



# **Aplicativos e desktops virtuais Citrix 7 2402 LTSR**

## Contents

<b>Citrix Virtual Apps and Desktops 7 2402 Long Term Service Release (LTSR)</b>	<b>3</b>
<b>O que há de novo</b>	<b>4</b>
<b>Atualização cumulativa 1 (CU1)</b>	<b>4</b>
<b>Problemas resolvidos</b>	<b>9</b>
<b>2402 LTSR (versão inicial)</b>	<b>13</b>
<b>Problemas resolvidos</b>	<b>23</b>
<b>Problemas conhecidos</b>	<b>28</b>
<b>Depreciação</b>	<b>33</b>
<b>Requisitos do sistema</b>	<b>51</b>
<b>Instalar e configurar</b>	<b>63</b>
<b>Ambientes de virtualização do Microsoft System Center Virtual Machine Manager</b>	<b>65</b>
<b>Instalar usando a linha de comando</b>	<b>67</b>
<b>Instale o Web Studio</b>	<b>84</b>
<b>Instalar VDAs</b>	<b>91</b>
<b>Instale VDAs usando o SCCM</b>	<b>108</b>
<b>Conexão com a AWS</b>	<b>126</b>
<b>Conexão com o Microsoft Azure</b>	<b>140</b>
<b>Gerenciamento de imagens (prévia)</b>	<b>160</b>
<b>Crie catálogos de máquinas</b>	<b>179</b>
<b>Crie um catálogo da AWS</b>	<b>211</b>
<b>Criar um catálogo do Microsoft Azure</b>	<b>222</b>
<b>Gerenciar catálogos de máquinas</b>	<b>292</b>
<b>Gerencie grupos de entrega</b>	<b>316</b>

<b>Remote PC Access</b>	<b>349</b>
<b>Atualize e migre</b>	<b>367</b>
<b>Atualizar uma implantação</b>	<b>371</b>
<b>Secure HDX (versão prévia)</b>	<b>395</b>
<b>Dispositivos compostos e divisão de dispositivos</b>	<b>398</b>
<b>Configuração de redirecionamento USB herdada</b>	<b>403</b>
<b>Otimização para Microsoft Teams (novo)</b>	<b>408</b>
<b>Otimização do Citrix HDX</b>	<b>411</b>
<b>Otimização do Microsoft SlimCore</b>	<b>417</b>
<b>Otimização para Microsoft Teams (clássico)</b>	<b>422</b>
<b>Tempo limite de sessão dinâmica</b>	<b>467</b>
<b>Configurações</b>	<b>470</b>
<b>Implantação segura do Director</b>	<b>474</b>
<b>Matriz de compatibilidade de recursos</b>	<b>477</b>
<b>Motivo de falhas e solução de problemas no Citrix Director</b>	<b>482</b>
<b>SDKs e APIs</b>	<b>506</b>

## Citrix Virtual Apps and Desktops 7 2402 Long Term Service Release (LTSR)

January 15, 2025

### Importante:

A estratégia de ciclo de vida do produto para versões atuais (CR) e versões de serviço de longo prazo (LTSR) é descrita em [Lifecycle Milestones](#).

O Citrix Virtual Apps and Desktops fornece 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 fornece estabilidade e suporte de longo prazo para as versões do Citrix Virtual Apps and Desktops.

A Atualização Cumulativa 4 (CU4) é a atualização mais recente do 2203 LTSR. 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 componentes e tecnologias nas implantações do Citrix Virtual Apps and Desktops, consulte [Visão geral técnica](#).

### Lançamentos anteriores

A documentação de outras versões atualmente disponíveis está localizada em [Citrix Virtual Apps and Desktops](#).

Para versões ainda mais antigas, a documentação está arquivada em [Legacy Documentation](#).

### Aplicativos e desktops virtuais Citrix no Citrix Cloud

A oferta de aplicativos e desktops virtuais do Citrix Cloud é o Citrix DaaS. Para obter mais informações, consulte [Citrix DaaS](#).

### Links úteis

- [Pacote de suporte Citrix](#)
- [PERGUNTAS FREQUENTES SOBRE LTSR](#)



- [Opções de manutenção do Citrix Virtual Apps and Desktops](#)
- [Datas do ciclo de vida do produto](#)
- [Programa LTSR para o aplicativo Citrix Workspace](#)

## O que há de novo

January 24, 2025

### Sobre este lançamento

A Atualização Cumulativa 1 (CU1) é a atualização mais recente do LTSR 2402.

Sobre a atualização cumulativa [1 \(CU1\)](#)

Sobre [2402 LTSR \(versão inicial\)](#)

## Atualização cumulativa 1 (CU1)

September 11, 2024

Data de lançamento: 20 de agosto de 2024

### Novidades

#### Suporte para autenticação de cartão inteligente

O Web Studio agora oferece suporte à autenticação de cartão inteligente, permitindo que os administradores acessem o Web Studio usando cartões PIV e CAC. Para obter mais informações, consulte [Configurar a autenticação de cartão inteligente para o Web Studio](#).

#### Aprimoramento dos relatórios de telemetria de uso

Com o aprimoramento do recurso de telemetria de uso da licença, os dados de utilização da licença para produtos, componentes e recursos da Citrix implantados nos ambientes gerenciados da Citrix são coletados e processados. Essa implementação é para confirmar a conformidade da licença e que os dados são gerenciados por meio do Citrix License Server. Você deve atualizar para a versão mais

recente do servidor de licenças e ter uma conta do Citrix Cloud. Para obter mais informações, consulte:

- [Telemetria de licenciamento da Citrix] (<https://docs.citrix.com/en-us/licensing/current-release/license-server/licensing-data-collection-programs.html#citrix-licensing-telemetry>)
- [Atualizações necessárias do servidor de licenças] (<https://support.citrix.com/article/CTX477636/required-license-server-update>)
- [Perguntas frequentes sobre a telemetria de licenças da Citrix] (<https://support.citrix.com/article/CTX477614/license-telemetry-faq>)

Para obter a lista de elementos de dados de telemetria de licenciamento, consulte [Elementos de dados de telemetria de licenciamento da Citrix](#).

## Sobre esta versão

A atualização cumulativa 1 (CU1) do Citrix Virtual Apps and Desktops 7 2402 LTSR corrige mais de 30 problemas relatados desde a versão inicial 2402 LTSR.

[2402 LTSR \(informações gerais\)](#)

[2402 LTSR \(recursos e informações de upgrade\)](#)

[Problemas corrigidos desde o Citrix Virtual Apps and Desktops 7 2402 LTSR \(versão inicial\)](#)

[Problemas conhecidos nesta versão](#)

[Substituição e remoções](#)

[Datas de qualificação do Citrix Product Subscription Advantage](#)

## Downloads

[Citrix Virtual Apps and Desktops 7 2402 LTSR CU1](#)

### Linux Virtual Delivery Agent 2402 LTSR CU1

O Linux Virtual Delivery Agent 2402 CU1 contém [correções](#).

### Profile Management 2402 LTSR CU1

O Profile Management 2402 CU1 contém [correções](#).

## Session Recording 2402 LTSR CU1

O Session Recording 2402 CU1 contém [correções](#).

## StoreFront 2402 LTSR CU1

O StoreFront 2402 CU1 contém [correções](#).

## Novas implantações

Como faço para implantar a CU1 do zero?

Você pode configurar um ambiente totalmente novo do Citrix Virtual Apps and Desktops baseado na CU1 usando o metainstalador CU1. Antes disso, recomendamos que você se familiarize com o produto:

Leia a seção [Citrix Virtual Apps and Desktops 7 2402 LTSR \(versão inicial\)](#) e preste muita atenção às seções [Visão técnica geral](#), [Instalar e configurar](#) e [Segurança](#) antes de começar a planejar a sua implantação. Certifique-se de que sua configuração atenda aos [requisitos do sistema](#) para todos os componentes.

## Implantações existentes

O que eu atualizo?

A CU1 fornece atualizações para 15 componentes de linha de base da versão 2402 LTSR. Lembre-se: a Citrix recomenda que você atualize todos os componentes LTSR de sua implantação para CU1. Por exemplo: se o Citrix Provisioning fizer parte da sua implantação LTSR, atualize os componentes do Citrix Provisioning para CU1. Se o Citrix Provisioning não fizer parte da sua implantação, você não precisa instalá-lo ou atualizá-lo.

## Componentes de linha de base da versão 2402 LTSR CU1

---

<b>Componente de linha de base da versão 2402 CU1</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
VDA de sessão única	2402.0.1100.1256	<a href="#">VDA de sessão única</a>
VDA de várias sessões	2402.0.1100.1256	<a href="#">VDA de várias sessões</a>
Delivery Controller	2402.0.1100.1256	<a href="#">Delivery Controller</a>

<b>Componente de linha de base da versão 2402 CU1</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
Citrix Studio	7.41.1100.48	<a href="#">Citrix Studio</a>
Citrix Director	7.41.1100.33	<a href="#">Citrix Director</a>
Gerenciamento de políticas de grupo Citrix	7.41.1100.34	<a href="#">Gerenciamento de políticas de grupo Citrix</a>
Extensão do lado do cliente da Política de Grupo Citrix	7.41.1100.34	
Citrix StoreFront	2402.0.1100.8	<a href="#">Citrix StoreFront</a>
Servidor de impressão universal	7.41.1100.58	<a href="#">Servidor de impressão universal</a>
Session Recording	24.2.1100	<a href="#">Session Recording</a>
Linux VDA	22.03.1000.7	<a href="#">Linux Virtual Delivery Agent</a>
Profile Management	24.2.1100.23	<a href="#">Profile Management</a>
Serviço de autenticação federada da Citrix	10.17.1100.16	<a href="#">Serviço de autenticação federada (FAS) da Citrix</a>
Redirecionamento de conteúdo do navegador	15.48.1100.65	<a href="#">Redirecionamento de conteúdo do navegador</a>
Citrix Probe Agent 2206	7.41.1100.15	<a href="#">Download</a>

### **Componentes compatíveis com a versão 2402 LTSR CU1**

Os seguintes componentes –nas versões fornecidas abaixo –são compatíveis com ambientes LTSR. Eles não são elegíveis para os benefícios do LTSR (ciclo de vida estendido e atualizações cumulativas somente para correção). A Citrix pode solicitar que você atualize para uma versão mais recente desses componentes em seus ambientes 2402.

<b>Componentes e recursos compatíveis</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
App Layering	2206.0.0	<a href="#">Citrix App Layering</a>
HDX RealTime Optimization Pack	2.9.400.2702	<a href="#">HDX RealTime Optimization Pack</a>
Servidor de licenças	11.17.2.0_BUILD_48000	<a href="#">Servidor de licenças</a>

<b>Componentes e recursos compatíveis</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
Camada de personalização de usuário	24.3.2	<a href="#">Camada de personalização de usuário</a>
Player da web do Session Recording	24.2.1100.16	<a href="#">Player da web do Session Recording</a>
Otimização do Microsoft Teams	15.32.1000.9	<a href="#">Otimização do Microsoft Teams</a>
Workspace Environment Management	2402.1.100.1	<a href="#">Workspace Environment Management</a>
XenApp e XenDesktop 7.15 LTSR VDA (versão mais recente)*	Somente atualização cumulativa mais recente	<a href="#">Documentação</a>

### **Exclusões notáveis da versão 2402 LTSR CU1**

Os seguintes recursos, componentes e plataformas não estão qualificados para marcos e benefícios do ciclo de vida 2402. Especificamente, atualizações cumulativas e benefícios de ciclo de vida estendido estão excluídos. Atualizações para recursos e componentes excluídos estão disponíveis por meio de versões atuais regulares.

#### **Componentes e recursos excluídos**

AppDisks  
 AppDNA  
 Citrix SCOM Management Pack  
 Framehawk  
 Personal vDisk  
 Integração com o StoreFront Citrix Online

#### **Plataformas Windows excluídas \***

Windows 2008 de 32 bits (para Universal Print Server)

\* A Citrix reserva-se o direito de atualizar o suporte à plataforma com base nos marcos do ciclo de vida de fornecedores terceirizados.

