entrem em vigor. Aconselha-se que as alterações no banco de dados do Monitor Service sejam feitas apenas sob a direção do Suporte Citrix.

As configurações GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays e GroomSessionMetricsDataRetentionDays são limitadas aos seus valores padrão de 1, enquanto GroomProcessUsageMinuteDataRetentionDays é limitada ao seu valor padrão de 3. Os comandos PowerShell para definir esses valores foram desabilitados, pois os dados de uso do processo tendem a crescer rapidamente. Além disso, as configurações de retenção baseadas em licença são as seguintes:

- **Sites com licença Premium -** a retenção de limpeza para todas as configurações é limitada a 1000 dias (a Citrix recomenda 365 dias).
- **Sites com licença Advanced -** a retenção de limpeza para todas as configurações é limitada a 31 dias.
- **Todos os outros sites -** a retenção de limpeza para todas as configurações é limitada a 7 dias.

Exceções:

- GroomApplicationInstanceRetentionDays pode ser definido apenas em sites com licença Premium.

- GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays são limitados a 31 dias em sites com licença Premium.

Reter dados por longos períodos tem as seguintes implicações nos tamanhos das tabelas:

- **Dados por hora.** Se os dados por hora puderem permanecer no banco de dados por até dois anos, um site de 1000 grupos de entrega pode fazer com que o banco de dados cresça da seguinte forma:

  1000 grupos de entrega x 24 horas/dia x 365 dias/ano x 2 anos = 17.520.000 linhas de dados. O impacto no desempenho de uma quantidade tão grande de dados nas tabelas de agregação é significativo. Dado que os dados do painel são extraídos desta tabela, os requisitos no servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto dramático no desempenho.
- **Dados de sessão e evento.** Dados coletados toda vez que uma sessão é iniciada e uma conexão/reconexão é feita. Para um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, dois anos de dados dessas tabelas acumulariam mais de um TB de dados, exigindo um banco de dados de nível empresarial de ponta.

Integrações e exportações de dados

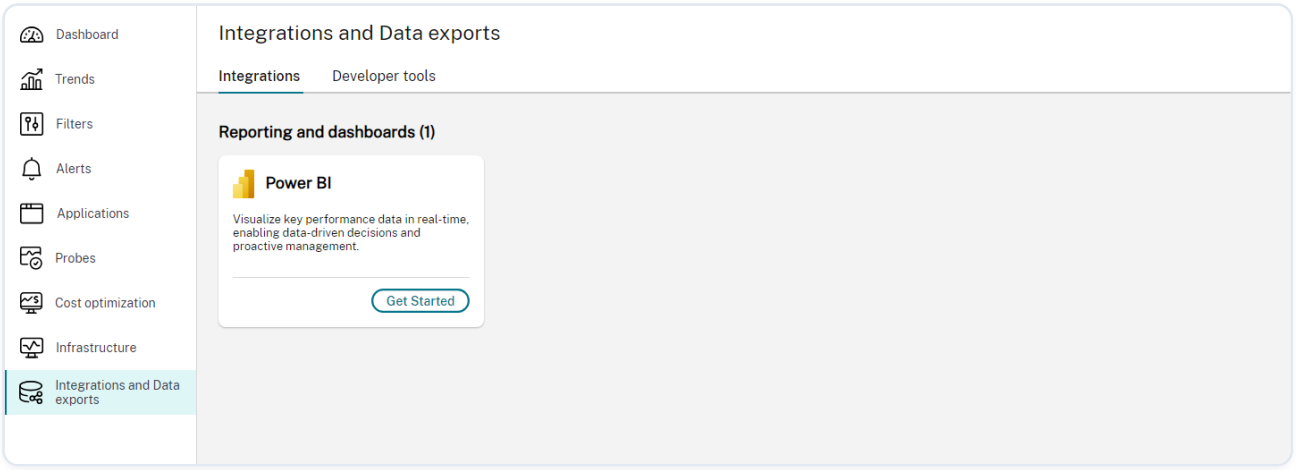
O Citrix Director agora oferece uma nova interface de usuário para integrações e exportações de dados. Esse recurso ajuda a melhorar o conhecimento das várias interfaces e integrações de terceiros disponíveis no Citrix Director. A página **Integrações e exportações de dados** recém-introduzida lista o seguinte:

- Integrações disponíveis
- Ferramentas de desenvolvedor compatíveis

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

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

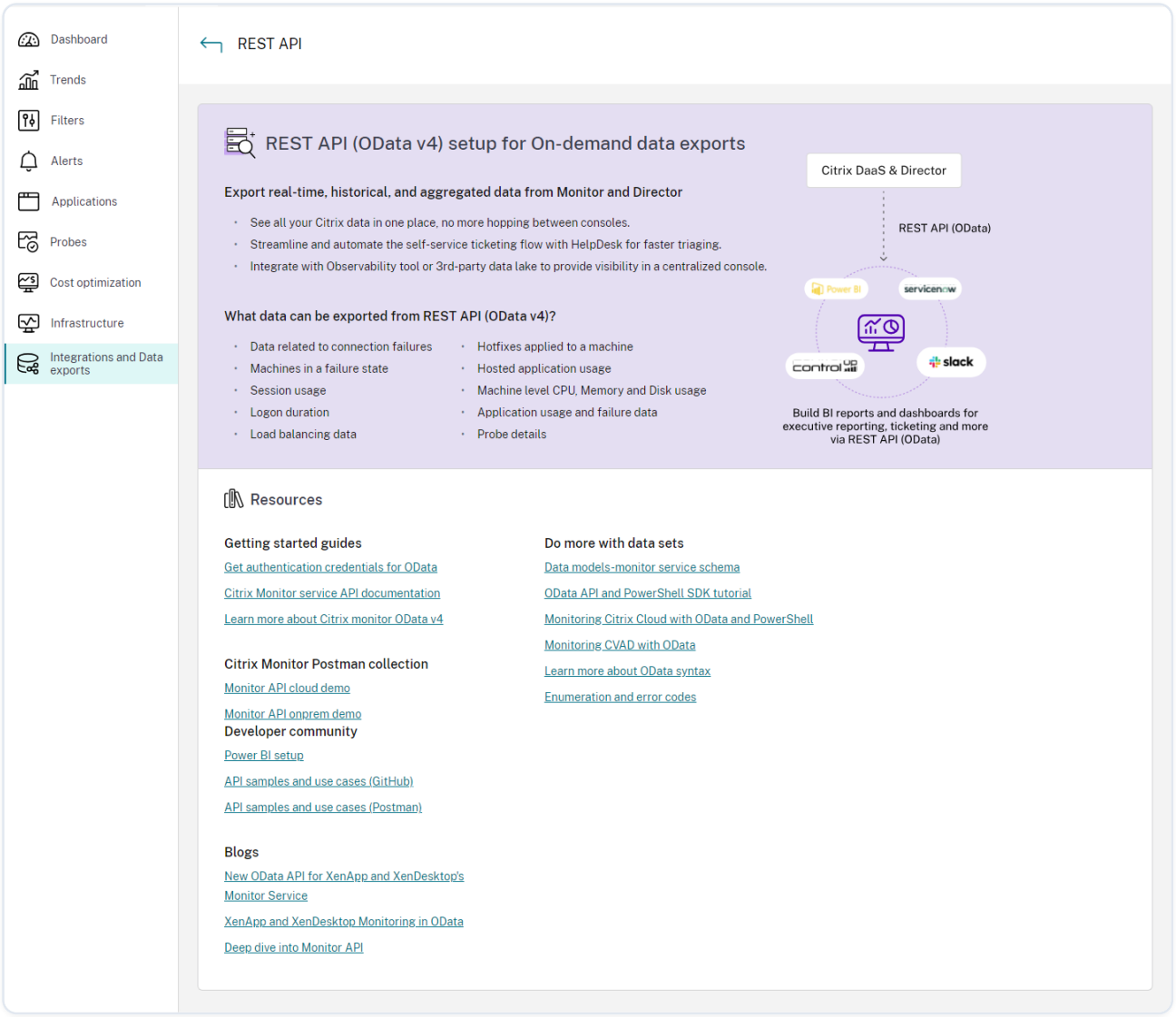
Clique em **Integrações e exportações de dados** no menu de navegação esquerdo. A página **Integrações e exportações de dados** é exibida.



Visualizar integrações disponíveis

A guia **Integrações** exibe as integrações disponíveis para o Citrix Director. Atualmente, o Citrix Director está integrado à observabilidade do Power BI.

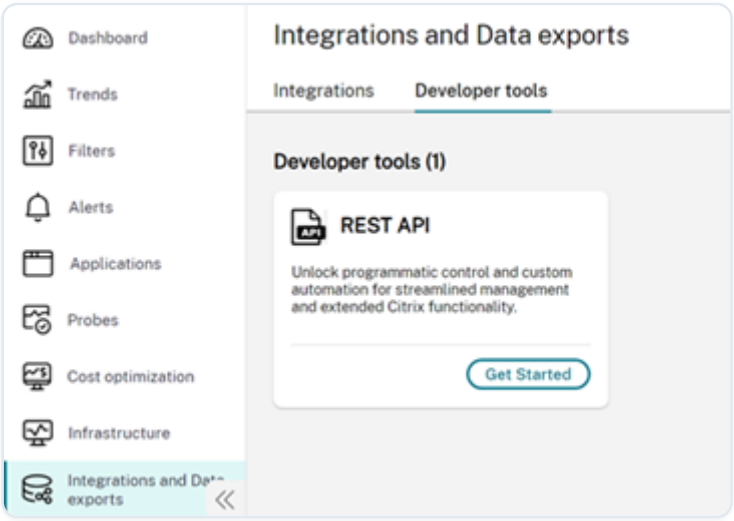
Clique em **Começar**. A página de detalhes das ferramentas de desenvolvedor da **API REST** é exibida.



Esta página fornece links de referência para recursos e blogs.

Exibir ferramentas de desenvolvedor compatíveis

1. Clique em **Ferramentas de desenvolvedor** para visualizar as ferramentas de desenvolvedor disponíveis.



2. Clique em **Começar**. A página de detalhes da ferramenta de desenvolvedor da **API REST** é aberta. Você pode acessar os links de referência para recursos e blogs.