## Problemas resolvidos

November 5, 2024

Os seguintes problemas foram resolvidos desde o Citrix Virtual Apps and Desktops 7 2402 LTSR (versão inicial):

### Citrix Director

- Na página Filtros - Todas as máquinas, quando você seleciona todas as máquinas listadas na tela e tenta rolar a lista para baixo, a seleção de objetos não funciona corretamente após uma atualização. [CVADHELP-25259]
- O layout da tabela parece limitado a uma pequena parte da tela. [CVADHELP-25473]
- Na página Director Filter Machine, depois de escolher a guia “Multissessão” e navegar até outra página, ela seleciona a guia Desktop Machines de sessão única padrão quando você volta à página Máquina. [CVADHELP-25439]
- Você pode encontrar um problema ao clicar nos detalhes do UserProfile e tentar selecionar o texto faz com que a UserProfileBox desapareça, impedindo a cópia de dados [CVADHELP-25211]
- Você pode notar que a opção UI.TaskManager.enableApplications é ignorada na interface do usuário, fazendo com que a lista de aplicativos ainda apareça no Director. [CVADHELP-25178]
- Você pode enfrentar falhas ocasionais do SSON em um diretor com balanceamento de carga após a atualização de 2203 CU4 para 2402. [CVADHELP-25646]
- Você pode notar que o Director não é mais exibido se a conexão HDX foi estabelecida usando o Secure ICA. [CVADHELP-25253]

### Política da Citrix

- Você pode portar o GPScanner para 2404 sem alterar o GpfxSettings.dll [CVADHELP-25384]
- Você pode experimentar uma alta utilização de memória no processo CseEngine.exe, o que pode causar problemas de registro da máquina. [CVADHELP-25488]
- Talvez você não consiga editar ou criar uma política após a atualização de uma versão anterior para 2402. O problema não acontece em um novo site de instalação. [CVADHELP-25696]
- Você pode encontrar problemas em que o redirecionamento de conteúdo bidirecional falhe após a atualização para o Citrix Virtual Apps and Desktops 2402 LTSR [CVADHELP-25455]

## Citrix Studio

- O console do Studio pode congelar ao usar o Studio como um aplicativo publicado ou usá-lo em um VDA publicado na sessão do ICA. [CVADHELP-24990]

## Delivery Controller

- O serviço ‘Citrix.Analytics’ falha quando você desinstala a versão LTSR 2203 CU5 do Desktop Delivery Controller (DDC) ou interrompe os serviços ‘Citrix.Analytics’. [CVADHELP-25344]

## Serviço de criação de máquinas

- Ao atualizar um site do Multi-Delivery Controller de algumas versões anteriores a 2402 LTSR (incluindo as versões 2302, 2305, 2308, 2311) para 2402 LTSR, as ações de energia em uma VM podem falhar se o site for atualizado apenas parcialmente. Para obter mais informações, consulte [CTX666299](#). [CVADHELP-25301]

## Gráficos

- Você pode encontrar apagões de tela intermitentes que duram aproximadamente 10 segundos durante o trabalho, durante os quais o processo gráfico do software Citrix (Ctxgfx.exe) é reiniciado. O thread twencode sofre uma exceção de violação de acesso, o que faz com que o ctxExceptionHandler registre minidumps e cause esse problema. O CTXExceptionHandler está configurado para gerar despejos completos para exame. [CVADHELP-24877]
- Ao iniciar o Desktop, você pode encontrar uma tela preta devido à falha do ctxgfx. [CVADHELP-25145]

## Metainstaller

- Quando você instala o Citrix Rendezvous V2 usando VDAWorkstationSetup\_2402.exe, VDAServerSetup\_2402.exe ou VDAWorkstationCoreSetup\_2402.exe, a instalação pode falhar, pois o arquivo Citrix.Diagnostics.Tracing.dll está ausente nesses pacotes. [CVADHELP-25368]
- Quando você tenta instalar o Citrix Virtual Apps and Desktops 2402 por meio da linha de comando, o comando `Exclude "Local Host Cache Storage (LocalDB)"` não está funcionando conforme o esperado. [CVADHELP-25270]
- Do Citrix Virtual Apps and Desktops 2402 em diante, quando você usa o comando `/exclude "Local Host Cache Storage (LocalDB)"` no controlador de entrega, a instalação do

software de banco de dados SQL Server Express LocalDB é interrompida em vez de continuar a instalação sem o LocalDB. [CVADHELP-25349]

## **Servidor de impressão universal**

### **Impressão**

- Você pode enfrentar uma falha nos serviços de spooler do Windows Print em VDAs com cpmon.dll, resultando na perda de impressoras e na incapacidade de imprimir após o envio de trabalhos de impressão. [CVADHELP-25484]

## **VDA para SO de sessão única**

### **Área de transferência**

- Quando você usa o VDA 2203 LTSR CU4 e copia e cola conteúdo no formato WebP, `WFSHELL` para de funcionar. [CVADHELP-25356]

### **Sessão/conexão**

- O aplicativo OpenTEXT ETX falha ao abrir devido a uma violação de acesso com o seguinte módulo: `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll` [CVADHELP-24985]
- Você pode experimentar desligamentos aleatórios da máquina em uma única sessão ao entrar ou sair de períodos de interrupção quando não há sessão ativa. [CVADHELP-25615]

## **Cartões inteligentes**

- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA do servidor, onde o consumo de memória chega a 100%. [CVADHELP-25389]

## **VDA para SO multissessão**

### **Área de transferência**

- Quando você usa o VDA 2203 LTSR Cu4 e copia e cola conteúdo no formato WebP, `WFSHELL` para de funcionar. [CVADHELP-25356]



## **Sessão/conexão**

- O aplicativo OpenTEXT ETX falha ao abrir devido a uma violação de acesso com o seguinte módulo: C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll [CVADHELP-24985]
- Você pode enfrentar falhas no TermService com o Citrix VDA. [CVADHELP-25104]
- Os VDAs podem deixar de responder de forma intermitente. [CVADHELP-25107]
- Você pode encontrar um erro em que os dados do Cloud Broker estão fora de sincronização com o VDA, fazendo com que uma sessão ativa no VDA apareça como desconectada no Director. [CVADHELP-25479]

## **Cartões inteligentes**

- Você pode encontrar um problema de vazamento de memória com o serviço Citrix Smart Card em instâncias de VDA do servidor, onde o consumo de memória chega a 100%. [CVADHELP-25389]

## **Linux VDA**

A [documentação do Linux VDA 2402 CU1](#) fornece informações específicas sobre as atualizações nesta versão.

## **Profile Management**

A [documentação do Profile Management 2402 CU1](#) fornece informações específicas sobre as atualizações nesta versão.

## **Session Recording**

A [documentação do Session Recording 2402 CU1](#) fornece informações específicas sobre as atualizações nesta versão.

## **StoreFront**

A [documentação do StoreFront 2402 CU1](#) fornece informações específicas sobre as atualizações nesta versão.

## 2402 LTSR (versão inicial)

September 11, 2024

### Sobre este lançamento de versão

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

Os LTSRs também estão disponíveis para Citrix Virtual Apps and Desktops 2203 e 1912.

Este lançamento do Citrix Virtual Apps and Desktops inclui novas versões de Windows Virtual Delivery Agents (VDAs) e novas versões de vários componentes principais. Você pode:

- **Instalar ou atualizar um site:** use o ISO para esta versão para instalar ou atualizar componentes principais e VDAs. Instalar ou atualizar esta 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, mas não está pronto para atualizar seus componentes principais, pode continuar usando vários dos recursos mais recentes do HDX instalando (ou atualizando) um novo VDA. Atualizar somente os VDAs pode ser útil quando você deseja testar aprimoramentos em um ambiente que não seja de produção.

Depois de atualizar seus VDAs para essa versão, você não precisa atualizar o nível funcional do catálogo de máquinas. Para obter mais informações, consulte [Versões do VDA e níveis funcionais](#).

Para obter instruções de instalação e atualização:

- Se você estiver criando um novo site, siga a sequência em [Instalar e configurar](#).
- Se você estiver atualizando um site, consulte [Atualizar uma implantação](#).

## Citrix Virtual Apps and Desktops 7 2402 LTSR

### Secure HDX (versão prévia)

Agora você pode usar o Secure HDX, que é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que qualquer elemento de rede no caminho de tráfego possa inspecionar o tráfego do HDX. Para obter mais informações, consulte [Secure HDX](#).

### **Nova política de Gráficos HDX - Permitir bloqueio de tela do Windows**

Com a nova política **Permitir bloqueio de tela do Windows** nos Gráficos HDX, agora você tem a opção de modificar os tempos limite de exibição do Windows em uma sessão do Citrix Virtual Desktop no sistema operacional Workstation, conforme sua necessidade.

Para obter mais informações, consulte [Permitir bloqueio de tela do Windows](#).

### **Novo política de modo de tolerância a perdas de áudio**

O modo de tolerância a perdas de áudio agora está disponível para permitir a entrega de áudio por meio da política de modo tolerante a perdas.

Para obter mais informações, consulte [Modo de tolerância a perdas de áudio](#).

### **Binários assinados por terceiros**

Os binários distribuídos pela Citrix agora estão assinados. Os binários assinados indicam que eles são validados por certificados gerados pela Citrix ou por certificados autênticos de terceiros. Para obter mais informações, consulte [Instalar VDAs](#).

### **Logs aprimorados do sistema para redirecionamento de conteúdo do navegador**

Com os aprimoramentos nos logs do sistema, o redirecionamento do conteúdo do navegador agora permite que os administradores monitorem o status do recurso. Para obter mais informações, consulte [Como solucionar problemas de redirecionamento de conteúdo do navegador](#).

### **Configuração aprimorada de redirecionamento de conteúdo bidirecional**

Anteriormente, a configuração do redirecionamento bidirecional de conteúdo envolvia o gerenciamento de três políticas distintas: permitir o redirecionamento bidirecional de conteúdo, permitir o redirecionamento de URLs para o VDA e permitir o redirecionamento de URLs para o cliente. Essas políticas exigem configurações no lado do servidor e no lado do cliente (configuradas por meio de políticas de grupo). A partir dessa versão, consolidamos todas as três políticas em uma política única e unificada. Ela não apenas simplifica e aprimora o processo de configuração, mas também elimina a necessidade de configurações do lado do cliente.

Para obter mais informações, consulte [Configuração de redirecionamento de conteúdo bidirecional](#).

## **Redutor HDX**

Agora você pode configurar a versão do algoritmo de compactação HDX, ou Redutor, que deseja usar no host da sessão.

Para obter mais informações, consulte [Redutor HDX](#).

## **Nova configuração de registro HDX para configurar o tempo limite de EDT**

Agora você tem a opção de configurar o tempo limite de EDT definindo o registro. Para obter mais informações, consulte [Configurar o tempo limite de EDT](#).

## **Otimização do Microsoft Teams - entrada de registro na lista de permissões**

A partir do Citrix Virtual Apps and Desktops 2402, você não precisa mais configurar manualmente a entrada do registro do `msedgewebview2.exe`, pois agora ela está listada como permitida por padrão.

Para obter mais informações, consulte a documentação da [Microsoft](#).

## **Suporte à lista de permissões do canal virtual para variáveis de ambiente**

Agora você pode usar variáveis de ambiente do sistema no caminho de processos confiáveis. Para obter mais informações, consulte [Uso de variáveis de ambiente do sistema](#).

## **Citrix Secure Private Access no local**

### **Secure Private Access no local e suporte para ZTNA e outros aprimoramentos**

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 de confiança zero a aplicativos baseados em navegador (aplicativos internos da Web e SaaS) usando o portal local StoreFront como um portal de acesso unificado para aplicativos web e SaaS, além de aplicativos e áreas de trabalho virtuais como parte integrada do Citrix Workspace. O Citrix Secure Private Access local é uma solução Zero Trust Network Access (ZTNA) gerenciada pelo cliente que fornece acesso sem VPN a aplicativos internos Web e SaaS com o seguinte, além de uma experiência perfeita para o usuário final:

- Princípio do menor privilégio
- Login único (SSO)
- Autenticação multifator
- Avaliação da postura do dispositivo

- Controles de segurança em nível de aplicativo
- Recursos de proteção de aplicativos

Para obter mais informações, consulte [Citrix Secure Private Access no local —Disponibilidade geral](#).

## **Virtual Delivery Agents (VDAs) 2402 LTSR**

### **Opção de instalar, atualizar ou desinstalar o aplicativo Citrix Workspace durante a instalação, atualização ou desinstalação do VDA**

Esse recurso permite que você escolha instalar, atualizar ou desinstalar o aplicativo Citrix Workspace durante a instalação, atualização ou desinstalação de um VDA nos seguintes cenários:

- Durante a instalação do VDA, você pode optar por instalar o aplicativo Citrix Workspace. Por padrão, o aplicativo Citrix Workspace não é instalado durante a instalação do VDA.
- Durante uma atualização do VDA, se o aplicativo Citrix Workspace ainda não estiver instalado no VDA, você poderá optar por instalar o aplicativo Citrix Workspace.
- Durante uma atualização do VDA, se a versão do aplicativo Citrix Workspace puder ser atualizada, a opção de atualizar o aplicativo Citrix Workspace será exibida.
- Durante a desinstalação do VDA, você pode optar por não desinstalar o aplicativo Citrix Workspace. Por padrão, o aplicativo Citrix Workspace é desinstalado durante a desinstalação do VDA. Para obter mais informações, consulte [Selecione os componentes para instalar e o local de instalação](#) e [Opções de linha de comando para instalar um VDA](#)

### **Suporte do WebSocket para VDAs**

O Citrix Virtual Apps and Desktops agora permite que você use a tecnologia WebSocket em vez do Citrix Brokering Protocol (CBP) para facilitar a comunicação entre VDAs e Delivery Controllers. Esse recurso requer somente a porta TLS 443 para comunicação do VDA com o Delivery Controller.

Para obter mais informações, consulte [Comunicação do WebSocket entre o VDA e o Delivery Controller](#).

### **Suporte a atualizações do VDA a partir de um compartilhamento de arquivos local ao qual os VDAs tenham acesso (prévia)**

Agora você pode oferecer suporte a atualizações de VDA a partir de um compartilhamento de arquivos local e especificar a localização do instalador do VDA por meio de comandos do PowerShell. Para obter mais informações, consulte [Suporte às atualizações do VDA a partir do armazenamento de arquivos local](#).

## Web Studio

### Suporte para provisionamento de VMs da VMware usando perfis de máquina

Ao provisionar VMs da VMware usando o Machine Creation Service (MCS), agora você pode selecionar uma VM existente como perfil da máquina, permitindo que as VMs do catálogo herdem as configurações da VM selecionada.

As configurações herdadas incluem:

- Marcas colocadas no modelo
- Atributos personalizados
- Políticas de armazenamento do vSAN
- Versão de hardware virtual
- TPM virtual (vTPM) do vSphere
- Contagem de CPUs e núcleos por soquete
- Contagem de NICs

Para obter mais informações, consulte [Criação de catálogos de máquinas](#).

### Gerenciamento de imagens preparadas com o nó **Imagens**

Agora, um nó **Imagens** está disponível no Web Studio, permitindo que você prepare uma imagem do MCS (imagem preparada) a partir de uma única imagem de origem e a implante em vários catálogos de máquinas do MCS. Esse nó facilita o gerenciamento completo do ciclo de vida da imagem, permitindo que você crie definições, versões e catálogos de imagens.

As imagens preparadas usando esse nó só podem ser usadas em ambientes do Azure e da VMware. Para obter informações detalhadas sobre gerenciamento de imagens, consulte [Gerenciamento de imagens \(prévia\)](#).

Como alternativa, você também pode criar catálogos com imagens preparadas usando o nó **Catálogos de computadores**. Para obter mais informações, consulte [Criação de catálogos de máquinas](#).

### Políticas relacionadas

**Novas validações de políticas.** Validações adicionais de políticas são adicionadas. Como resultado, habilitar políticas ou fazer uma atualização no local poderá levar à perda de dados da política se houver configurações de política inválidas. Se você criar ou editar as políticas usando um método diferente do Web Studio, a Citrix recomendará que você use a versão mais recente do SDK e do snap-in. Para obter mais informações, consulte [CTX676686](#).

## Recursos preteridos

Os seguintes recursos e configurações foram descontinuados no Web Studio:

- Ambientes do Azure:

O provisionamento de VMs usando uma imagem mestre de uma região diferente foi descontinuado. Recomendamos usar a Galeria de Computação do Azure para replicar a imagem mestre na região em que as VMs serão criadas.

- Ambientes da AWS:

A opção **Aplicar propriedades de modelo da máquina a máquinas virtuais**, na página **Configuração do catálogo de máquinas > Modelo de máquina**, foi descontinuada. Em vez disso, recomendamos usar perfis de máquina para especificar as propriedades da máquina para VMs.

- Todos os ambientes de hipervisor e serviço de nuvem:

A configuração do cache de write-back com apenas um cache de disco e sem cache de memória foi descontinuada. Recomendamos definir o tamanho do cache de memória para um valor maior que zero.

## Citrix Director

### Integração do Secure Private Access com o Director (versão prévia)

A integração do Secure Private Access com o Director permite que o administrador do suporte técnico ou 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, aplicativo Citrix Workspace e VDA.

As ações disponíveis incluem a exibição dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário no pop-up **Selecionar uma sessão > guia Sessões > Aplicativos Web e aplicativos SaaS**
- Falha do Secure Private Access ou bloqueio de enumerações e falhas na inicialização de aplicativos no pop-up **Selecionar uma sessão > guia Acesso negado**
- Exibição dos detalhes da sessão e do aplicativo para inicializações de aplicativos ativas e com falha
- Exibição de detalhes da sessão e do aplicativo para enumerações com falha e bloqueadas

Para obter mais informações, consulte a página [Integração do Secure Private Access com o Director \(versão prévia\)](#).

## **Painel aprimorado de métricas de desempenho**

O painel **Métricas de desempenho** tem uma visualização aprimorada das métricas em tempo real. Ao clicar na guia **Desempenho da sessão**, junto com os dados em tempo real, você pode exibir os dados dos últimos 15 minutos sem esperar pelo tempo de carregamento da página. Esse aprimoramento ajuda a reduzir o tempo médio de resolução, permitindo que os administradores possam correlacionar várias métricas de desempenho de componentes em uma única exibição. Para obter mais informações, consulte a seção [Métricas de desempenho](#).

## **Suporte para a versão mais recente do Microsoft Teams**

O Citrix Director agora oferece suporte ao Microsoft Teams versão 2.1 ou anterior.

## **Machine Creation Services (MCS)**

### **Gerenciamento de imagens (prévia)**

Com a funcionalidade de gerenciamento de imagens, o MCS separa a fase de masterização do fluxo de trabalho geral de provisionamento.

Você pode preparar uma imagem do MCS (Imagem preparada) a partir de uma única imagem de origem e usá-la em vários catálogos diferentes de máquinas do MCS. Essa implementação reduz significativamente os custos de armazenamento e tempo e simplifica o processo de implantação da VM e de atualização de imagens.

Os benefícios de usar essa funcionalidade de gerenciamento de imagens são:

- Gere imagens preparadas com antecedência sem criar um catálogo.
- Reutilize imagens preparadas em vários cenários, como criar e atualizar um catálogo.
- Reduza significativamente o tempo de criação ou atualização do catálogo.

Para obter informações detalhadas sobre gerenciamento de imagens, consulte [Gerenciamento de imagens \(prévia\)](#).

## **Verificar se há várias NICs na VMware**

Em ambientes da VMware, introduzimos várias verificações antes do voo quando a unidade de hospedagem e o modelo de perfil de máquina têm várias redes e o parâmetro `-NetworkMapping` é usado nos comandos `New-ProvScheme` e `Set-ProvScheme`. Para obter mais informações sobre a lista de verificação pré-implantação para várias NICs, consulte [Verificar se há várias NICs](#).



## **Suporte para criar VMs do Windows 11 no GCP**

Agora você pode criar VMs do Windows 11 no GCP. Se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, você deve habilitar o vTPM na origem do perfil de máquina (VM ou modelo de instância).

Esse recurso é aplicável a:

- Catálogos de máquinas do MCS persistentes e não persistentes
- Somente grupo de nós de locatário único

Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte [Criar VMs do Windows 11 no nó de locatário único](#).

## **Suporte à criação de catálogos do Citrix Provisioning usando comandos do MCS PowerShell na VMware**

Agora você pode criar catálogos do Citrix Provisioning usando os comandos do MCS PowerShell na VMware.

Essa implementação oferece as seguintes vantagens:

- Uma única API unificada para gerenciar os catálogos do MCS e do Citrix Provisioning.
- Tenha novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Para obter mais informações, consulte [Criar catálogos do Citrix Provisioning no Citrix Studio](#).

## **Profile Management**

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## **Linux VDA**

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## **Session Recording**

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## Workspace Environment Management

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## Citrix Provisioning

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## Serviço de autenticação federada

Para obter informações sobre novos recursos, consulte o artigo [O que há de novo](#) em seu próprio documento.

## Componentes da linha de base da versão inicial 2402 LTSR

<b>Componente de linha de base 2402</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
VDA de sessão única	2402.0.4000.4310	<a href="#">VDA de sessão única</a>
VDA de várias sessões	2402.0.4000.4310	<a href="#">VDA de várias sessões</a>
Delivery Controller	7.41.100.229	<a href="#">Delivery Controller</a>
Citrix Studio	7.41.100.251	<a href="#">Citrix Studio</a>
Citrix Director	7.33.4000.26	<a href="#">Citrix Director</a>
Gerenciamento de políticas de grupo Citrix	7.41.100.115	<a href="#">Gerenciamento de políticas de grupo Citrix</a>
Extensão do lado do cliente da Política de Grupo Citrix	7.41.100.115	
Citrix StoreFront	2402.0.100.64	<a href="#">Citrix StoreFront</a>
Citrix Provisioning	7.41.100	<a href="#">Citrix Provisioning</a>
Servidor de impressão universal	7.33.4000.11	<a href="#">Servidor de impressão universal</a>
Session Recording	24.2.100.35	<a href="#">Session Recording</a>
Linux VDA	24.02.0.93	<a href="#">Linux Virtual Delivery Agent</a>

<b>Componente de linha de base 2402</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
Profile Management	24.2.100.52	<a href="#">Profile Management</a>
Serviço de autenticação federada da Citrix	10.17.100.90	<a href="#">Serviço de autenticação federada (FAS) da Citrix</a>
Redirecionamento de conteúdo do navegador	15.32.4000.12	<a href="#">Redirecionamento de conteúdo do navegador</a>
Citrix Probe Agent 2402	7.41.100.78	<a href="#">Download</a>

### Componentes compatíveis com a versão inicial 2402 LTSR

Os seguintes componentes –nas versões fornecidas abaixo –são compatíveis com ambientes LTSR. Eles não são elegíveis para os benefícios do LTSR (ciclo de vida estendido e atualizações cumulativas somente para correção). A Citrix pode solicitar que você atualize para uma versão mais recente desses componentes em seus ambientes 2402.

<b>Componentes e recursos compatíveis</b>	<b>Versão conforme mostrada em programas e recursos</b>	<b>Documentação</b>
HDX RealTime Optimization Pack	2.9.600	<a href="#">HDX RealTime Optimization Pack</a>
Servidor de licenças	11.17.2.0_BUILD_47000	<a href="#">Servidor de licenças</a>
Camada de personalização de usuário	23.9.1	<a href="#">Camada de personalização de usuário</a>
Player da web do Session Recording	22.3.4000.4	<a href="#">Player da web do Session Recording</a>
Otimização do Microsoft Teams	15.32.3000.9	<a href="#">Otimização do Microsoft Teams</a>
Workspace Environment Management	2402.1.100.1	<a href="#">Workspace Environment Management</a>

### Exclusões notáveis da versão inicial 2402 LTSR

Os seguintes recursos, componentes e plataformas não estão qualificados para marcos e benefícios do ciclo de vida 2402. Especificamente, atualizações cumulativas e benefícios de ciclo de vida estendido estão excluídos. Atualizações para recursos e componentes excluídos estão disponíveis por meio de versões atuais regulares.

---

## Componentes e recursos excluídos

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integração com o StoreFront Citrix Online

---

---

## Plataformas Windows excluídas \*

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* A Citrix reserva-se o direito de atualizar o suporte à plataforma com base nos marcos do ciclo de vida de fornecedores terceirizados.

## Problemas resolvidos

September 11, 2024

Os seguintes problemas foram resolvidos desde o Citrix Virtual Apps and Desktops 7 2311.