Motivos de falha e solução de problemas do Citrix Director

As tabelas a seguir descrevem as várias categorias de falha, os motivos e a ação que você precisa tomar para resolver os problemas. Para obter mais informações, consulte Enums, códigos de erro e descrições.

Erros de falha de conexão

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
N/A	[0] Desconhecido. Este código de erro não está mapeado.	O serviço de Monitoramento não consegue determinar o motivo da falha de lançamento ou conexão relatada a partir das informações compartilhadas pelo serviço de Brokering.	Colete logs CDF no controlador e entre em contato com o suporte da Citrix.
[0] Nenhum	[1] Nenhum	Nenhum	N/A
[2] MachineFailure	[2] SessionPreparation	A solicitação de preparação de sessão do Delivery Controller para o VDA falhou. Causas possíveis: Problemas de comunicação entre o controlador e o VDA, problemas encontrados pelo Serviço de Broker ao criar uma solicitação de preparação ou problemas de rede que resultam na não	Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com Delivery Controllers no Citrix Virtual Apps and Desktops para problemas comuns que causam problemas de

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		aceitação da solicitação pelo VDA.	comunicação entre o controlador e o VDA.
[2] MachineFailure	[3] RegistrationTimeout	O VDA foi ligado, mas ocorreu um tempo limite enquanto ele tentava se registrar no Delivery Controller.	Verifique se o Citrix Broker Service está em execução no delivery controller e se o Desktop service está em execução no VDA. Inicie cada um se estiverem parados.
[1] ClientConnectionFailure	[4] ConnectionTimeout	O cliente não se conectou ao VDA depois que o VDA foi preparado para o lançamento da sessão. A sessão foi intermediada com sucesso, mas ocorreu um tempo limite enquanto se aguardava a conexão do cliente ao VDA. Causas possíveis: Configurações de firewall, interrupções de rede ou configurações que impedem conexões remotas.	Verifique o console do Director para ver se o cliente tem uma conexão ativa no momento, o que significa que nenhum usuário é impactado. Se nenhuma sessão existir, revise os logs de eventos no cliente e no VDA para quaisquer erros. Resolva quaisquer problemas de conectividade de rede entre o cliente e o VDA.
[4] NoLicensesAvailable	[5] Licensing	A solicitação de licenciamento falhou. Causas possíveis: Número insuficiente de licenças, ou o servidor de licenças	Verifique se o servidor de licenças está online e acessível. Resolva quaisquer problemas de conectividade de rede com o servidor

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		está inativo há mais de 30 dias.	de licenças ou reinicie o servidor de licenças se ele parecer estar com mau funcionamento. Verifique se há licenças suficientes no ambiente e aloque mais, se necessário.
[1] ClientConnectionFailure	[6] Ticketing	Ocorreu uma falha durante a emissão do ticket, indicando que a conexão do cliente com o VDA não corresponde à solicitação intermediada. Um ticket de solicitação de lançamento é preparado pelo Broker e entregue no arquivo ICA®. Quando o usuário tenta iniciar uma sessão, o VDA valida o ticket de lançamento no arquivo ICA com o Broker. Causas possíveis: O arquivo ICA está corrompido ou o usuário está tentando fazer uma conexão não autorizada.	Verifique se o usuário tem acesso ao aplicativo ou desktop com base nos grupos de usuários definidos nos grupos de entrega. Instrua o usuário a relançar o aplicativo ou desktop para determinar se este é um problema pontual. Se o problema ocorrer novamente, revise os logs de eventos do dispositivo cliente em busca de erros. Verifique se o VDA ao qual o usuário está tentando se conectar está registrado. Se não estiver registrado, revise os logs de eventos no VDA e resolva quaisquer problemas de registro.

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[1] ClientConnectionFailure	[7] Other	Uma sessão foi relatada como encerrada a partir do VDA depois que o cliente contatou inicialmente o VDA, mas antes de completar a sequência de conexão.	Verifique se a sessão não foi encerrada pelo usuário antes do lançamento. Tente relançar a sessão; se o problema persistir, colete os logs CDF e entre em contato com o suporte da Citrix.
[1] ClientConnectionFailure	[8] GeneralFail	A sessão falhou ao iniciar. Causas possíveis: Um lançamento intermediado foi solicitado enquanto o broker ainda estava iniciando ou inicializando, ou um erro interno durante a fase de intermediação de um lançamento.	Verifique se o Serviço de Broker da Citrix está em execução e tente novamente iniciar a sessão.
[5] Configuration	[9] MaintenanceMode	O VDA, ou o grupo de entrega ao qual o VDA pertence, está definido no modo de manutenção.	Determine se o modo de manutenção é necessário. Desative o modo de manutenção no grupo de entrega ou na máquina em questão, se não for necessário, e instrua o usuário a tentar reconectar.

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[5] Configuration	[10] ApplicationDisabled	O aplicativo não pode ser acessado pelos usuários finais porque foi desativado pelo administrador.	Se o aplicativo for destinado a uso em produção, habilite o aplicativo e instrua o usuário a reconectar.
[4] NoLicensesAvailable	[11] Recurso de Licença Recusado	O recurso que está sendo usado não é coberto pelas licenças existentes.	Entre em contato com um representante de vendas da Citrix para confirmar os recursos cobertos pela edição e tipo de licença existentes do Citrix Virtual Apps and Desktops™.
[3] Nenhuma Capacidade Disponível	[13] Limite de Sessões Atingido	Todos os VDAs estão em uso e não há capacidade para hospedar mais sessões. Causas possíveis: Todos os VDAs estão em uso (para VDAs de SO de sessão única), ou todos os VDAs atingiram o número máximo configurado de sessões simultâneas permitidas (para VDAs de SO de múltiplas sessões).	Verifique se há VDAs em modo de manutenção. Desative o modo de manutenção, se não for necessário, para liberar mais capacidade. Considere aumentar o valor de **Número Máximo de Sessões** na configuração da política Citrix para permitir mais sessões por VDA de servidor. Considere adicionar mais VDAs de SO de múltiplas sessões. Considere adicionar mais VDAs

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
			de SO de sessão única.
[5] Configuração	[14] Protocolo Não Permitido	Os protocolos ICA e RDP não são permitidos.	Execute o comando PowerShell **Get-BrokerAccessPolicyRule** no delivery controller e verifique se o valor de **AllowedProtocols** lista todos os protocolos desejados. Este problema ocorre apenas se houver uma configuração incorreta.
[5] Configuração	[15] Recurso Indisponível	O aplicativo ou desktop ao qual o usuário está tentando se conectar não está disponível. Este aplicativo ou desktop pode não existir, ou não há VDAs disponíveis para executá-lo. Causas possíveis: O aplicativo ou desktop foi despublicado, ou os VDAs que hospedam o aplicativo ou desktop atingiram a carga máxima, ou o aplicativo ou desktop está definido em modo de manutenção.	Verifique se o aplicativo ou desktop ainda está publicado e se os VDAs não estão em modo de manutenção. Determine se os VDAs de SO de múltiplas sessões estão com carga total. Se sim, provisione mais VDAs de SO de múltiplas sessões. Verifique se há VDAs de SO de sessão única disponíveis para conexões. Provisione mais VDAs de SO de sessão única, se necessário.

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[5] Configuração	[16] ActiveSessionReconnectDisabled	A sessão ICA está ativa e conectada a um endpoint diferente. No entanto, como a **Reconexão de Sessão Ativa** está desabilitada, o cliente não consegue se conectar à sessão ativa.	No controlador de entrega, verifique se a **Reconexão de Sessão Ativa** está habilitada. Verifique se o valor de **DisableActiveSessionReconnect** no registro, em **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server**, está definido como 0.
[2] MachineFailure	[17] NoSessionToReconnect	O cliente tentou se reconectar a uma sessão específica, mas a sessão foi encerrada.	Tente novamente a reconexão do controle de workspace.
[2] MachineFailure	[18] SpinUpFailed	O VDA não pode ser ligado para o lançamento da sessão. Este é um problema relatado pelo hypervisor.	Se a máquina ainda estiver desligada, tente iniciá-la a partir do Citrix Studio. Se isso falhar, revise a conectividade e as permissões do hypervisor. Se o VDA for uma máquina provisionada por PVS, verifique no console PVS se a máquina está em execução. Caso contrário, verifique se a máquina tem um Personal vDisk atribuído, faça login

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
			no hypervisor para redefinir a VM.
[2] MachineFailure	[19] Refused	O controlador de entrega envia uma solicitação ao VDA para se preparar para uma conexão de um usuário final, mas o VDA recusa ativamente essa solicitação.	Verifique via ping se o delivery controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas de firewall ou roteamento de rede.
[2] Falha da Máquina	[20] Falha de ConfigurationSet	O delivery controller não enviou os dados de configuração necessários, como configurações de política e informações de sessão, para o VDA durante o lançamento da sessão. Causas possíveis: Problemas de comunicação entre o controller e o VDA, problemas encontrados pelo Serviço Broker ao criar uma solicitação de conjunto de configuração, ou problemas de rede que resultam na não aceitação da solicitação pelo VDA.	-

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
[3] NenhumaCapacidadeDisponível	[21] MaxTotalInstancesExcedido	O número máximo de instâncias de um aplicativo foi atingido. Nenhuma instância adicional do aplicativo pode ser aberta no VDA. Este problema está relacionado ao recurso de limites de aplicativo.	Considere aumentar a configuração do aplicativo, **Limitar o número de instâncias em execução ao mesmo tempo**, para um valor mais alto, se o licenciamento permitir.
[3] NenhumaCapacidadeDisponível	[22] MaxPerUserInstancesExcedido	O usuário está tentando abrir mais de uma instância de um aplicativo, mas o aplicativo está configurado para permitir apenas uma única instância do aplicativo por usuário. Este problema está relacionado ao recurso de limites de aplicativo.	Apenas uma instância do aplicativo é permitida por usuário por padrão. Se várias instâncias por usuário forem necessárias, considere desmarcar a configuração **Limitar a uma instância por usuário** nas configurações do aplicativo.
[1] FalhaDeConexãoDoCliente	[23] Erro de comunicação	O delivery controller tentou enviar informações ao VDA, como uma solicitação para se preparar para uma conexão, mas ocorreu um erro durante a tentativa de comunicação. Isso pode ser	Se já iniciado, reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verifique se o VDA se registra com sucesso. Confirme se os controladores de entrega configurados para o VDA estão corretos através dos detalhes