### Geral

- Quando o nome do dispositivo de áudio tem mais de 200 caracteres, o dispositivo pode não conseguir redirecionar para a sessão virtual. [HDX-58341]
- Para redirecionamento de webcam, não há suporte para o cliente RDP para o segundo salto. [HDX-55630]
- Quando você digitaliza uma imagem em uma sessão de área de trabalho com o ambiente configurado conforme descrito abaixo, a imagem pode não ser digitalizada. Esse problema é intermitente.
  - Instalação do driver do scanner e do aplicativo de imagem.
  - Política de direção USB ativada no DDC.
  - Configuração do ambiente:

- \* DDC: Win2k19 + 7.33CU4
- \* VDA: Win2k19/Win2k16+ 7.40.0.191
- \* Cliente: Win10x64 22H2 + CWA 24.1.0.597

[HDX-58888]

- A inicialização de um segundo aplicativo contínuo falhará se o SSL estiver ativado e a confiabilidade da sessão estiver desativada. Se um aplicativo integrado for iniciado, a inicialização subsequente de outro aplicativo contínuo no mesmo servidor deverá ser realizada na sessão existente (compartilhamento de sessão), enquanto o cliente tende a iniciar o aplicativo em uma nova sessão, fazendo com que uma solicitação de validação inesperada seja enviada ao agente. [HDX-52439].
- Se você estiver usando áudio mono para fluxos de áudio estéreo, poderá ouvir apenas um canal de áudio em um fone de ouvido em vez de receber os dois canais nos dois ouvidos. [HDX-56344]

## Delivery Controller

- As atualizações na tabela `MonitorData.ResourceUtilization` do banco de dados de monitoramento estão atrasadas. [CVADHELP-22724]
- Quando você usar um VDA versão 2203 CU3 com o Windows 10, o instalador do VDA não hospedará a porta WCF personalizada se o Proxy do Rendezvous estiver configurado. [CVADHELP-24199]

## Director

- Quando você usa um VDA de área de trabalho com várias sessões ou uma única sessão no **Site de várias florestas**, o recurso de pesquisa centrada no usuário não funciona. [CVADHELP-23174]

## Gráficos

- No Windows 11 versão 22H2, ao mover uma janela do Windows Media Player em uma sessão, somente a metade inferior do vídeo é exibida. Como solução alternativa, selecione: Configurações > Sistema > Multitarefa > Ajustar janelas > Mostrar layouts de ajuste quando arrasto uma janela para o topo da tela [HDX-42092]
- Ao usar o Citrix Virtual Apps and Desktops 2203, você pode observar uma tela preta ao se reconectar às sessões desconectadas. [CVADHELP-23615]

## Política

- Depois de atualizar o Citrix Virtual Apps and Desktops da versão 1912 LTSR CU3 para a versão CU4 ou CU5, os VDAs podem não se registrar no Delivery Controller e permanecer sem registro. [CVADHELP-19834]
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA. [CVADHELP-20908, CVADHELP-19916]

## Studio

- Os administradores personalizados que não têm o escopo “Todos” não podem editar ou excluir políticas do conjunto de políticas padrão. Como solução alternativa, adicione um escopo à política padrão que o administrador personalizado possa acessar. [GP-1569]
- Ao usar o *Citrix Studio* e o *Web Studio* em sua implantação, você poderá encontrar: se você criar uma pasta de aplicativos no *Citrix Studio*, mas não adicionar nenhum aplicativo a ela, essa pasta vazia não aparecerá no *Web Studio*. [STUD-27526]
- Ao criar uma conexão de hospedagem com o Azure usando o Web Studio, se você clicar em **Criar entidade de serviço** na página **Detalhes da conexão** e clicar em **Avançar**, poderá receber um erro. Para resolver o problema, permita cookies de terceiros no navegador. [STUD-24463]
- Quando você adiciona o endereço do servidor StoreFront por meio do Citrix Studio e o atribui a um grupo de entrega, o armazenamento é definido como desativado por padrão. [CVADHELP-24862]

## Servidor de impressão universal

### Impressão

- Quando você usa o VDA versão 1912 CU5 e a versão do sistema operacional 2012 R2, vários trabalhos de impressão estão falhando no servidor de impressão do Citrix UPS de produção com a seguinte mensagem de erro:  
`CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt  
: Failed to Open Stream. Abort Job.`  
[CVADHELP-22354]
- Quando você usa o UPS versão 2212 ou 2305 no Citrix Virtual Apps and Desktops versão 2212 ou 2305 com o Windows 10 VDA, as impressoras que usam o CUPS exibem a seguinte mensagem:  
`Access Denied, cannot connect message`  
[CVADHELP-23644]

## VDA para SO de sessão única

- Ao usar o Windows VDA, você pode enfrentar um erro de mapeamento do teclado ao alternar do teclado japonês para o coreano. [HDX-59307]
- Os valores `SaveRsoPToFile`, `SaveRsoPToMemory` e `SaveRsoPToRegistry` na chave do registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` podem não ser restaurados. [CVADHELP-23184]
- Depois de atualizar um VDA para a versão 2203, o aplicativo Skype for Business pode deixar de responder na tela inicial. [CVADHELP-21021]
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA. [CVADHELP-19916]
- Um impasse no Broker Agent impede que as máquinas se registrem novamente em uma alteração de IP do DNS. [CVADHELP-18952]
- Esta correção introduz uma opção de linha de comando `/no_pending_reboot_check` que impede a verificação de uma reinicialização pendente de uma instalação anterior do Windows no computador ao instalar ou atualizar os componentes principais. [CVADHELP-21686]
- O processo `WebSocketService.exe` falha ao iniciar após a reinicialização do VDA. [CVADHELP-24771]
- Quando você usa um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de bug com a seguinte mensagem a qualquer momento no início ou durante uma sessão.

Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys

[CVADHELP-24891]

- Quando você usa uma máquina, a inicialização da sessão do usuário falha de forma intermitente. [CVADHELP-23922]
- Durante a reconexão de uma sessão do ICA, a janela de chat de um aplicativo de mensagens de terceiros pode aparecer automaticamente em primeiro plano. [CVADHELP-24000]
- O processo `Wfshell.exe` pode falhar quando você copia e cola arquivos de uma estação de trabalho local na sessão da Citrix para VDA LTSR 2203. [CVADHELP-24146]
- Quando você usa um Windows 10 VDA versão 2308, o processo `ctxappvservice.exe` pode falhar. [CVADHELP-24575]
- A cópia do conteúdo de um aplicativo Microsoft Visio ou Visio publicado em uma área de trabalho para um aplicativo no dispositivo do usuário pode falhar. [CVADHELP-23647]
- O `WebSocketService` (serviço WebSocker de redirecionamento de vídeo HTML5) pode falhar. [CVADHELP-23917]

- Um aplicativo definido na metade esquerda do monitor esquerdo aparece incorretamente nesse centro da tela depois que você se reconecta ao usar o Virtual Apps and Desktops 2203 LTSR, o aplicativo Citrix Workspace 2203 LTSR CU3 (2303 ou 2205) e o VDA 2203 LTSR com Windows 11 22h2. [CVADHELP-23878]

## VDA para SO multissessão

- O processo `WebSocketService.exe` pode consumir mais memória do que o esperado nos VDAs. [CVADHELP-23870]
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA. [CVADHELP-19916]
- Um impasse no Broker Agent impede que as máquinas se registrem novamente em uma alteração de IP do DNS. [CVADHELP-18952]
- O processo `WebSocketService.exe` falha ao iniciar após a reinicialização do VDA. [CVADHELP-24771]
- Quando você usa um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de bug com a seguinte mensagem a qualquer momento no início ou durante uma sessão.  
`Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys`  
[CVADHELP-24891]
- Alguns processos do aplicativo Citrix Workspace podem não fechar conforme o esperado quando são executados em uma sessão de aplicativo publicada. [CVADHELP-24225]
- No Server 2019 VDA versão LTSR 2203 CU3, `WmiPrvSE.exe` falha. [CVADHELP-24436]
- O processo `Wfshell.exe` pode falhar quando você copia e cola arquivos de uma estação de trabalho local na sessão da Citrix para VDA LTSR 2203. [CVADHELP-24146]
- O processo dos Serviços de Terminal pode falhar após uma reconexão do ACR. [CVADHELP-24364]
- No Windows Server 2022, se um mouse for movido para uma posição dedicada pelo aplicativo ou sistema operacional, você não poderá movê-lo para a posição novamente até que o mouse seja movido para outro local pelo aplicativo ou sistema operacional. [CVADHELP-24444]
- A caixa de diálogo **Mensagem de aviso de tempo ocioso expirado** não aparece na sessão do ICA no OS VDA 2022, embora o limite de tempo de **Sessão ociosa** entre em vigor. [CVADHELP-24646]
- A cópia do conteúdo de um aplicativo Microsoft Visio ou Visio publicado em uma área de trabalho para um aplicativo no dispositivo do usuário pode falhar. [CVADHELP-23647]



## Profile Management

- A [documentação do Profile Management 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Linux VDA

- A [documentação do Linux VDA 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Session Recording

- A [documentação do Session Recording 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Workspace Environment Management

- A [documentação do Workspace Environment Management 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Citrix Provisioning

- A [documentação do Citrix Provisioning 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Serviço de autenticação federada

- A [documentação do Federated Authentication Service 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Problemas conhecidos

January 24, 2025

## Notas

- Os problemas conhecidos descritos nas seções da versão inicial 2402 deste artigo continuam presentes no CU1, a menos que estejam incluídos na lista de problemas corrigidos.
- Se um problema conhecido tiver uma solução alternativa, ela será fornecida após a descrição do problema.
- O aviso a seguir se aplica a qualquer solução alternativa que sugira alterar uma entrada do registro:

### Advertência:

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

## Problemas conhecidos em 2402 CU1

- O recurso Virtual Channel Dynamim Plugin Manager aparece na interface do usuário, mas não é suportado na versão atual. [LCM-14914]
- Ao fazer login no Web Studio com o Delivery Groups Administrator e o Delivery Groups custom Scope, você pode encontrar um erro ao tentar excluir uma tag de uma máquina com sistema operacional de sessão única ou de uma máquina multissessão selecionando Gerenciar tags. [LCM-15079]
- Depois de atualizar o StoreFront 2402 para 2402 CU1, os usuários de dispositivos em alemão talvez não consigam entrar no aplicativo Citrix Workspace e no cliente web Citrix Workspace em navegadores. A página de login pode carregar sem nenhum resultado. Para obter mais informações, consulte [CTX691873](#). [CVADHELP-26301]

## Problemas conhecidos na versão inicial 2402

- O aviso a seguir se aplica a qualquer solução alternativa que sugira alterar uma entrada do registro:

### Advertência:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do

uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

## Geral

- Se o Citrix Files for Windows e/ou o Citrix Files for Office forem instalados antes da atualização do VDA, esses componentes serão desinstalados durante o processo de atualização. Para resolver isso, reinstale o (s) componente (s) após a conclusão da atualização do VDA. [HDX-65579]
- Se você iniciar a barra de aplicativos e abrir o menu Connection Center no aplicativo Citrix Workspace para Windows, a barra de aplicativos não aparecerá abaixo do servidor que a hospeda. [HDX-27504]
- Se você usar o aplicativo Citrix Workspace para Windows e iniciar a barra de aplicativos na posição vertical, a barra cobrirá o menu Iniciar ou a bandeja do relógio do sistema. [HDX-27505]
- 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. [HDX-21671]
- O Citrix Desktop Service pode falhar ao iniciar após realizar uma atualização local do sistema operacional do Windows 10 para o Windows 11. Para resolver o problema, reinicie o computador. [HDX-58399]
- As configurações **Session Limits** para VDAs multissessão foram recusadas em hosts de sessão executando Windows Server 2022, Windows 10 Enterprise multissessão e Windows 11 Enterprise multissessão. Como solução alternativa, você pode configurar **RDS Session Time Limits** por meio do GPO. [HDX-47001]
- A caixa de diálogo Segurança do Windows associada ao FIDO2 não será exibida na frente da janela da sessão do ICA se você estiver executando o aplicativo com privilégios de administrador. É pelo design do sistema operacional que a caixa de diálogo de Segurança do Windows ficará oculta atrás da janela da sessão do ICA se estiver sendo executada como um processo elevado. [HDX-26794]
- A cópia e colagem da área de transferência podem falhar em dados maiores que 100 MB do cliente para a sessão do ICA. Cópias grandes de buffer não são suportadas. [HDX-59028]
- O sistema operacional multissessão Windows 10 ou Windows 11 não oferece suporte à Restauração do Sistema Windows. Portanto, 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 **Disabling System Restore**, como não suportada atualmente no sistema operacional multissessão Windows 10/11, é registrada. [HDX-58915]

- 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 coincidem. 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 antigo e instale o novo VDA. Isso se assemelha a uma nova instalação de VDA e as versões assinadas são aplicadas.

[HDX-62302]

- Em alguns cenários, quando você usa o filtro de política IP do cliente, o endereço IP usado para avaliar a política está incorreto. [HDX-62375]
- Quando você usa a passagem avançada de domínio para login único, o SSO na sessão pode falhar se o dispositivo cliente ou o host da sessão estiver executando o Windows 11. [HDX-62973]
- 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.