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
		causado por interrupções na rede.	no log de eventos do aplicativo.
[3] NoCapacityAvailable	[100] NoMachineAvailable O serviço de monitoramento converte [12] NoDesktopAvailable para este código de erro.	O VDA atribuído para iniciar a sessão está em um estado inválido ou indisponível. Causas possíveis: O estado de energia do VDA é desconhecido ou indisponível, o VDA não reiniciou desde a última sessão do usuário, o compartilhamento de sessão está desabilitado enquanto a sessão atual exige que ele esteja habilitado, ou o VDA foi removido do grupo de entrega ou do site.	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se há VDAs suficientes registrados e em estado pronto para poder iniciar o desktop compartilhado publicado ou o aplicativo solicitado pelo usuário. Verifique se o hipervisor que hospeda o VDA não está em modo de manutenção.
[2] MachineFailure	[101] MachineNotFunctional. O serviço de monitoramento converte [12] NoDesktopAvailable para este código de erro.	O VDA não está operacional. Causas possíveis: O VDA foi removido do grupo de entrega, o VDA está não registrado, o estado de energia do VDA está indisponível, ou o VDA está enfrentando problemas internos.	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se o VDA aparece como ligado no Citrix Studio. Se o estado de energia for desconhecido para várias máquinas, resolva quaisquer problemas de conectividade com o hipervisor ou falhas

CATEGORIA	MOTIVO	PROBLEMA	AÇÃO
			do host. Verifique se o hipervisor que hospeda o VDA não está em modo de manutenção. Reinicie o VDA assim que esses problemas forem resolvidos.

Tipo de falha da máquina

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
Desconhecido	-	-	-
Não registrado	3	-	-
Capacidade Máxima (representada como Carga Máxima no Director)	4	A máquina está se reportando com capacidade máxima, ou seja, Índice de Carga Máxima	Certifique-se de que todos os hipervisores estejam ligados. Adicione mais máquinas aos Delivery Groups afetados, adicionando mais capacidade ao hipervisor ou adicionando mais hipervisores.
StuckOnBoot	2	A VM não concluiu sua sequência de inicialização e não está se comunicando com o hipervisor.	Certifique-se de que a VM inicializou com sucesso no hipervisor. Verifique outras mensagens na VM, como problemas de SO. Certifique-se de que as ferramentas do

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			hipervisor estejam instaladas na VM. Certifique-se de que o VDA esteja instalado na VM.
FailedToStart	1	A VM encontrou problemas ao tentar iniciar no hipervisor.	Verifique os logs do hipervisor.
Nenhum	0	-	-

Motivo da desativação da máquina (aplicável quando o tipo de falha é Não Registrado ou Desconhecido)

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
AgentShutdown	0	O VDA passou por um desligamento normal.	Ligue o VDA se você não espera que ele esteja desligado com base nas políticas de gerenciamento de energia existentes. Revise quaisquer erros nos logs de eventos.
AgentSuspended	1	O VDA está em hibernação ou modo de suspensão.	Tire o VDA do modo de hibernação. Considere desabilitar a hibernação para VDAs do Citrix Virtual Apps and Desktops através das configurações de energia.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
IncompatibleVersion	100	O VDA não consegue se comunicar com o delivery controller devido a uma incompatibilidade nas versões do protocolo Citrix.	Alinhe as versões do VDA e do delivery controller.
AgentAddressResolutionFailed	101	O delivery controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta de máquina do VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão corretos. Caso contrário, corrija-os. Se for generalizado, valide as configurações de DNS nos delivery controllers. Verifique a resolução de DNS a partir do controller executando o comando `nslookup`.
[Cloud]:AgentAddressResolutionFailed	101	O delivery controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta de máquina do VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão corretos. Caso contrário, corrija-os.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
AgentNotContactable	102	Ocorreu um problema de comunicação entre o delivery controller e o VDA.	Use um ping para verificar se o delivery controller e o VDA podem se comunicar com êxito. Caso contrário, resolva quaisquer problemas de firewall ou de rede. Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA.
[Cloud]: AgenteNãoContactável	102	Ocorreu um problema de comunicação entre o delivery controller e o VDA.	Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			(CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA. Entre em contato com o suporte da Citrix.
AgentWrongActiveDirectoryOU	103	Ocorreu uma configuração incorreta de descoberta do Active Directory. A OU específica do site (onde as informações do controlador do site são armazenadas no AD) configurada no registro do VDA é para um site diferente.	Certifique-se de que a configuração do Active Directory esteja correta ou verifique as configurações do registro.
EmptyRegistrationRequest	104	A solicitação de registro enviada do VDA para o delivery controller estava vazia. Isso pode ser devido a uma instalação de software VDA corrompida.	Reinicie o serviço Desktop no VDA para reiniciar o processo de registro e verifique se o VDA se registra corretamente por meio do log de eventos do aplicativo.
MissingRegistrationCapabilities	105	A versão do VDA não é compatível com o delivery controller.	Atualize o VDA ou remova o VDA e reinstale-o.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
MissingAgentVersion	106	A versão do VDA não é compatível com o delivery controller.	Reinstale o software VDA se o problema estiver afetando todas as máquinas.
InconsistentRegistrationCapabilities	107	O VDA não consegue comunicar suas capacidades ao Broker. Isso pode ser devido à incompatibilidade entre as versões do VDA e do delivery controller. As capacidades de registro, que mudam a cada versão, são expressas em um formato que não corresponde à solicitação de registro.	Alinhe as versões do VDA e do delivery controller.
NotLicensedForFeature	108	O recurso que você está tentando usar não está licenciado.	Verifique sua edição de licenciamento Citrix ou remova o VDA e reinstale-o.
[Cloud]: NotLicensedForFeature	108	O recurso que você está tentando usar não está licenciado.	Entre em contato com o suporte da Citrix.
Versão de segurança de credencial não suportada	109	O VDA e o controlador de entrega não estão usando o mesmo mecanismo de criptografia.	Alinhe as versões do VDA e do controlador de entrega.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
Solicitação de Registro Inválida	110	O VDA fez uma solicitação de registro ao Broker, mas o conteúdo da solicitação está corrompido ou é inválido.	Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Solução de problemas de registro do Virtual Delivery Agent com controladores de entrega no Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA.
Incompatibilidade de Sessão Única/ Múltipla	111	O tipo de sistema operacional do VDA não é compatível com o catálogo de máquinas ou grupo de entrega.	Adicione o VDA ao tipo de catálogo de máquinas ou grupo de entrega correto que contenha máquinas com o mesmo sistema operacional.
FunctionalLevelTooLowForCatalog	112	O catálogo de máquinas está configurado para um nível funcional de VDA superior à versão do VDA instalada.	Verifique se o nível funcional do catálogo de máquinas do VDA corresponde ao do VDA. Atualize ou faça o downgrade do catálogo de máquinas para corresponder ao do VDA.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
FunctionalLevelTooLowForDesktopGroup	113	O grupo de entrega está configurado para um nível funcional de VDA superior à versão do VDA instalada.	Verifique se o nível funcional do grupo de entrega do VDA corresponde ao do VDA. Atualize ou faça o downgrade do catálogo de máquinas para corresponder ao do VDA.
PowerOff	200	O VDA não foi desligado corretamente.	Se o VDA deveria estar ligado, tente iniciar o VDA a partir do Citrix Studio e verifique se ele inicializa e se registra corretamente. Solucione quaisquer problemas de inicialização ou registro. Revise os logs de eventos no VDA assim que ele estiver novamente ativo para ajudar a determinar a causa raiz do desligamento.
AgentRejectedSettingsUpdate	203	Configurações como políticas do Citrix foram alteradas ou atualizadas, mas houve um erro ao enviar as atualizações para o VDA. Isso pode ocorrer se as	Atualize o VDA se necessário. Verifique se as atualizações aplicadas são compatíveis com a versão do VDA.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		atualizações forem incompatíveis com a versão do VDA instalada.	
SessionPrepareFailure	206	O Broker não concluiu uma auditoria das sessões em execução no VDA.	Se generalizado, reinicie o Citrix Broker Service no delivery controller.
[Cloud]: SessionPrepareFailure	206	O Broker não concluiu uma auditoria das sessões em execução no VDA.	Entre em contato com o suporte da Citrix.
ContactLost	207	O delivery controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções de rede.	Verifique se o Citrix Broker Service está em execução no delivery controller e se o Desktop service está em execução no VDA. Inicie cada um se estiverem parados. Se já estiverem iniciados, reinicie o Desktop service no VDA para reiniciar o processo de registro e verifique se o VDA se registra com sucesso. Confirme se os delivery controllers configurados para o VDA estão corretos através dos detalhes no log de eventos do

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			Aplicativo. Use um ping para verificar se o delivery controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva quaisquer problemas de firewall ou rede.
[Cloud]: ContactLost	207	O controlador de entrega perdeu a conexão com o VDA. Isso pode ser causado por interrupções de rede.	Verifique se o serviço Desktop está em execução no VDA. Inicie-o se estiver parado.
BrokerRegistrationLimitReached	301	O controlador de entrega atingiu o número máximo configurado de VDAs que podem se registrar simultaneamente com ele. Por padrão, o controlador de entrega permite 10.000 registros simultâneos de VDA.	Considere adicionar controladores de entrega ao Site ou criar um Site. Você também pode aumentar o número de VDAs permitidos para se registrar simultaneamente com o controlador de entrega por meio da chave de registro **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers**. Consulte o artigo da Central de Conhecimento, Entradas da Chave de Registro Usadas pelo Citrix Virtual Apps and Desktops

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
			(CTX117446) para obter mais informações. Aumentar esse número pode exigir mais recursos de CPU e memória para o controlador.
SettingsCreationFailure	208	O Broker não construiu um conjunto de configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falhará e o VDA ficará não registrado.	Verifique os logs de eventos no controlador de entrega em busca de erros. Reinicie o Serviço Broker se um problema específico não for evidente nos logs. Depois que o Serviço Broker for reiniciado, reinicie o serviço Desktop nos VDAs afetados e verifique se eles se registram com sucesso.
[Cloud]: SettingsCreationFailure	208	O Broker não construiu um conjunto de configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falhará e o VDA ficará não registrado.	Reinicie o serviço Desktop nos VDAs afetados e verifique se eles se registram com sucesso. Entre em contato com o suporte da Citrix.
SendSettingsFailure	204	O Broker não enviou as configurações e	Se limitado a um único VDA, reinicie o

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
		os dados de configuração para o VDA. Se o Broker puder coletar os dados, mas não conseguir enviá-los, o registro falhará.	serviço Desktop no VDA para forçar o novo registro e valide se o VDA se registra com sucesso através do log de eventos do aplicativo. Solucione quaisquer erros observados. Consulte as etapas de solução de problemas listadas no artigo da Central de Conhecimento, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para problemas comuns que causam problemas de comunicação entre o controlador e o VDA.
AgentRequested	2	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.
DesktopRestart	201	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.
DesktopRemoved	202	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.