## Políticas

- Se você atualizar de qualquer versão anterior do Citrix Virtual Apps and Desktops para 2311 ou 2402 LTSR, os dados da política poderão ser perdidos se houver valores de dados inválidos presentes nas configurações [Policy](#) . Para saber mais sobre o problema e as soluções alternativas relacionadas, consulte [CTX666304](#). [GP-1671]

## Gráficos

- Se você iniciar uma pré-visualização de vídeo usando um aplicativo de webcam de 64 bits com compressão Theora, a sessão poderá falhar. [HDX-21443]
- Você pode notar webcams extras conectadas à área de trabalho remota no aplicativo Skype para desktop. A visualização prévia dessas webcams extras está bloqueada e pode mostrar uma tela preta por motivos de segurança. Você pode ignorar a webcam extra e continuar usando a webcam como endpoint. [HDX-58807]
- O H265 444 na Intel e em algumas GPUs NVIDIA pode resultar na visibilidade de artefatos na sessão. Para problemas relacionados às GPUs Intel, há uma solução temporária para redimensionar a sessão ou alternar o modo de tela cheia. [PMCS-41084]

## Serviços de criação de máquinas

- Em um ambiente VMware hospedado na AWS, a criação do catálogo de máquinas MCS falhará se a imagem mestre estiver habilitada para vTPM. Esse problema afeta todas as versões do Citrix Virtual Apps and Desktops e se deve a um problema no ambiente VMware. Para obter ajuda, entre em contato com [VMware support](#). [PMCS-38514]
- Ao atualizar um site do Multi-Delivery Controller de algumas versões anteriores a 2402 LTSR (incluindo as versões 2302, 2305, 2308, 2311) para 2402 LTSR, as ações de energia em uma VM podem falhar se o site for atualizado apenas parcialmente. Para obter mais informações, consulte [CTX666299](#).

## 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 somente no Windows 10. Para obter mais informações, consulte [CTX213540](#). [HDX-5043, 335153]
- 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. [HDX-12755]
- Alguns trabalhos de impressão de impressoras de rede com balanceamento de carga podem falhar quando as conexões SSL com os servidores de impressão universais estão habilitadas. Isso acontece quando os trabalhos de impressão são executados rapidamente, um após o outro. [HDX-58316]

## Problemas de terceiros

- O Chrome oferece suporte à automação de interface do usuário somente para barras de ferramentas, guias, menus e botões em uma página da Web. Por causa desse problema do Chrome, o recurso de exibição automática do teclado pode não funcionar em um navegador Chrome em dispositivos sensíveis ao toque. Como solução alternativa, execute `chrome --force-renderer-accessibility` ou abra uma nova guia do navegador, digite `chrome: //accessibility` ative o suporte à **Native Accessibility API** para páginas específicas ou para todas as páginas. Além disso, ao publicar um aplicativo integrado, você pode publicar o Chrome com a opção `--force-renderer-accessibility`. [HDX-20858]
- 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. [HDX-46159]

## Gerenciamento de perfil

- A documentação [Profile Management 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Linux VDA

- [A documentação LTSR do Linux VDA 2402](#) fornece informações específicas sobre as atualizações nesta versão.

## Gravação da sessão

- A documentação [Session Recording 2402 LTSR](#) fornece informações específicas sobre as atualizações desta versão.

## Gerenciamento do ambiente de trabalho

- [A documentação LTSR do Workspace Environment Management 2402](#) fornece informações específicas sobre as atualizações desta versão.

## Provisionamento Citrix

- [A documentação do Citrix Provisioning 2402 LTSR](#) fornece informações específicas sobre as atualizações nesta versão.

## Serviço de autenticação federada

- [A documentação LTSR do Federated Authentication Service 2402](#) fornece informações específicas sobre as atualizações nesta versão.

## Depreciação

January 15, 2025

Os anúncios neste artigo têm como objetivo fornecer um aviso prévio sobre plataformas, produtos Citrix e recursos que estão sendo eliminados para que você possa tomar decisões comerciais oportunas. A Citrix monitora o uso e o feedback dos clientes para determinar quando eles são retirados. Os

anúncios podem mudar em versões subsequentes e podem não incluir todos os recursos ou funcionalidades obsoletos. 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 manutenção do Long Term Service Release (LTSR), consulte <https://support.citrix.com/article/CTX205549>.

## Depreciações e remoções

A tabela a seguir mostra as plataformas, os produtos Citrix e os recursos que foram descontinuados ou removidos. As datas em **em negrito** indicam mudanças neste lançamento.

### Depreciações

A descontinuação significa que pretendemos remover o recurso ou a capacidade de uma versão futura. O recurso ou recurso continuará funcionando e terá suporte total até que seja oficialmente removido. Essa notificação de descontinuação pode durar alguns meses ou anos. Após a remoção, o recurso ou a capacidade não funcionarão mais. Este aviso é para permitir que você tenha tempo suficiente para planejar e atualizar seu código antes que o recurso ou a capacidade sejam removidos. Alternativas para itens obsoletos são sugeridas sempre que possível.

---

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Alternativa</b>
Rendezvous V1	2402	Use o Rendezvous V2.
ICA seguro	2402	-
Suporte de VDA no Windows Server 2016	2402	Atualize para as versões mais recentes do Windows Server.

Item	Depreciação anunciada na versão	Alternativa
Suporte para Delivery Controller, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI para sistema operacional de sessão única, VDA para sistema operacional multissessão, 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, registro de configuração e monitoramento do site	2402	Atualize para a versão mais recente do Microsoft SQL Server.
Suporte para configurar o cache de gravação para incluir somente um cache de disco e nenhum cache de memória	2402	Use a opção de configuração do tamanho do cache de memória e aloque um tamanho diferente de zero.
Suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos “antigos”)	2402	Recrie VMs do catálogo legado do Azure. Os catálogos são provisionados sob demanda e, assim, economizam custos de armazenamento.



Item	Depreciação anunciada na versão	Alternativa
A política <b>Target Minimum Frame Rate</b>	2311	Use <b>Graphics Status Indicator</b> para modificar a taxa de quadros mínima alvo.
Suporte ao Citrix Connector 3.1 para o System Center Configuration Manager	2311	Faça a atualização manual da imagem ou do aplicativo.
Suporte para usar uma imagem mestre em uma região diferente da região em que o catálogo foi criado	2311	Use a Galeria de Computação do Azure para replicar a imagem mestre na região desejada.
Configuração do limite de memória do HDX Graphics Display	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 o Thinwire. Veja <a href="#">Modo progressivo</a> .
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 AWS Volume Worker	2311	Use o upload e o download diretos do disco. Veja <a href="#">Upload e download diretos do disco</a> .

Item	Depreciação anunciada na versão	Alternativa
Suporte para SQL Server 2016 no Broker	2308	Use as versões mais recentes. Para obter mais informações, consulte <a href="#">Requisitos do sistema</a> .
Suporte para o XenApp 5.x no Director	2308	—
Suporte para o XenApp 6.x no Director	2308	—
Pacote SCOM para alertas no Director	2308	—
Suporte para plug-in no Director	2308	—
Suporte para o formato WebRTC SDP (Plano B)	2308	Atualize o aplicativo Citrix Workspace para uma versão compatível.
Suporte para o modo de janela única no Microsoft Teams Optimization	2308	Atualize o aplicativo Citrix Workspace para uma versão compatível com o modo MultiWindow. Para obter mais informações, consulte <a href="#">Matriz de recursos e suporte à versão</a> .
Suporte para <code>AWSCaptureInstanceProperties</code> usado em ambientes da AWS	2308	Use um perfil de máquina. Consulte <a href="#">Crie um catálogo usando um perfil de máquina</a> .
<code>Schedule-provVmUpdate</code> comando PowerShell	2305	Use <code>Set-ProvVmUpdateTimeWindow</code> .

Item	Depreciação anunciada na versão	Alternativa
comando <code>Request -provVmUpdate</code> PowerShell	2305	Use <code>Set-ProvVmUpdateTimeWindow</code> com os parâmetros <code>-StartSnow</code> e <code>-DurationInMinutes -1</code> .
comando <code>Cancel-provVmUpdate</code> PowerShell	2305	Use <code>Clear-ProvVmUpdateTimeWindow</code> .
Parâmetro <code>dedicatedTenancy</code> usado no comando <code>New-provScheme</code>	2303	Use o parâmetro <code>TenancyType</code> .
Servidor de licenças 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: <code>Revoke-HypSecurityGroupIngress</code> , <code>Revoke-HypSecurityGroupEgress</code> , <code>Grant-HypSecurityGroupEgress</code> e <code>Grant-HypSecurityGroupIngress</code> usados em ambiente de nuvem e local.	2203	—

Item	Depreciação anunciada na versão	Alternativa	
Citrix Files para Windows e Citrix Files para Outlook a partir do metainstaller VDA.	2203	Use os instaladores autônomos .	
Componente WEM Agent do metainstaller VDA.	2203	—	
Opção Wake on LAN integrada ao SCCM para acesso remoto ao PC.	2012	Use o recurso Wake on LAN autônomo .	
Suporte para o assistente de importação de PVS no Citrix Studio	1912 LITROS	—	Provisione máquinas do Citrix Provisioning usando uma das seguintes formas:
Pacotes de gerenciamento Citrix SCOM para XenApp e XenDesktop, serviços de provisionamento e StoreFront. Para ver as versões do produto que podem ser monitoradas, consulte <a href="#">Documentação dos pacotes de gerenciamento do Citrix SCOM</a> .	1912	Use o Director para monitorar e gerenciar sua implantação. Para obter mais informações sobre o SCOM EOL e alternativas, consulte <a href="https://support.citrix.com/article/CTX266943">https://support.citrix.com/article/CTX266943</a> .	Provisione máquinas usando o Citrix Provisioning Console e exporte-as para o Citrix Virtual Apps and Desktops usando o Citrix Provisioning Devices Export Wizard. Consulte <a href="#">Export Devices Wizard</a> para obter mais detalhes.
SDK de mobilidade/SDK móvel (do antigo Citrix Labs)	7,16	Substituído por 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	Depreciação anunciada na versão	Removido na versão	Alternativa
Aplicativo Citrix Workspace para Windows 1912 HDX Graphics FullScreen + Otimização de texto	—	2402	Use as versões mais recentes.
Suporte para NVIDIA Frame Buffer Capture (NVFBC) com HDX 3D Pro	2311	2311	Use a API de duplicação de desktop (DDAPI).
Suporte de VDA para configuração de política “Instalação automática de drivers de impressora embutidos”.	2308	2311	Nenhuma. Configuração de política compatível com VDAs somente em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores).
Codificação de hardware de GPU NVIDIA (NVENC) com: vGPU 11 e anterior e driver versão 466.77 e anterior.	7,16	2311	Use os drivers NVIDIA atualmente suportados: vGPU 13 ou mais recente, versão 471.41 ou mais recente.
Ferramentas de suporte Citrix (SupportabilityTool_x64.msi) do VDA Meta-Installer.	2305	2305	—
	—	2212	—

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Console de administração de licenças Citrix (incluído pela última vez no Windows License Server 11.16.3 build 30000 e removido no Windows License Server v11.16.6 build 31000).	2003	2006	Use o Citrix Licensing Manager.
Suporte ao adaptador gráfico Citrix Indirect Display Driver (IDD) no Windows 10 versão 1709 e anteriores.	2003	2003	Use o Citrix Virtual Apps and Desktops 7 1912 LTSR VDAs.
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 Citrix Virtual Apps and Desktops 7 2003 ou posteriores, ou use Citrix Virtual Apps and Desktops 7 1912 LTSR VDAs.
Recurso de redefinição de senha de autoatendimento (SSPR).	2003	2006	—
Suporte para versões do Microsoft.NET Framework anteriores à versão 4.8 para VDAs e componentes do servidor principal. Inclui Delivery Controller, Studio e Director.	1912	2003	Atualize para o .NET Framework versão 4.8.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
VDA's no Windows Server 2012 R2.	1912	2003	Instale os VDAs em um sistema operacional compatível.
Componente de migração de aplicativos AppDNA da edição Premium do Citrix Virtual Apps and Desktops.	1909	2003	—
Instalando o Studio em máquinas de 32 bits (x86).	1909	2003	Instale em um sistema operacional x64 compatível.
Suporte para o gancho do Excel em aplicativos perfeitos. Isso foi usado para criar ícones de barra de tarefas separados para cada pasta de trabalho do Microsoft Excel 2010.	1909	1909	—
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.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Suporte para bancos de dados de configuração do site, registro de configuração e monitoramento nas versões 2008 R2, 2012 e 2014 do Microsoft SQL Server (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 os VDAs em um sistema operacional x64 compatível. \*Esse recurso ainda é suportado no 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	—
Remoção das opções do Delivery Controller para os seguintes produtos em fim de vida útil no StoreFront: VDI-in-a-Box e XenMobile (9.0 e versões anteriores).	1903	1903	—
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.