CÓDIGO DE ERRO	ID DO CÓDIGO DE ERRO	PROBLEMA	AÇÃO
SessionAuditFailure	205	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.
UnknownError	300	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.
RegistrationStateMismatch	302	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.
Desconhecido	-	Ocorreu um erro desconhecido.	Entre em contato com o suporte da Citrix.

Integração do Secure Private Access com o Director (Prévia)

A integração do Secure Private Access com o Director permite que o administrador de help desk ou o administrador completo monitore e solucione problemas de todas as sessões do Secure Private Access no Director. Para oferecer suporte a esse recurso, você deve usar as versões 2402 ou posteriores do Director, Secure Private Access, Citrix Workspace™ app e VDA.

As ações disponíveis incluem a visualização dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário no pop-up **Selecionar uma Sessão** > guia **Sessões** > **Aplicativos Web SaaS e Cliente/Servidor**
- Enumerações falhas ou bloqueadas do Secure Private Access e inicializações de aplicativos falhas no pop-up **Selecionar uma Sessão** > guia **Acesso Negado**
- Visualização de detalhes da sessão e do aplicativo para inicializações de aplicativos ativas e falhas
- Visualização de detalhes da sessão e do aplicativo para enumerações falhas e bloqueadas

> **Observação:**

> A integração do Secure Private Access com o Director é suportada apenas para autenticação baseada em formulários do Director e não é suportada para Autenticação Integrada do Windows ou autenticação baseada em Smart Card.

Pré-requisitos

1. Para oferecer suporte a esse recurso, você deve usar o seguinte:
   - Director 2402 ou versão posterior
   - Secure Private Access 2402 ou versão posterior
   - Citrix Workspace app 2402 ou versão posterior
2. Certifique-se de que pelo menos um site do Citrix Virtual Apps and Desktops™ esteja configurado no Director.
3. Configurar o Secure Private Access.
4. Certifique-se de que o servidor Director tenha conectividade de rede com o servidor Secure Private Access.

   > **Observação:**
   >
   > Um certificado confiável deve ser instalado no servidor Secure Private Access para estabelecer uma conexão bem-sucedida com o Citrix Director.

5. Certifique-se de que o usuário administrador do Director tenha as seguintes permissões:
   a. Administrador Completo (Full Admin) ou Administrador Somente Leitura (ReadOnly Admin) do Secure Private Access no console de administração do Secure Private Access.
   b. Help desk do Citrix Virtual Apps™ ou Desktops ou Administrador Completo (Full Admin) ou Administrador Somente Leitura (ReadOnly Admin) no console do Citrix Studio.

Configurar o Director com o Secure Private Access

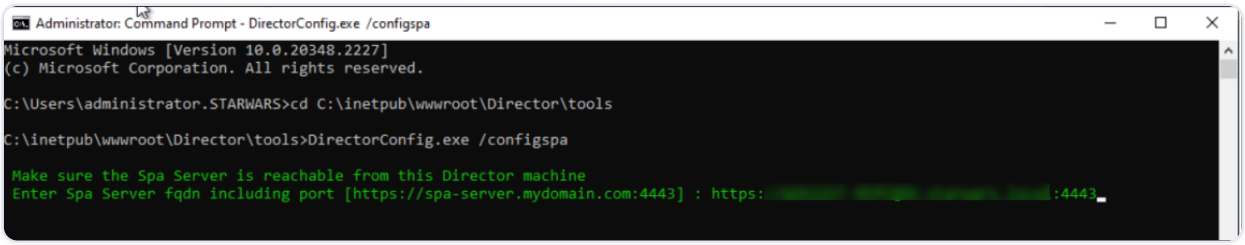
1. Abra um prompt de comando como administrador na máquina onde o Director está instalado.
2. Vá para o caminho da ferramenta `DirectorConfig` executando o seguinte comando:

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Execute o seguinte comando para configurar o Secure Private Access:

```
DirectorConfig.exe /configspa
```

4. Insira o FQDN da máquina onde o Secure Private Access está instalado, juntamente com o número da porta.
5. Certifique-se de que a conexão com o Secure Private Access (servidor ou balanceador de carga) seja segura e tenha um certificado confiável aplicado a ela.



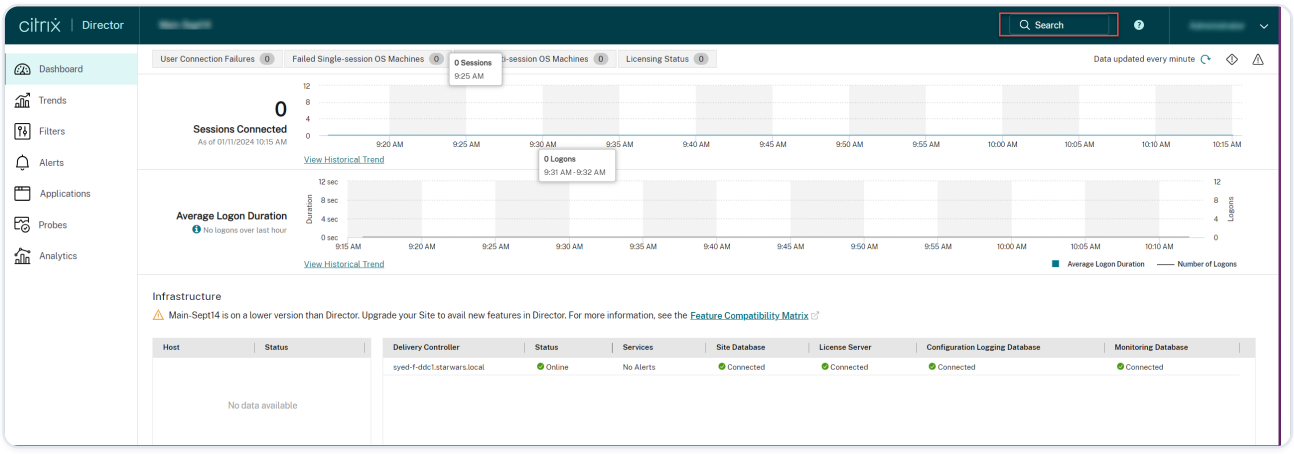
Observação:

Os administradores devem ser adicionados ao console do Secure Private Access para visualizar os detalhes da sessão do Secure Private Access no Director. Para obter mais informações, consulte Gerenciar administradores.

Visualizar uma sessão do Secure Private Access por usuário

No painel do Director, clique em **Pesquisar** e insira o nome de usuário. A tela **Selecionar uma sessão** é exibida.

Administrador completo:



Administrador de help desk:

Administrador de suporte técnico do SPA do Director(/en-us/citrix-virtual-apps-desktops/2407/media/director-spa-helpdesk-admin-user-access.png)

Visualizar o Gerenciador de Atividades para a sessão do Secure Private Access

O Citrix Director oferece a visualização do Gerenciador de Atividades para sessões do Secure Private Access, que fornece uma visão geral das atividades da sessão. O Gerenciador de Atividades oferece uma visão abrangente de todos os aplicativos e desktops que foram abertos com sucesso, que falharam ao abrir e o resultado das políticas definidas no aplicativo Secure Private Access. Este recurso está disponível a partir do Citrix Virtual Apps and Desktops versão 2407 ou posterior.

Pré-requisitos:

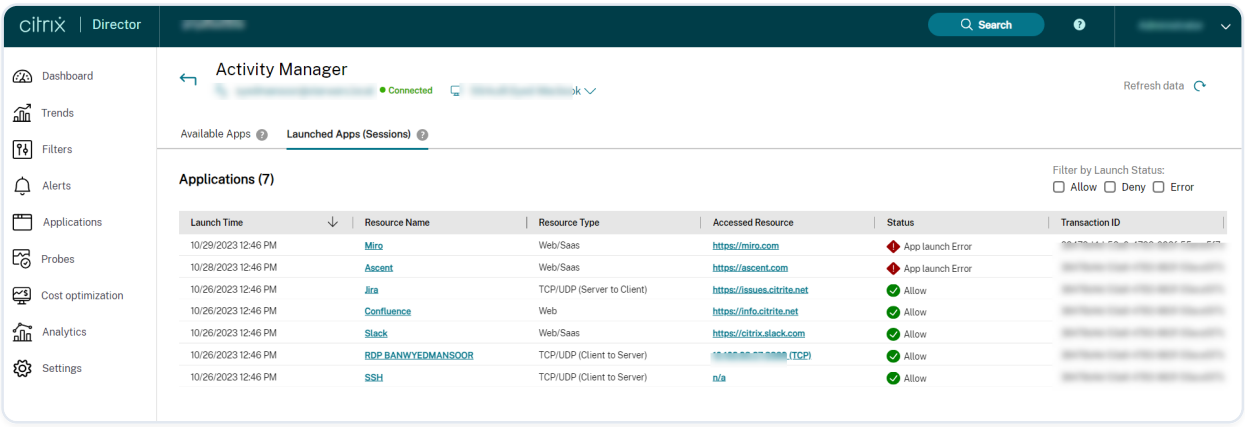
- Director 2407 ou versão posterior
- Secure Private Access 2407 ou versão posterior

O Gerenciador de Atividades é exibido com os detalhes de **Aplicativos Disponíveis** e **Aplicativos Iniciados**. Você pode encontrar os seguintes detalhes da sessão:

- Hora de lançamento
- Nome do recurso
- Tipo de recurso
- Recurso acessado
- Status
- ID da Transação

Para visualizar o Gerenciador de Atividades, faça o seguinte:

1. No painel do Director, clique em **Pesquisar** e insira o nome de usuário. A tela **Selecionar uma sessão** é exibida.
2. Selecione uma sessão que foi aberta usando a sessão do Secure Private Access. O Gerenciador de Atividades para a sessão selecionada é exibido.