<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Suporte do StoreFront para protocolos TLS 1.0 e TLS 1.1 entre Citrix Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) e Citrix Receiver e Workspace Hub.	7,17	2203	Atualize o Citrix Receivers para um aplicativo Citrix Workspace compatível com o protocolo TLS 1.2. Para obter mais informações sobre o aplicativo Citrix Workspace, consulte <a href="https://docs.citrix.com/en-us/citrix-workspace-app">https://docs.citrix.com/en-us/citrix-workspace-app</a> .
Suporte de VDA para configuração de política “Instalação automática de drivers de impressora embutidos”.	7,16	2311	Nenhuma. Configuração de política compatível com VDAs somente em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e anteriores).
Suporte do StoreFront para usuários acessarem desktops em sites de Desktop Appliance	1811	1912	Use <a href="#">Desktop Lock</a> para casos de uso não associados a domínios.
Suporte para a tecnologia de controle remoto de tela Framehawk	1811	1903	Use <a href="#">Thinwire</a> com o transporte adaptativo ativado.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Suporte ao Citrix Smart Scale em todas as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Essa funcionalidade chegará ao fim da vida útil em 31 de maio de 2019.	1808	1906	Considere usar o <a href="#">Virtual Apps and Desktops Service</a> no Citrix Cloud para melhorar a funcionalidade de gerenciamento de energia.
Suporte para as versões 4.5.1, 4.5.2, 4.6, 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.	7,18	1808	Atualize para o .NET Framework versão 4.7.1 ou posterior. (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 compatível do SUSE.
Suporte para o driver Citrix WDDM em VDAs	7,16	7,16	O driver Citrix WDDM não está mais instalado com VDAs.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
VDA's no Windows 10 versão 1511 (Threshold 2) e versões anteriores do sistema operacional Windows de sessão única, incluindo Windows 8.x e Windows 7 (consulte <a href="https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/">https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/</a> ).	7,15 LTSR (e 7,12)	7,16	Instale VDA's com sistema operacional de sessão única no Windows 10 versão mínima 1607 (Redstone 1) ou canais semestrais mais recentes. Se estiver usando 1607 LTSB, recomendamos um VDA 7.15. Veja <a href="#">CTX224843</a> .
VDA's no Windows Server 2008 R2 e no Windows Server 2012 (incluindo service packs)	7,15 LTSR (e 7,12)	7,16	Instale os VDA's em um sistema operacional compatível.
Redirecionamento de composição de desktop (anteriormente conhecido como DirectX Command Remoting) (DCR)	7,15 L	7,16	Use <a href="#">Thinwire</a> .
Experiência clássica do Citrix Receiver for Web (interface de usuário com “bolhas verdes”)	7.15 LTSR (e StoreFront 3.12)	1903	Experiência unificada do Citrix Receiver for Web.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Componentes principais no Windows Server 2012 e no Windows Server 2008 R2 (incluindo Service Packs). Inclui: Delivery Controller, Studio, Director, StoreFront, License Server e Universal Print Server.	7,15 L	7,18	Instale os componentes em um sistema operacional compatível.
Recurso de redefinição de senha de autoatendimento (SSPR) no Windows Server 2012 e no Windows Server 2008 R2 (incluindo Service Packs)	7,15 L	7,18	Instale em um sistema operacional compatível mais recente.
Studio no Windows 7, Windows 8 e Windows 8.1 (incluindo Service Packs)	7,15 L	7,18	Instale o Studio em um sistema operacional compatível.
Redirecionamento de Flash	7,15 L	1912	Crie conteúdo de vídeo como vídeo HTML5. Use o redirecionamento de vídeo HTML5 para conteúdo gerenciado e o redirecionamento de conteúdo do navegador para sites públicos. Para obter mais informações, consulte a nota <a href="#">Flash Redirection End of Life</a> .

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Integração on-line da Citrix (produto Goto) com o 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 é removido.	7,14	7,14	O serviço do Windows CTXAppvService executa a mesma função. Ele é instalado e configurado automaticamente e não requer interação do usuário.
Suporte ao componente UPSServer do Universal Print Server no Windows Server 2008 de 32 bits	7,14	7,14	Instale em um sistema operacional compatível mais recente.
StoreFront e Receiver para Web no Internet Explorer 8	7,13	7,13	—
Opção de instalação da linha de comando do VDA /no_appv para impedir a instalação dos componentes do Citrix App-V	7,13	7,13	Use a opção de instalação da linha de comando /exclude “Citrix Personalization for App-V —VDA”.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
O instalador completo do produto não instala mais o snap-in Citrix.Common.Commands em novas instalações e o remove automaticamente ao atualizar as instalações existentes.	7,13	7,13	Alguns comandos do PowerShell fornecidos pelo snap-in Citrix.Common.Commands ainda estão disponíveis no SDK do XenApp 6.5.
Funcionalidade parcial para manipular dados de ícones fornecidos pelos cmdlets\*-CTXicon.	7,13	7,13	Agora fornecido pelos cmdlets\ *-BrokerIcon no Broker Service.
Modo Legacy Thinwire	7,12	7,16	Use <a href="#">Thinwire</a> . Se você estiver usando o modo Legacy Thinwire no Windows Server 2008 R2, migre para o Windows Server 2012 R2 ou Windows Server 2016 e use o Thinwire.
Atualizações locais do StoreFront 2.0, 2.1, 2.5 e 2.5.2	7,13	7,16	Atualize de uma dessas versões para uma versão compatível posterior e depois para o XenApp e o XenDesktop 7.16.

<b>Item</b>	<b>Depreciação anunciada na versão</b>	<b>Removido na versão</b>	<b>Alternativa</b>
Atualizações locais 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 XenDesktop 7.6 LTSR (com a UC mais recente) e, em seguida, atualize para a versão mais recente do Citrix Virtual Desktops (antigo XenDesktop) ou LTSR.
Instalação do Delivery Controller, Director, StoreFront ou License Server em máquinas de 32 bits (x86).	7,12	7,16	Instale em um sistema operacional x64 compatível.
Localização de conexões XenDesktop 5.6 usado no Windows XP. Não há suporte para instalações de VDA no Windows XP.	7,12	7,16	Use <a href="#">Local Host Cache</a> .
Instalações de VDA no Windows XP.	7,12	7,16	Instale os VDAs em um sistema operacional compatível.
Suporte para conexões CloudPlatform	7,12	2003	Use um hipervisor ou serviço de nuvem compatível diferente.
Suporte para conexões do Azure Classic (também conhecido como Gerenciamento de Serviços do Azure)	7,12	2003	Considere usar o serviço Virtual Apps and Desktops no Citrix Cloud.

Item	Depreciação anunciada na versão	Removido na versão	Alternativa
Funcionalidade do AppDisks (e a integração do AppDNA com o Studio, que o suporta)	7,13	2003	Use o Citrix App Layering.
Funcionalidade pessoal do vDisk	7,15	2006†	Use a tecnologia <a href="#">da camada de usuário</a> do Citrix App Layering ou <a href="#">da camada</a> de personalização do usuário.

† 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

September 11, 2024

### Introdução

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

Revise [Preparar a instalação](#) antes de iniciar uma instalação.

Salvo indicação, o instalador do componente implementa os pré-requisitos de software automaticamente (como pacotes .NET e C++) se as versões necessárias não forem detectadas no computador. A mídia de instalação Citrix também contém alguns desses softwares de pré-requisitos.

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

Para obter informações sobre globalização, consulte o artigo do Knowledge Center [CTX119253](#).



Para componentes e recursos que podem ser instalados em servidores Windows, 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 além dos requisitos para a imagem do produto, sistema operacional e outros softwares no computador. 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 o StoreFront em um servidor, apenas para avaliação, não uma implantação de produção	5 GB de RAM
Todos os componentes principais e o 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 cache de host local)	5 GB de RAM, disco rígido de 800 MB, banco de dados: consulte a <a href="#">Orientação para dimensionamento</a>
Studio	1 GB de RAM, disco rígido de 100 MB
Director	2 GB de RAM, disco rígido de 200 MB
StoreFront	2 GB de RAM, consulte a <a href="#">documentação do StoreFront</a> para obter recomendações de disco
Servidor de licenças	8 GB de RAM; consulte a <a href="#">documentação de licenciamento</a> para obter recomendações de disco

---

### Dimensionamento de VMs que fornecem áreas de trabalho 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, 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:

- O [Citrix Tech Zone](#) contém orientações sobre dimensionamento.
- O [Citrix Virtual Apps and Desktops Single Server Scalability](#) trata de 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 Pacote Redistribuível Microsoft Visual C++ 2015–2022.

- Se a máquina contiver uma versão anterior do Runtime (como 2015-2019), o instalador Citrix a atualizará.
- Se a máquina contiver uma versão anterior a 2015, a Citrix instalará a versão mais recente em paralelo.

## Delivery Controller

Sistemas operacionais compatíveis:

- Windows Server Core 2022
- 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

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++ 2015–2019 redistribuível.

## Bancos de dados

Versões suportadas do Microsoft SQL Server para bancos de dados de monitoramento, log de configuração e configuração do site.

- SQL Server 2022, edições Express, Standard e Enterprise.
- SQL Server 2019, edições Express, Standard e Enterprise.
- SQL Server 2017, edições Express, Standard e Enterprise.
  - Para novas instalações: por padrão, o SQL Server Express 2017 com atualização cumulativa 16 é instalado ao instalar o Controller, se uma instalação existente suportada do SQL Server não for detectada.

- 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 suportadas (exceto para SQL Server Express, que suporta apenas o modo autônomo):

- Instâncias de cluster de failover AlwaysOn do SQL Server
- Grupos de disponibilidade AlwaysOn do SQL Server (incluindo grupos de disponibilidade básica)
- 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 de host local:** o Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o cache de host local usa de modo autônomo. O cache de host local não requer nenhum componente do SQL Server Express que não seja o SQL Server Express LocalDB.

- Ao instalar um controlador, o Microsoft SQL Server 2022 LocalDB é instalado para uso com o recurso Cache de 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 obter 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 com suporte mais atual
- [Orientação de dimensionamento do banco de dados](#)
- [Cache do host local](#)

## **Web Studio**

### **Nota:**

- Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente 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 melhorar a experiência do usuário e geralmente responde mais rápido do que o Citrix Stu-

dio, o console de gerenciamento baseado no Windows. Consulte [Instalar o Web Studio](#).

Sistemas operacionais compatíveis:

- Windows Server Core 2022
- 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

## Citrix Director

Sistemas operacionais compatíveis:

- Windows Server Core 2022
- 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

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 a função de servidor IIS tenha o serviço de função de conteúdo estático instalado. Se esse software ainda não estiver instalado, você será solicitado a fornecer a mídia de instalação do Windows Server. Em seguida, o software é instalado para você.
- Para visualizar os logs de eventos em computadores 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 de **componentes adicionais** no assistente de instalação) e se o Citrix Profile Management Service estiver sendo executado para exibir os detalhes do perfil do usuário no Director.

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

- System Center 2012 R2 Operations Manager

Navegadores compatíveis para visualização do Director:

- Internet Explorer 11. O modo de compatibilidade não é suportado para o Internet Explorer. Use as configurações recomendadas do navegador para acessar o Director. Quando você instalar o Internet Explorer, aceite o padrão para usar as configurações recomendadas de segurança e compatibilidade. Se você já instalou o navegador e optou por não usar as configurações recomendadas, vá para **Ferramentas > Opções da Internet > Avançado > Redefinir** e siga as instruções.
- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

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

### **Virtual Delivery Agent (VDA) para SO de sessão única**

Sistemas operacionais compatíveis:

- Windows 11
- Windows 10 (somente x64), qualquer versão que esteja atualmente no suporte base.
  - Para obter suporte à edição, consulte o artigo do Knowledge Center [CTX224843](#).

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015–2019 redistribuível.

O Remote PC Access usa esse VDA, que você instala em PCs de escritórios físicos. Esse VDA suporta a Inicialização Segura para o Remote PC Access do Citrix Virtual Desktops no Windows 10 e Windows 11.

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

Para obter informações sobre o Linux VDA, consulte os artigos do [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 Windows de sessão única em uma máquina Windows Server com suporte. Consulte [Server VDI](#) para obter orientação.

Para obter informações sobre como instalar um VDA em uma máquina Windows 7, consulte [Sistemas operacionais anteriores](#).

## Virtual Delivery Agent (VDA) para SO multissessão

Sistemas operacionais compatíveis:

- Windows 11 (compatível somente com Citrix DaaS)
- Windows 10 (somente x64; compatível somente com o Citrix DaaS), qualquer versão que esteja atualmente no suporte principal.
- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter

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

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015–2019 redistribuível.

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

Vários recursos de aceleração de multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado no computador em que você instala o VDA. Se o computador não tiver o Media Foundation instalado, os recursos de aceleração de multimídia não serão instalados e não funcionarão. Não remova o Media Foundation do computador depois de instalar o software da Citrix; caso contrário, os usuários não poderão fazer logon no computador. Na maioria das versões do Windows Server, o recurso Media Foundation é instalado por meio do Gerenciador do Servidor. Para obter mais informações, consulte [Preparar a instalação](#).