3. Clique em **Aplicativos Disponíveis** para visualizar os aplicativos que estão disponíveis no aplicativo Citrix Workspace.

Ou,

Clique em **Aplicativos Iniciados (sessões)** para visualizar os aplicativos que foram abertos no aplicativo Citrix Workspace.

Você pode filtrar os recursos com o status do recurso definido no aplicativo Secure Private Access:

- Permitir - Recursos que um usuário tem permissão para acessar. Este status é definido usando uma política no aplicativo Secure Private Access. Este recurso está presente para o usuário no aplicativo Citrix Workspace.
- Negar - Recursos que um usuário não tem permissão para acessar. Este status é definido usando uma política no aplicativo Secure Private Access. Este recurso está presente para o usuário no aplicativo Citrix Workspace.
- Erro - Recursos que um usuário tem permissão para acessar no aplicativo Secure Private Access. No entanto, devido a algum erro, o recurso não está disponível no aplicativo Citrix Workspace. Existem dois tipos de erros: erro de enumeração e erro de sessão.

Visualizar aplicativos disponíveis

Os aplicativos Web e SaaS disponíveis no aplicativo Citrix Workspace são exibidos na seção **Aplicativos Disponíveis**. Esta seção mostra a última tentativa de enumeração dos aplicativos e o status da tentativa de enumeração.

Você pode visualizar os seguintes detalhes:

- Nome do recurso
- Status
- ID da Transação

Você também pode filtrar os detalhes anteriores pelo status do aplicativo, como **Permitir**, **Negar** e **Erro**. Você também pode classificar os detalhes usando as setas para cima e para baixo.

> **Observação:**
>
> Aplicativos TCP/UDP não estão presentes na seção **Aplicativos Disponíveis**.

Visualizar aplicativos iniciados

Os aplicativos que são abertos no aplicativo Citrix Workspace são exibidos na seção **Aplicativos Iniciados (sessões)**. Você pode visualizar os seguintes detalhes:

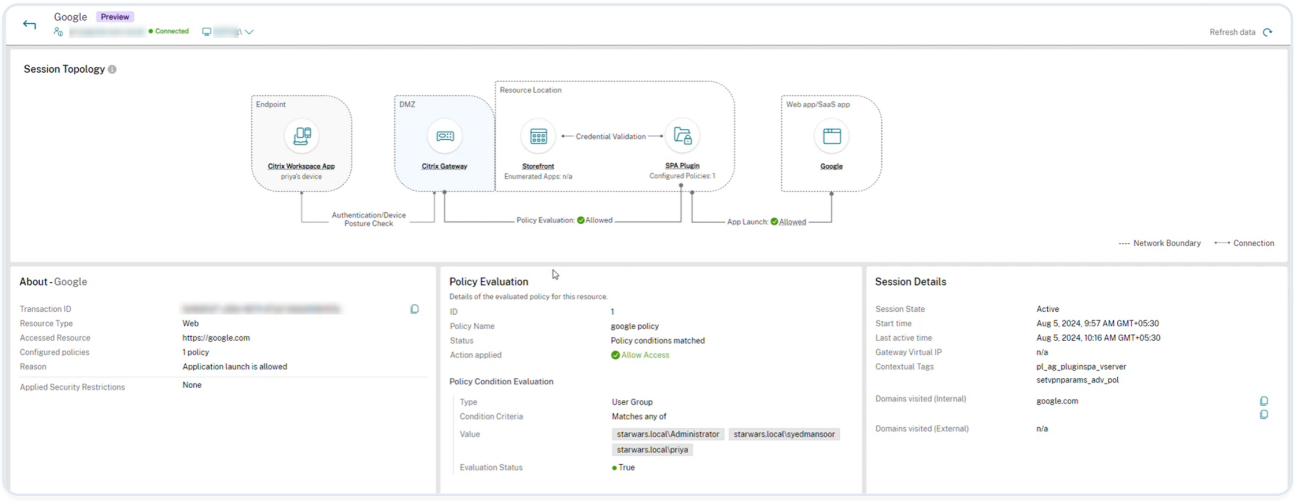
- Hora de início
- Nome do recurso
- Tipo de recurso
- Recurso acessado
- Status
- ID da Transação

Você também pode filtrar os detalhes anteriores pelo status do aplicativo, como **Permitir**, **Negar** e **Erro**. Você também pode classificar os detalhes usando as setas para cima e para baixo.

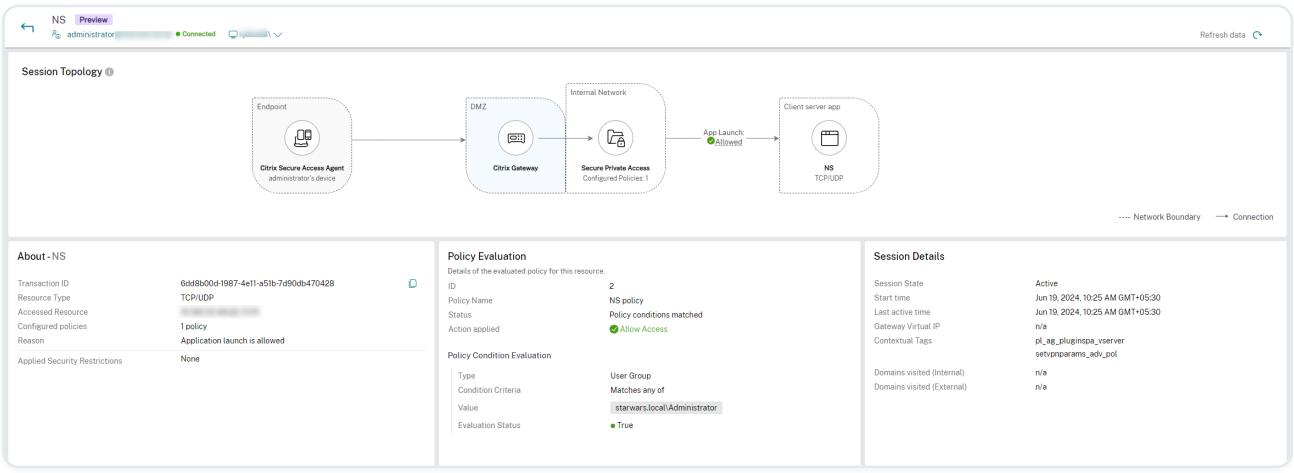
Visualização da topologia da sessão para aplicativos Secure Private Access

Você pode visualizar a topologia de sessão para os aplicativos abertos usando o Secure Private Access. Clique no aplicativo desejado no **Gerenciador de Atividades** para visualizar a Topologia de Sessão do aplicativo selecionado.

Aplicativos Web/SaaS:



Aplicativos TCP/UDP:



Topologia de Sessão

A visualização da Topologia de Sessão fornece o fluxo do processo de inicialização do aplicativo. O endpoint se conecta ao Citrix Gateway e o Citrix Gateway se conecta ao plug-in do Secure Private Access. Usando as informações do plug-in do Secure Private Access, o aplicativo é iniciado. Este recurso está disponível a partir do Citrix Virtual Apps and Desktops versão 2407 ou posterior.

Pré-requisitos:

- Director 2407 ou versão posterior
- Secure Private Access 2407 ou versão posterior
- Citrix Secure Access 24.8.1.x ou versão posterior

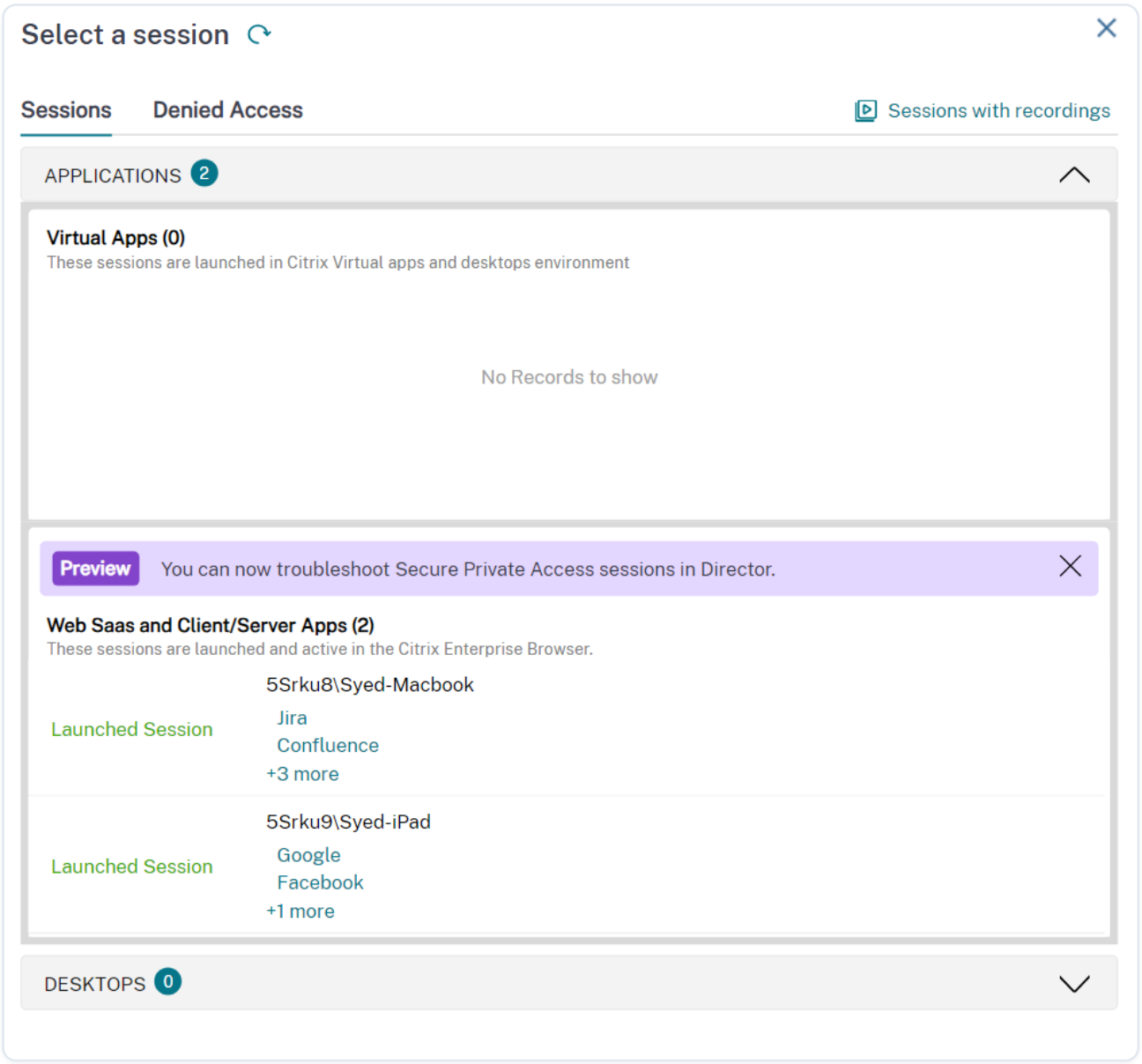
Você pode visualizar o seguinte:

- Endpoint - Exibe o endpoint onde o aplicativo é aberto. As opções possíveis são Citrix Workspace app e Citrix Secure Agent. O ID do dispositivo é exibido.

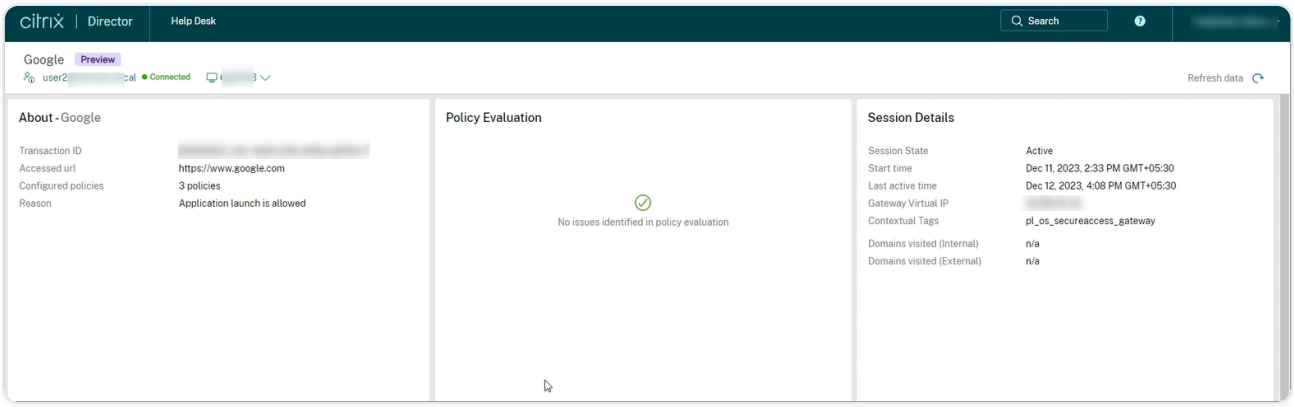
- Rede interna - Exibe o número de aplicativos enumerados e o número de políticas configuradas.
- Avaliação de política - Exibe o resultado da política definida no aplicativo Secure Private Access. Os diferentes valores são **Permitido**, **Negado**, **Acesso permitido com restrições** e **Erro**. Isso é aplicável apenas para aplicativos Web ou SaaS.
- Aplicativo iniciado - Exibe o tipo de aplicativos e o status de inicialização do aplicativo. Os valores possíveis para tipos de aplicativo são aplicativo Web/SaaS ou aplicativo TCP/UDP. Da mesma forma, os valores possíveis para status de inicialização de aplicativo são **Permitido**, **Negado**, **Acesso permitido com restrições** e **Erro**.

Visualizar aplicativos Web e SaaS iniciados com sucesso

Os aplicativos iniciados com sucesso são exibidos na seção **Aplicativos Web SaaS e Cliente/ Servidor**.



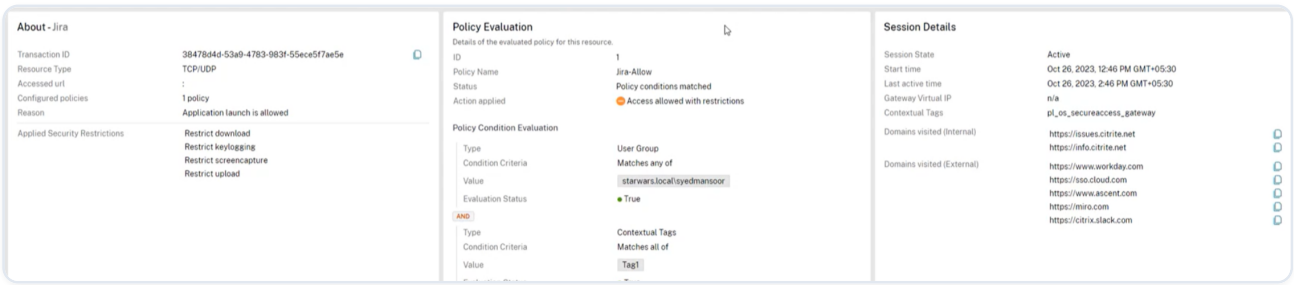
Clique em um aplicativo na seção **Aplicativos Web SaaS e Cliente/Servidor** para visualizar os detalhes.



Para obter mais informações sobre códigos de sucesso, consulte Códigos relacionados ao Citrix Director.

Visualizar detalhes sobre os aplicativos com acesso negado

Clique em **Verificar Detalhes de Acesso** na tela **Selecionar uma sessão**.



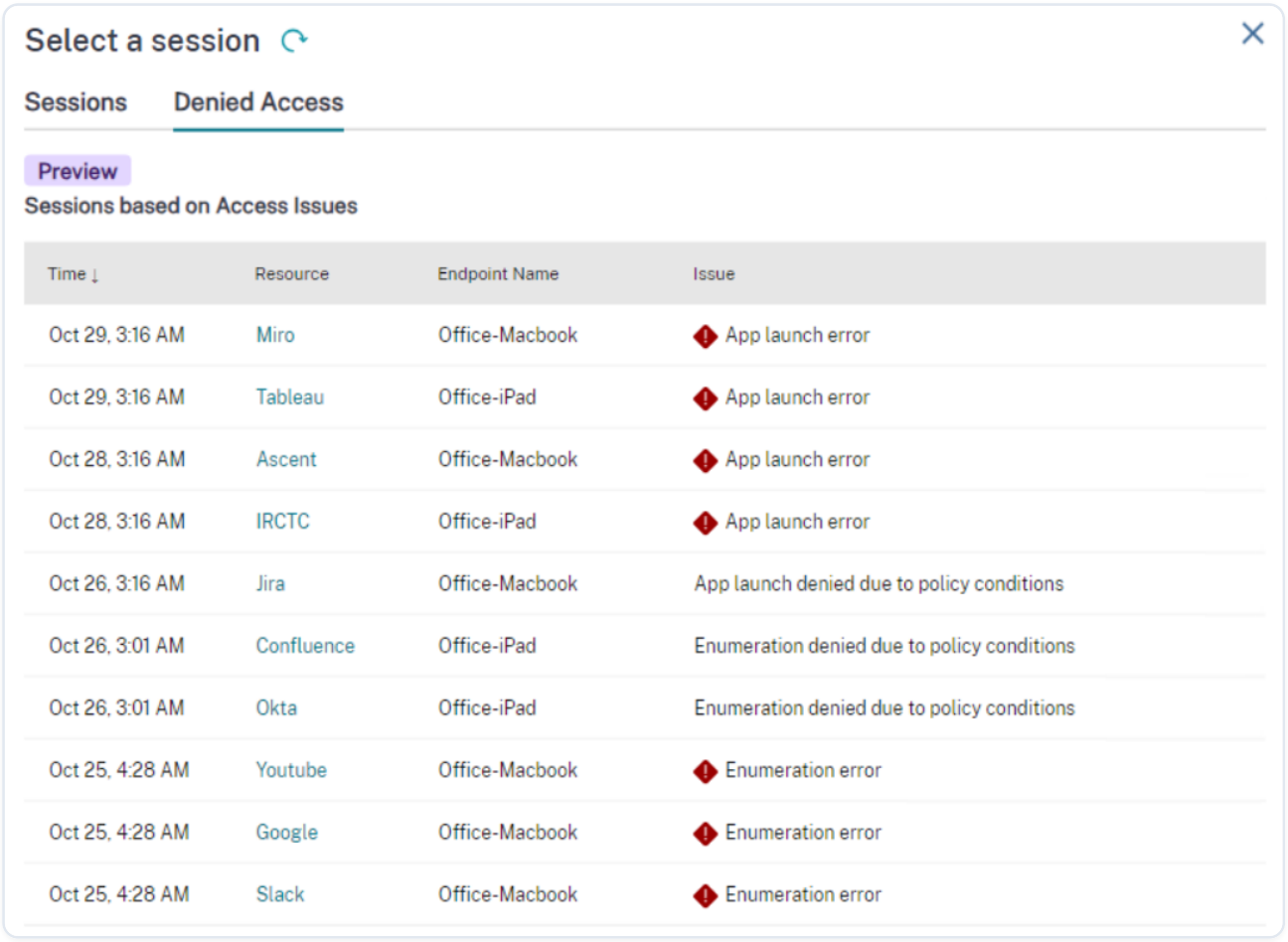
> **Observação:**

> O botão **Verificar Detalhes de Acesso** aparece quando não há uma sessão ativa.

> Ou,

Clique na guia **Acesso Negado** para visualizar os aplicativos cujo acesso foi negado.

A guia **Acesso Negado** é aberta.