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

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

Para obter informações sobre o Linux VDA, consulte os artigos do [Linux Virtual Delivery Agent](#).

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

## Recursos de virtualização e hosts

Os seguintes recursos de virtualização/host (listados alfabeticamente) são suportados. Quando aplicável, as versões *superior.inferior* são suportadas, incluindo atualizações a essas versões. O artigo do Knowledge Center [CTX131239](#) contém informações sobre a versão atual, além de links para problemas conhecidos.

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

O recurso Wake on LAN do Remote PC Access requer, no mínimo, o Microsoft System Center Configuration Manager 2012.

Hipervisores compatíveis:

- **XenServer (anteriormente Citrix Hypervisor)**

[CTX131239](#) contém informações sobre a versão atual, além de links para problemas conhecidos.

Para obter mais informações, consulte [Ambientes de virtualização do XenServer](#).

- **Microsoft System Center Virtual Machine Manager**

Inclui qualquer versão do Hyper-V que possa se registrar nas versões suportadas do System Center Virtual Machine Manager.

[CTX131239](#) contém informações sobre a versão atual, além de links para problemas conhecidos.

Para obter mais informações, consulte [Ambientes de virtualização do Microsoft System Center Virtual Machine Manager](#).

- **Nutanix Acropolis**

[CTX131239](#) contém informações sobre a versão atual, além de links para problemas conhecidos.

Para obter mais informações, consulte [Ambientes de virtualização do Nutanix](#).

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

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

[CTX131239](#) contém informações sobre a versão atual, além de links para problemas conhecidos.

Para obter mais informações, consulte [Ambientes de virtualização do VMware](#).

Hosts de nuvem pública compatíveis:

- **Amazon Web Services (AWS)**

Para obter informações sobre como usar a AWS para provisionar máquinas virtuais, consulte [Ambientes de virtualização da 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 Microsoft Azure Resource Manager para provisionar máquinas virtuais, consulte [Ambientes de virtualização do Microsoft Azure Resource Manager](#).

- **Soluções de nuvem e parceiros da Nutanix**

Para obter informações sobre como usar as soluções de nuvem e parceiros da Nutanix, consulte [Soluções de nuvem e parceiros da Nutanix](#).

- **Soluções de nuvem e de parceiros da VMware**

Para obter informações sobre o uso de soluções de nuvem e parceiros do VMware, consulte [Soluções de nuvem e parceiros do VMware](#).

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

- Você precisa da Licença Hybrid Rights. Para obter informações sobre a Licença Hybrid Rights, consulte [Transition and Trade-Up \(TTU\) com Hybrid Rights](#). Para obter informações sobre como adicionar uma licença, consulte [Criar um site](#).
- As fontes de informação levam você para a documentação do Citrix DaaS. Se você estiver familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local tem várias diferenças.
  - No Citrix DaaS, a interface de gerenciamento é conhecida como Full Configuration. No Citrix Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio.
  - As atualizações do Citrix DaaS são lançadas aproximadamente a cada quatro semanas. Portanto, você notará 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 2016
- Windows Server 2012



- Windows Server 2008 R2
- Windows Server 2008

## HDX

### Áudio

O áudio UDP para ICA Multi-Stream é compatível com o aplicativo Citrix Workspace para Windows e com 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 do recurso HDX. Para obter mais informações sobre os recursos HDX e os aplicativos Citrix Workspace, consulte a [Matriz de recursos](#).

### HDX e entrega do Windows Media

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

Para usar a obtenção 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 os programas padrão**, selecione **Citrix Multimedia Redirector** e clique em **Definir este programa como padrão** ou **Escolher os 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 Windows detecta a presença do hardware GPU em tempo de execução.

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

- GPU Passthrough está disponível com:
  - XenServer
  - Nutanix AHV
  - VMware vSphere e VMware ESX, onde é referido como Virtual Direct Graphics Acceleration (vDGA)

- Microsoft Hyper-V no Windows Server 2016, onde é referido como Discrete Device Assignment (DDA).
- vGPU está disponível com:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

Veja <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2402-ltsr/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 igual ou superior a 2,3 GHz.

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 com suporte pelo software NVIDIA Virtual GPU (vGPU) versão 13 ou superior, consulte <https://docs.nvidia.com/grid/index.html>. Para obter uma lista detalhada de hipervisores e hardware compatíveis, consulte a documentação do [software NVIDIA vGPU](#).
- A aceleração gráfica virtualizada tem suporte na família de processadores Intel Xeon E3 de plataformas gráficas de data center e na série Intel Data Center GPU Flex. Para obter mais informações, consulte [Série GPU Flex](#).
- As GPUs AMD são compatíveis com a virtualização MxGPU da AMD. Para obter mais informações sobre o hardware compatível, consulte a [documentação da AMD](#).

Dispositivo do usuário:

- O Citrix oferece suporte a até 8 monitores 4K, dependendo dos recursos de hardware. Dependendo da GPU usada, pode haver outras restrições de hardware nesse máximo.
- A Citrix recomenda que os dispositivos de usuário tenham pelo menos 4 GB de RAM e CPU com uma velocidade de clock igual ou superior a 1,6 GHz. Para um desempenho ideal, recomendamos que os dispositivos de 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 vários monitores, a Citrix recomenda dispositivos de usuário com CPUs quad-core.
- O aplicativo Citrix Workspace deve ser instalado.

Para obter mais informações, consulte os [artigos HDX 3D Pro](#) e [www.citrix.com/xenapp/3d](http://www.citrix.com/xenapp/3d).

## Servidor de impressão universal

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

O componente UpsServer é compatível com:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Requisitos:

- Microsoft Visual C++ 2015–2019 redistribuível
- Microsoft .NET Framework 4.8 (mínimo)

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

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

Para obter mais informações, consulte [Provisionar impressoras](#).

## Outros

Somente o Citrix License Server 11.17.2 e posterior são suportados. Para obter mais informações, consulte [Licenciamento](#).

Consulte [Product Matrix](#) para obter mais informações sobre compatibilidade de versão.

Para ver as versões compatíveis com o StoreFront, consulte os [requisitos do sistema StoreFront](#).

O Console de Gerenciamento de Política de Grupo (GPMC) da Microsoft é necessário se você armazenar informações de políticas da Citrix no Active Directory em vez de no banco de dados de configuração do site. Se você instalar `CitrixGroupPolicyManagement_x64.msi` separadamente (por exemplo, em um computador que não tenha um componente principal do Citrix Virtual Apps and Desktops instalado), o computador deverá ter o Visual Studio 2015 Runtime instalado. Para obter mais informações, consulte a documentação da Microsoft.

Se você quiser editar GPOs de domínio usando o GPMC, ative o recurso Gerenciamento de Política de Grupo (no Windows Server Manager) em todos os computadores que contêm Delivery Controllers.

Várias NICs são suportadas.

Por padrão, o aplicativo Citrix Workspace para Windows não é instalado quando você instala um VDA atual. Para obter mais informações, consulte a [documentação do aplicativo Citrix Workspace para Windows](#).

Consulte [Acesso a aplicativo local](#) para obter informações do navegador suportado 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 ao PowerShell versões 3 a 5.

## Instalar e configurar

November 5, 2024

Revise os artigos mencionados antes de iniciar cada etapa de implantação, para saber mais sobre o que você vê e especifica durante a implantação.

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

### Preparar

Revisão [Prepare-se para instalar o](#) e concluir todas as tarefas necessárias.

- Onde encontrar informações sobre conceitos, recursos, diferenças de versões anteriores, requisitos do sistema e bancos de dados.
- Considerações ao decidir onde instalar os componentes principais.
- Requisitos de permissão e do Active Directory.
- Informações sobre 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 [Instale os componentes principais](#) ou [Instale usando a linha de comando](#).

### Crie 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 [Instale os VDAs](#) ou [Instale usando a linha de comando](#). Os exemplos de scripts são fornecidos se você quiser instalar VDAs por meio do Active Directory.

Para máquinas com um sistema operacional Linux, siga as orientações no [Linux Virtual Delivery Agent](#).

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

## Instalar componentes opcionais

Se você planeja usar o Citrix Universal Print Server, instale seu componente de servidor nos servidores de impressão. Consulte [Instale os componentes principais](#) ou [Instale usando a linha de comando](#).

Para permitir que o StoreFront use opções de autenticação, como asserções SAML, instale o [Citrix Federated Authentication Service](#).

Para que os usuários tenham maior controle sobre suas contas de usuário, instale [Self-Service Password Reset](#).

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

- O [Citrix Provisioning](#) é um componente opcional que provisiona máquinas fazendo o streaming de uma imagem mestre para dispositivos de destino.
- O [Citrix Gateway](#) é uma solução segura de acesso a aplicativos que fornece aos administradores controles granulares de política e ação em nível de aplicativo para proteger o acesso a aplicativos e dados.
- O [Citrix SD-WAN](#) é um conjunto de dispositivos que otimizam o desempenho WAN.

## Criar um catálogo de máquinas

Depois de criar um site no Studio, você é guiado para [criar um catálogo de máquinas](#).

Um catálogo pode conter máquinas físicas ou virtuais (VMs). Máquinas virtuais podem ser criadas a partir de uma imagem mestre. Quando usa um hipervisor ou outro serviço para fornecer VMs, você

primeiro cria uma imagem mestre no host. Depois, quando cria o catálogo, você especifica a 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 as 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 de grupos de entrega.

### **Limitação conhecida**

Quando você usa o aplicativo Citrix Workspace para Windows versão 1912 ou anterior, a sessão é interrompida após algum tempo. Esse problema foi corrigido nas versões mais recentes LTSR e CR do aplicativo Citrix Workspace. Para obter mais informações sobre as versões de lançamento suportadas, consulte [Aplicativo Citrix Workspace para Windows/Citrix Receiver for Windows Long Term Service Releases](#).

## **Ambientes de virtualização do Microsoft System Center Virtual Machine Manager**

November 5, 2024

Siga estas instruções se você usa o Hyper-V com 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 versões diferentes do Hyper-V) não são suportados.

Você pode usar o Citrix Provisioning (anteriormente Provisioning Services) e Machine Creation Services para provisionar:

- VMs de SO de área de trabalho ou servidor compatíveis com a geração 1.
- VMs de SO de área de trabalho ou servidor compatíveis com a geração 2, incluindo suporte a Inicialização Segura.

## 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 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 falhará 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 do VMM ou administrador delegado do 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 dá suporte ao gerenciamento do ciclo de vida da VM, como criação, atualização e exclusão de VM.

A instalação de um Controller em um servidor executando o Hyper-V não é suportada.

Em grandes implantações em que um único SCVMM gerencia vários clusters em diferentes data centers, você pode limitar o escopo dos grupos de host dos administradores delegados.

Para limitar o escopo dos grupos de hosts, use a função Delegated Admin no console do Microsoft System Center Virtual Machine Manager (VMM):

1. Em **Create User Roles Wizard**, selecione Fabric Administrator (Delegated Administrator) como a função do usuário.
2. Em **Members**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Scope**, selecione os grupos de hosts aos quais deseja que o administrador delegado tenha acesso.

4. Crie uma nova **Run As Account** usando credenciais de usuário administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

## Mais informações

- [Crie e gerencie conexões e recursos](#)
- [Criar catálogos de máquinas](#)

## Instalar usando a linha de comando

November 5, 2024

### Importante:

- Se você estiver atualizando e sua versão atual usa ou tem 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 [Citrix Licensing Data](#).

## Introdução

Este artigo aplica-se à instalação de componentes em máquinas com sistemas operacionais Windows. Para obter informações sobre sistemas operacionais VDAs para Linux, consulte [Linux Virtual Delivery Agents](#).

Este artigo descreve como emitir comandos de instalação de produto. Antes de iniciar qualquer instalação, revise [Preparar para instalar](#). Este 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 a opção **Executar como administrador**. Para obter mais informações, consulte a documentação sobre comandos da Microsoft.

Como complemento ao uso dos comandos de instalação diretamente, são fornecidos scripts de exemplo 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 compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem lhe fornecerá 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 de produto completo

Para acessar a interface da linha de comando do instalador do produto completo:

1. Baixe o pacote de produtos da Citrix. As credenciais da conta da 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 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 os componentes principais:** Execute `XenDesktopServerSetup.exe`, com as opções listadas em Opções de linha de comando para instalar os 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 Serviço de autenticação federada:** a Citrix recomenda o uso da 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 opções de parâmetros a seguir são válidas ao instalar componentes principais com o comando `XenDesktopServerSetup.exe`. Para obter mais detalhes sobre as opções, consulte [Instalar componentes principais](#).

- **/ceiptina** *ceiptina* [,ceiptina]...