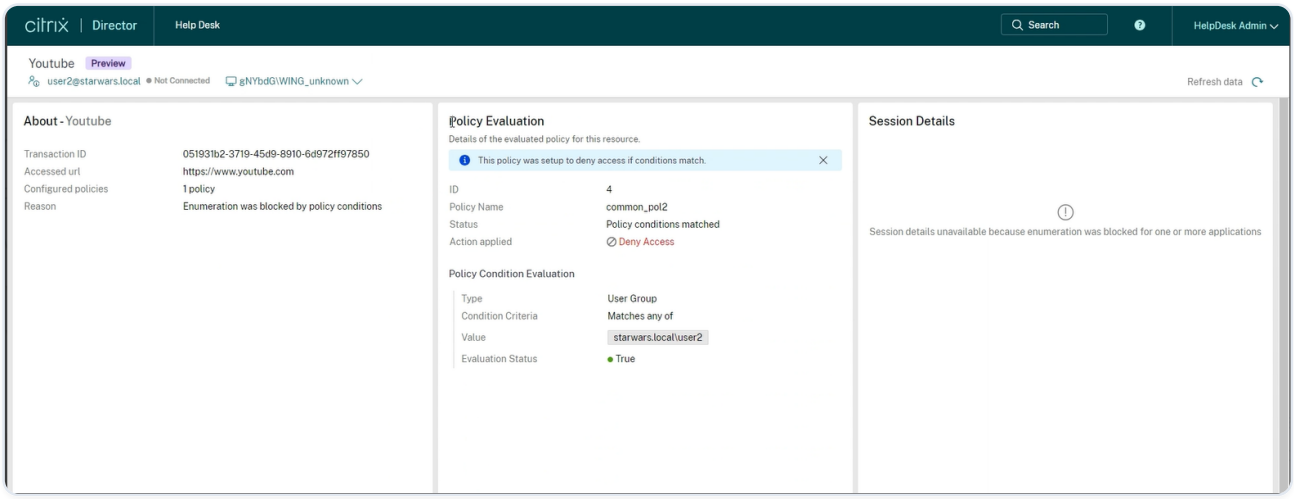


Os detalhes da sessão, como hora, recurso, nome do endpoint e motivo da falha, são exibidos. Para obter mais informações sobre códigos de erro, consulte Códigos relacionados ao Citrix Director.

Atualmente, os seguintes problemas são identificados:

- Enumeração negada devido às condições da política
- Erro de inicialização do aplicativo
- Erros de enumeração
- Inicialização do aplicativo negada devido às condições da política

Selecione um aplicativo na guia **Acesso Negado** > coluna **Recurso** para visualizar os detalhes:



Os seguintes detalhes são exibidos para as sessões bem-sucedidas ou com falha:

- Sobre o aplicativo
- Avaliação da política
- Detalhes da sessão

Sobre o aplicativo

O nome do aplicativo bem-sucedido, com falha ou negado é exibido. Juntamente com ele, os seguintes detalhes do aplicativo para o sucesso ou falha são exibidos:

CAMPO	DESCRIÇÃO
ID da Transação	ID de Transação Citrix durante a sessão ou enumeração.
Tipo de Recurso	Exibe o tipo de recurso. Os valores possíveis são Web, SaaS, TCP/UDP (Servidor para Cliente) e TCP/UDP (Cliente para Servidor).
Recurso Acessado	A URL do recurso acessado durante a sessão ou enumeração. No caso de um aplicativo TCP ou UDP, ele mostra se o tipo de recurso acessado é TCP ou UDP.
Políticas configuradas	O número de políticas que são usadas em uma sessão ou enumeração.
Motivo	A análise da sessão ou atividade de enumeração.

CAMPO	DESCRIÇÃO
Restrições de Segurança Aplicadas	Exibe as restrições de segurança aplicadas no aplicativo Secure Private Access.

Avaliação da política

Exibe que nenhum problema foi encontrado durante a avaliação para uma sessão bem-sucedida. Para uma sessão ou enumeração com falha, os seguintes detalhes das políticas avaliadas são exibidos:

CAMPO	DESCRIÇÃO
ID	ID de Transação Citrix.
Nome da Política	O nome da política. Se houver várias políticas, a primeira política que corresponder à condição definida será exibida.
Status	O status da política.
Ação aplicada	A ação aplicada à política. Por exemplo, negar acesso.
Avaliação da Condição da Política	
Tipo	O tipo da condição da política.
Critérios da Condição	Os critérios de condição da política aplicada na sessão ou enumeração com falha.
Valor	O valor da política.
Status da Avaliação	O status de avaliação da política. Os diferentes valores são **Permitido**, **Negado**, **Acesso permitido com restrições** e **Erro**.

Detalhes da sessão

Para uma sessão com falha, o motivo da falha da sessão é exibido. Para uma sessão bem-sucedida, os seguintes detalhes são exibidos:

CAMPO	DESCRIÇÃO
Estado da Sessão	Exibe o estado da sessão, seja ela ativa ou inativa.
Hora de início	Exibe a hora de início da sessão.
Última hora ativa	Exibe a última hora ativa da sessão bem-sucedida.
IP Virtual do Gateway	Exibe o endereço IP virtual do gateway ao qual a sessão bem-sucedida está conectada.
Tags Contextuais	Exibe as tags contextuais. A tag contextual no plug-in do Secure Private Access é o nome de uma política do NetScaler® Gateway (sessão, pré-autenticação, EPA) que é aplicada às sessões dos usuários autenticados.
Domínios visitados (Internos)	Exibe os domínios internos acessados usando a sessão bem-sucedida.
Domínios visitados (Externos)	Exibe os domínios externos acessados usando a sessão bem-sucedida.

Problemas conhecidos

- No caso de um aplicativo TCP ou UDP, os detalhes da enumeração não são exibidos na página **Gerenciador de Atividades**.
- Você pode notar que as sessões encerradas estão disponíveis como ativas no pop-up **Seletor de Sessão**.

SDKs e APIs

Vários SDKs e APIs estão disponíveis nesta versão. Para acessar os SDKs e APIs, vá para Crie qualquer coisa com Citrix. A partir daí, selecione **Citrix Workspace** para acessar informações de programação para Citrix Virtual Apps and Desktops e seus componentes relacionados.

> **Observação:**
>
> O SDK do Citrix Virtual Apps and Desktops™ e o SDK da Política de Grupo do Citrix podem ser instalados como um módulo ou um snap-in. Vários SDKs de componentes (como Citrix Licensing, Citrix Provisioning e StoreFront) são instalados usando apenas um snap-in.

> Este produto oferece suporte às versões 3 a 5 do PowerShell.

SDK do Citrix Virtual Apps and Desktops

Este SDK é instalado automaticamente como um módulo do PowerShell quando você instala um Delivery Controller™ ou o Studio. Isso permite que você use os cmdlets deste SDK sem precisar adicionar snap-ins. (As instruções são fornecidas abaixo se você optar por instalar este SDK como um snap-in.)

Permissões

Você deve executar o shell ou script usando uma identidade que tenha direitos de administração Citrix. Embora os membros do grupo de administradores locais no Controller tenham automaticamente privilégios administrativos completos para permitir a instalação do Citrix Virtual Apps ou Citrix Virtual Desktops™, a Citrix recomenda que, para operação normal, você crie administradores Citrix com os direitos apropriados, em vez de usar a conta de administradores locais.

Acessar e executar os cmdlets

1. Inicie um shell no PowerShell: Abra o Studio, selecione a guia **PowerShell** e clique em **Launch PowerShell**.

2. Para usar cmdlets do SDK em scripts, defina a política de execução no PowerShell. Para obter informações sobre a política de execução do PowerShell, consulte a documentação da Microsoft.
3. Se você quiser usar o snap-in (em vez do módulo), adicione o snap-in usando o cmdlet `Add-PSSnapin` (ou `asnp`).

   V1 e V2 denotam a versão do snap-in. Os snap-ins do XenDesktop 5 são a versão 1. Os snap-ins do Citrix Virtual Apps and Desktops e das versões anteriores do XenDesktop 7 são a versão 2. Por exemplo, para instalar o snap-in do Citrix Virtual Apps and Desktops, digite `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Para importar todos os cmdlets, digite: `Add-PSSnapin Citrix.*.Admin.V*`

Agora você pode usar os cmdlets e os arquivos de ajuda.

- Para acessar os arquivos de ajuda para este SDK, selecione o produto ou componente na lista Categorias e, em seguida, selecione **Citrix Virtual Apps and Desktops SDK**.
- Para obter orientação sobre o PowerShell, consulte Windows PowerShell Integrated Scripting Environment (ISE).

SDK da Política de Grupo

O SDK da Política de Grupo do Citrix permite exibir e configurar as configurações e filtros da Política de Grupo. Este SDK usa um provedor do PowerShell para criar uma unidade virtual que corresponde às configurações e filtros da máquina e do usuário. O provedor aparece como uma extensão para `New-PSDrive`.

Para usar o SDK da Política de Grupo, o Studio ou o SDK do Citrix Virtual Apps and Desktops deve estar instalado.

O provedor PowerShell de Política de Grupo da Citrix está disponível como um módulo ou um snap-in.

- Para usar o módulo, nenhum trabalho adicional é necessário.
- Para adicionar o snap-in, digite `Add-PSSnapin citrix.common.grouppolicy`.

Para acessar a ajuda, digite: `help New-PSDrive -path localgpo:/`.

Para criar uma unidade virtual e carregá-la com configurações, digite `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` onde a string do

Controller é o nome de domínio totalmente qualificado de um Controller no site ao qual você deseja se conectar e carregar as configurações.

APIs REST do Citrix Virtual Apps and Desktops

Com as APIs REST do Citrix Virtual Apps and Desktops, você pode automatizar o gerenciamento de recursos em uma implantação do Citrix Virtual Apps and Desktops.

As APIs REST do Citrix Virtual Apps and Desktops estão disponíveis em `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>`. As APIs não aplicáveis ao Citrix Virtual Apps and Desktops são marcadas de acordo. Siga as orientações para configurar o acesso ao serviço de API e usar as APIs para gerenciar e otimizar seus recursos.

OData do Serviço de Monitoramento

A API Monitor permite o acesso aos dados do Serviço de Monitoramento usando a Versão 3 ou 4 da API OData. Você pode criar painéis de monitoramento e relatórios personalizados com base nos dados consultados do Serviço de Monitoramento. O OData V.4 é baseado na API Web ASP.NET e oferece suporte a consultas de agregação.

Para obter mais informações, consulte a API OData do Serviço de Monitoramento.

__index__

Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site.

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar por gráficos de tendências, ampliando um período de tempo (clicando em um ponto de dados no gráfico) e detalhando para ver os detalhes associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que é afetado.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

Escolha um período para o qual você precisa das informações de tendências históricas. A disponibilidade do período depende da sua implantação do Director da seguinte forma:

- Relatórios de tendências de até Último ano (365 dias) estão disponíveis em sites com licença Premium.
- Relatórios de tendências de até Último mês (31 dias) estão disponíveis em sites com licença Advanced.

- Relatórios de tendências de até Últimos 7 dias em sites com licença não Premium e não Advanced.

Observação:

- Em todas as implantações do Director, as informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Último mês (**Terminando agora**) ou menor. Para o período escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendências estão disponíveis como gráficos e não como tabelas.
- Os valores de retenção de limpeza do Serviço de Monitoramento controlam a disponibilidade dos dados de tendências. Os valores padrão estão disponíveis em Granularidade e retenção de dados. Clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção.
- Os seguintes parâmetros no Gerenciador do IIS controlam o intervalo de datas de término personalizadas disponíveis para seleção. No entanto, a disponibilidade dos dados para as datas selecionadas depende da configuração de retenção de limpeza para a métrica específica que está sendo medida.

PARÂMETRO	VALORES PADRÃO
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

Tendências disponíveis

Exibir tendências para sessões: Na guia **Sessões**, selecione o Grupo de Entrega e o período para visualizar informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas de Confiabilidade da Sessão

ou de Reconexão Automática do Cliente estão em vigor. Quando há uma interrupção de rede no endpoint, as seguintes políticas entram em vigor:

- A confiabilidade da sessão entra em vigor (por padrão, por 3 minutos) onde o Citrix Receiver™ ou o aplicativo Citrix Workspace™ tenta se conectar ao VDA.
- A reconexão automática do cliente entra em vigor entre 3 e 5 minutos, onde o cliente tenta se conectar ao VDA.

Ambas as reconexões são capturadas e exibidas para o usuário. Essas informações podem levar no máximo 5 minutos para aparecer na interface do usuário do Director após a reconexão ter ocorrido.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções. Também analisam redes com uma experiência contínua. Você pode visualizar o número de reconexões para um Grupo de Entrega específico ou período selecionado nos Filtros. Uma análise detalhada fornece informações adicionais, como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Esse recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Esse recurso requer o Delivery Controller™ versão 7 1906 ou posterior e VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações de política de reconexão automática do cliente e Configurações de política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Director pelos seguintes motivos:

- O aplicativo Workspace não está enviando dados de reconexão automática para o VDA.
- O VDA não está enviando dados para o serviço de monitoramento.
- Os Delivery Controllers descartam as cargas úteis do VDA, pois podem não ter as sessões correspondentes.

> **Observação:**

> Às vezes, o endereço IP do cliente pode não ser obtido corretamente se certas políticas do Citrix Gateway estiverem definidas.

> **Ver tendências de falhas de conexão:** Na guia Falhas, selecione a conexão, o tipo de máquina, o tipo de falha, o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em seu site.

Ver tendências de falhas de máquina: Na guia **Falhas de Máquina de SO de Sessão Única** ou na guia Máquinas de SO de Múltiplas Sessões, selecione o tipo de falha, o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre as falhas de máquina em seu site.

Ver tendências de desempenho de logon: Na guia **Desempenho de Logon**, selecione o Delivery Group e o período para visualizar um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em seu site e se o número de logons afeta o desempenho. Esta exibição também mostra a duração média das fases de logon, como duração de corretagem e tempo de inicialização da VM. Esses dados são especificamente para logons de usuário e não incluem usuários tentando se reconectar de sessões desconectadas. A tabela abaixo do gráfico mostra a Duração do Logon por Sessão do Usuário. Você pode escolher as colunas a serem exibidas e classificar o relatório por qualquer uma das colunas. Você também pode exportar esses relatórios para um arquivo .CSV. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

Ver tendências de avaliação de carga: Na guia **Índice do Avaliador de Carga**, visualize um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas de SO de Múltiplas Sessões. As opções de filtro para este gráfico incluem o Delivery Group ou a máquina de SO de Múltiplas Sessões em um Delivery Group, a máquina de SO de Múltiplas Sessões (disponível apenas se a máquina de SO de Múltiplas Sessões em um Delivery Group tiver sido selecionada) e o intervalo.

Ver uso de aplicativos hospedados: A disponibilidade deste recurso depende da licença da sua organização. Na guia **Gerenciamento de Capacidade**, selecione a guia **Uso de Aplicativos Hospedados**. Selecione o Delivery Group e o período para visualizar um gráfico exibindo o pico de uso simultâneo e uma tabela exibindo o uso baseado em aplicativo. Na tabela Uso Baseado em Aplicativo, você pode escolher um aplicativo específico para ver detalhes e uma lista de usuários que estão usando ou usaram o aplicativo.

Ver uso de SO de Sessão Única e Múltiplas Sessões: A exibição Tendências mostra o uso de SO de Sessão Única por site e por Delivery Group. Ao selecionar **Site**, o uso é mostrado por Delivery Group. Ao selecionar Delivery Group, o uso é mostrado por Usuário. A exibição Tendências também mostra o uso de SO de Múltiplas Sessões por site, por Delivery Group e por Máquina. Ao selecionar **Site**, o uso é mostrado por Delivery Group. Ao selecionar Delivery Group, o uso é mostrado por Máquina e por Usuário. Quando Máquina é selecionada, o uso é mostrado por Usuário.

Ver uso de máquina virtual: Na guia **Uso da Máquina**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter uma visualização em tempo real do uso da sua VM, permitindo que você avalie rapidamente as necessidades de capacidade do seu site. Disponibilidade de SO de Sessão Única - exibe o estado atual das máquinas de SO de Sessão Única (VDIs) por disponibilidade para todo o site ou um Delivery Group específico. Disponibilidade de SO de Múltiplas Sessões - exibe o estado atual das máquinas de SO de Múltiplas Sessões por disponibilidade para todo o site ou um Delivery Group específico.

> **Nota:** O número de máquinas exibidas em Contador Disponível inclui máquinas em modo de manutenção.

> **Ver utilização de recursos:** Na guia **Utilização de Recursos**, selecione **Máquinas de SO de Sessão Única ou Máquinas de SO de Múltiplas Sessões** para obter informações sobre dados de tendências históricas para uso de CPU e memória, e IOPS e latência de disco para cada máquina VDI para um melhor planejamento de capacidade. Este recurso requer Delivery Controllers e VDAs **versão 7.11** ou posterior. Os gráficos mostram dados para CPU média, memória média, IOPS médio, latência de disco e pico de sessões simultâneas. Você pode detalhar a máquina e visualizar dados e gráficos para os 10 principais processos que consomem CPU.

Filtre por Delivery Group e Período. Os gráficos de uso de CPU, memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, mês e ano. Os gráficos de IOPS médio e latência de disco estão disponíveis para as últimas 24 horas, mês e ano.

> **Observação:**

> - A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como **Permitido** para coletar e exibir dados na tabela dos 10 Principais

Processos na página Utilização Histórica da Máquina. A política é definida como **Proibido** por padrão. Todos os dados de utilização de recursos são coletados por padrão. Isso pode ser desabilitado usando a configuração da política **Habilitar Monitoramento de Recursos**. A tabela abaixo dos gráficos mostra os dados de utilização de recursos por máquina. Para obter mais informações, consulte Configurações da política de monitoramento.

- O IOPS médio mostra as médias diárias. O IOPS de pico é calculado como o maior das médias de IOPS para o intervalo de tempo selecionado. (Uma média de IOPS é a média horária de IOPS coletados durante a hora no VDA).
- O detalhamento da máquina lista processos com uso médio de CPU ou memória média superior a 1%, o que pode significar que, às vezes, menos de 10 processos são listados.

Ver dados de análise de rede: A disponibilidade deste recurso depende da licença da sua organização e das suas permissões de administrador. Este recurso requer Delivery Controllers **versão 7.11** ou posterior.

Na guia **Rede**, monitore sua análise de rede, que fornece uma visão contextual de usuário, aplicativo e desktop da rede. Com este recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação por meio de relatórios HDX Insight do Citrix ADM. Para obter mais informações, consulte Configurar análise de rede

Visualizar falhas de aplicativo: A guia **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de múltiplas sessões executando Windows Server 2008 e posterior são suportados. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas falhas de aplicativo de VDAs de SO de múltiplas sessões são exibidas. Você pode configurar o monitoramento de falhas de aplicativo usando políticas de Monitoramento. Para obter mais informações, consulte Configurações de política de monitoramento.

Visualizar resultados da sondagem: A guia **Resultados da Sondagem** exibe os resultados da sondagem para aplicativos e desktops que foram configurados para sondagem na página Configuração. Aqui, o estágio de inicialização durante o qual a falha ocorreu é registrado.

Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

Criar relatórios personalizados: A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados em tempo real e históricos do banco de dados de Monitoramento em formato tabular.

Este recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas de Relatório Personalizado salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente, ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique condições de filtro com base em campos como máquina, Grupo de Entrega ou período de tempo. Especifique colunas adicionais necessárias em seu Relatório Personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta de Relatório Personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta de Relatório Personalizado com base em uma consulta OData copiada. Para fazer isso, selecione a opção Consulta OData e cole a consulta OData copiada. Você pode salvar a consulta resultante para execução posterior.

> **Nota:** Os nomes das colunas no relatório de Visualização e Exportação gerado usando consultas OData não são localizados, mas aparecem em inglês.

> Os ícones de bandeira no gráfico indicam eventos ou ações significativas para aquele intervalo de tempo específico. Passe o mouse sobre a bandeira e clique para listar eventos ou ações.

> **Observação:**
>
> - Os dados de logon de conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
> - Os Grupos de Entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros de Tendências do Director até que os dados relacionados a eles sejam removidos. A seleção de um Grupo de Entrega excluído exibe gráficos para os dados disponíveis até a retenção. No entanto, as tabelas não mostram dados.

- Mover uma máquina contendo sessões ativas de um Grupo de Entrega para outro faz com que as tabelas de **Utilização de Recursos e Índice do Avaliador de Carga** do novo Grupo de Entrega exibam métricas consolidadas dos Grupos de Entrega antigo e novo.