Permite a coleta de dados do Call Home e do Programa de Aperfeiçoamento da Experiência do Usuário (CEIP). Os valores válidos são:

- **DIAGNÓSTICO**: Escolha esse valor para permitir que o Citrix Licensing colete dados do Call Home.
- **ANÔNIMO**: Escolha esse valor para permitir que o Citrix Licensing colete dados não identificados do CEIP (que não identificam os usuários).
- **NONE**: Escolha esse valor para desativar a coleta de dados do 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 do CEIP, consulte [Citrix Licensing Customer Experience Improvement Program](#).

Para obter mais detalhes sobre os dados do 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* [,componente]...

Lista de componentes separados por vírgula para instalar ou remover. Os valores válidos são:

- **CONTROLLER**: Controlador
- **DESKTOPSTUDIO**: Estúdio
- **WEBSTUDIO**: Estúdio Web
- **DESKTOPDIRECTOR**: Diretor
- **LICENSESERVER**: Servidor de licenças Citrix
- **SECUREPRIVATEACCESS**: Acesso privado seguro

Se essa opção for omitida, todos os componentes serão instalados (ou removidos, se a opção `/remove` também for especificada).

(Nas 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 Usar o instalador completo do produto).

- **/configure\_firewall**

Abre todas as portas no firewall do Windows usadas pelos componentes que estão sendo instalados, se o Serviço do Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall de terceiros, ou se não estiver usando nenhum firewall, deverá abrir as portas manualmente.

- **/disableexperiencemetrics**

Impede o carregamento automático de análises coletadas durante a instalação, atualização ou remoção para a Citrix.

- **/exclude** “feature“\ [,”feature“]

Impede a instalação de um ou mais recursos, serviços ou tecnologias separados por vírgula, cada qual entre aspas retas normais. Os valores válidos são:

- “[Local Host Cache Storage \(LocalDB\)](#)”: Impede a instalação do banco de dados usado para o Local Host Cache. Esta opção não afeta se a instalação do SQL Server Express é realizada para usar como banco de dados do site ou não.

- **/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 à RAM insuficiente). Para obter mais informações, consulte [Verificação de hardware](#).

- **/ignore\\_site\\_teste\\_falha**

Válido somente durante a atualização do Controller. Normalmente, as falhas de teste do site são ignoradas e a atualização prossegue. Se omitido (ou definido como false), qualquer falha de teste do site faz com que o instalador falhe, sem executar a atualização. Padrão = false

Durante uma atualização, esta opção é ignorada se uma versão do SQL Server não suportada for detectada. Para obter detalhes, consulte [Verificação da versão do SQL Server](#).

- **/installdir**diretório\*\*

Diretório vazio existente onde os componentes serão instalados. Padrão = c:\Arquivos de programas\Citrix.

- **/logpath**caminho\*\*

Localização do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = TEMP%\ [Citrix\XeNDesktop Installer](#)

- **/no\_remote\_assistance**

Válido somente ao instalar o Director. Desativa o recurso de sombreamento de usuário que usa a Assistência Remota do Windows.

- **/noreboot**

Impede uma reinicialização após a instalação. (Para a maioria dos componentes principais, a reinicialização não é ativada por padrão.)

- **/noresume**

Por padrão, quando uma reinicialização de máquina é necessária durante uma instalação, o instalador continua automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso é útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/nosql**

Impede a instalação do Microsoft SQL Server Express no servidor em que você está instalando o Controller. Se esta opção for omitida, o SQL Server Express é instalado para uso como o banco de dados do site.

Essa 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.

- **/remove**

Remove os componentes principais especificados com a opção `/components`.

- **/removeall**

Remove todos os componentes principais instalados.

- **/SKIPHDXDRIVERCHECK**

Ignora a verificação dos drivers HDX no Meta-instalador do VDA.

- **/sendexperiencemetrics**

Envia automaticamente análises coletadas durante a instalação, atualização ou remoção para a Citrix. Se essa opção for omitida (ou `/disableexperiencemetrics` for especificada), as análises serão coletadas localmente, mas não enviadas automaticamente.

- **/tempdir** *diretório*

Diretório que mantém os 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 comunicações de componentes são abertas automaticamente.

```
\x64\XeConfiguração do nDesktop\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 de componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /controlador de componentes,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 de componentes são abertas automaticamente.

```
\x64\XeConfiguração do nDesktop XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall
```

## Usar um instalador autônomo de VDA

As credenciais da conta da 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 sistema operacional multissessão: `VDA ServerSetup_xxxx.exe`
- Agente de entrega virtual de sistema operacional de sessão única: `VDA WorkstationSetup_xxxx.exe`
- Agente de entrega virtual do OS Core Services de sessão única: `VDA WorkstationCoreSetup_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 falhará. Depois, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

- Para `VDAServerSetup_XXXX.exe`, execute `<extract folder>\ Extract\ Image-Full\x64\XeNDesktop Setup\XenDesktopVDASetup.exe`
- Para `VDAWorkstationCoreSetup_XXXX.exe`, execute `<extract folder>\ Extract\ Image-Full\x64\XeNDesktop Setup\XenDesktopRemotePCSetup.exe`
- Para `VDAWorkstationSetup_XXXX.exe`, execute `<extract folder>\ Extract\ Image-Full\x64\XeNDesktop Setup\XenDesktopVDASetup.exe`

Para executar o pacote baixado, execute seu nome: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Use as opções válidas listadas neste artigo.

Se você estiver familiarizado com o instalador do produto completo:

- 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 suporta 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 aplicativo VDA e 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 somente o VDA e excluir a instalação do aplicativo Citrix Workspace, especifique `/components vda`.

Essa opção não é válida ao usar o instalador `VDAWorkstationCoreSetup_XXXX.exe`. Esse instalador não pode instalar o aplicativo Citrix Workspace.

- **/controllers** “controlador \ [controlador]”

FQDNs separados por espaço de Controllers com os quais o VDA pode se comunicar, entre aspas retas normais. Não especifique as opções `/site_guide` e `/controllers`.

- **/disableexperiencemetrics**

Impede o carregamento automático de análises coletadas durante a instalação, atualização ou remoção para a Citrix.

- **/habilitar\\_hdx\\_ports**

Abre as portas no firewall do Windows exigidas pelo VDA e recursos habilitados (exceto a Assistência Remota do Windows), se o Serviço do Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente. Para obter informações sobre portas, consulte [Network ports](#).

Para abrir as portas UDP que o transporte adaptativo HDX usa, especifique a opção `/enable_hdx_udp_ports`, além dessa opção `/enable_hdx_ports`.

- **/habilitar\\_hdx\\_udp\\_portas**

Abre portas UDP no firewall do Windows que o transporte adaptativo HDX usa, se o Serviço do Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente. Para obter informações sobre portas, consulte [Network ports](#).

Para abrir portas extras que o VDA usa, especifique a opção `/enable_hdx_ports`, além dessa opção `/enable_hdx_udp_ports`.

- **/enable\_hdx\_tls\_dtls**

Abre as portas TCP e UDP 443 para HDX Direct V1.

- **/habilitar transporte em\\_tempo real\\_**

Ativa ou desativa o uso de UDP para pacotes de áudio (transporte de áudio em tempo real para áudio). Ativar esse recurso pode melhorar o desempenho do áudio. Inclua a opção `/enable_hdx_ports` se quiser que as portas UDP sejam abertas automaticamente quando o Serviço de Firewall do Windows for detectado.

- **/enable\_remote\_assistance**

Ativa o recurso de sombreamento na Assistência Remota do Windows para uso com o Director. Se você especificar esta opção, a Assistência Remota do Windows abre as portas dinâmicas no firewall.

- **/enablerestore** ou **/enablerestorecleanup**

(Válido somente para VDAs de sessão única) Permite o retorno automático ao ponto de restauração, se a instalação ou atualização do VDA falhar.

Se a instalação/atualização for concluída com sucesso:

- `/enablerestorecleanup` instrui o instalador a remover o ponto de restauração.
- `/enablerestore` instrui o instalador a reter o ponto de restauração, mesmo que ele não tenha sido usado.

Para obter detalhes, consulte [Restaurar em caso de falha de instalação ou atualização](#).

• **`/habilitar\_ss\_ports`**

Abre portas no Firewall do Windows que são necessárias para o compartilhamento de tela, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente.

• **`/exclude`** “*componente*“\[,”*componente*“]

Impede a instalação de um ou mais componentes opcionais separados por vírgula, cada um entre aspas retas. 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 de SO de sessão única
Componente de proteção de aplicativo Citrix	Componente de proteção de aplicativo Citrix	Componente de proteção de aplicativo Citrix
Plug-in de Asserção de Identidade de Autenticação Citrix VDA	Plug-in de Asserção de Identidade de Autenticação Citrix VDA	Plug-in de Asserção de Identidade de Autenticação Citrix VDA
Citrix Backup and Restore	Citrix Backup and Restore	
Redirecionamento de conteúdo do navegador Citrix	Redirecionamento de conteúdo do navegador Citrix	Redirecionamento de conteúdo do navegador Citrix
Driver de filtro Citrix HyperV	Driver de filtro Citrix HyperV	
Citrix MCS IODriver	Citrix MCS IODriver	



SO multissessão	SO de sessão única	Serviços principais de SO de sessão única
Citrix Personalization <b>for</b> App-V - VDA	Citrix Personalization <b>for</b> App-V - VDA	Citrix Personalization <b>for</b> 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	
Citrix Telemetry Service	Citrix Telemetry Service	Citrix Telemetry Service
Citrix Universal Print Client	Citrix Universal Print Client	Citrix Universal Print Client
Serviço de captura de log Citrix Vda	Serviço de captura de log Citrix Vda	Serviço de captura de log Citrix Vda
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
Componente CSE	Componente CSE	Componente CSE
Plug-in Diretor VDA	Plug-in Diretor VDA	Plug-in Diretor VDA
Machine Identity Service	Machine Identity Service	
Provedor de gerenciamento de máquinas	Provedor de gerenciamento de máquinas	Provedor de gerenciamento de máquinas
	User Personalization Layer	
Plug-in <b>do</b> monitor VDA	Plug-in <b>do</b> monitor VDA	Plug-in <b>do</b> monitor VDA
Plug-in de proxy VDA WMI	Plug-in de proxy VDA WMI	Plug-in de proxy VDA WMI

A exclusão do 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 **User details** e **EndPoint**, o painel Personalization e o painel Logon Duration falham. Nas páginas **Dashboard** e **Trends**, o painel Average Logon Duration exibe dados somente para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Citrix Profile Management Service. A ativação do Citrix Profile Management Service não é necessária.

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, esse componente não será instalado.

Essa opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente muitos destes itens.

- **/h** ou **/help**

Exibe a ajuda do comando.

- **/includecomponente** “*adicional*“ [,”*component*“]

Inclui a instalação de um ou mais componentes opcionais separados por vírgula, cada qual entre aspas retas normais. Esta opção é útil quando você estiver criando uma implantação do Remote PC Access e quiser instalar outros componentes que não estão 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 <b>for</b> App-V – VDA	Citrix Personalization <b>for</b> 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
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent
Ferramenta de registro Citrix Web Socket Vda	Ferramenta de registro Citrix Web Socket Vda
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:\Arquivos de programas\Citrix`.

- **`/install_mcsio_driver`**

Não use. Em vez disso, use `/includeadditional` “Citrix MCS IODriver” ou `/exclude` “Citrix MCS IODriver”

- **`/logpath`** *caminho*

Localização do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = “%TEMP%\Citrix\XenDesktop Installer”

Esta opção não está disponível na interface gráfica.

- **`/masterimage`**

Válido somente ao instalar um VDA em uma VM. Configura o VDA como uma imagem para ser usada para criar outras máquinas. Essa opção é equivalente a `/mastermcsimage`.

Essa opção não é válida ao usar o instalador `VDAWorkstationCoreSetup_xxxx.exe`.

- **`/mastermcsimage`**

Especifica que a máquina será usada como uma imagem com Machine Creation Services. Essa opção é equivalente a `/masterimage`.

- **`/masterpvsimage`**

Especifica que a máquina será usada como uma imagem com o Citrix Provisioning ou com uma ferramenta de provisionamento de terceiros (como o Microsoft System Center Configuration Manager) para provisionar VMs.

- **`/websockettoken`** *websocketToken*

Cria um VDA do Web Socket. O WebSocketToken é para o token necessário.

- **`/no\_mediafoundation\_ack`**

Reconhece que o Microsoft Media Foundation não está instalado, e vários recursos multimídia HDX não serão instalados e não funcionarão. Se essa 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 vem com o Media Foundation já instalado, exceto as edições N. Se você habilitar o Windows Features > Media Features *manualmente*, a chave de registro procurada pelo Citrix Meta Installer pode não ter um valor definido. Verifique

a chave de registro `SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Setup\ Windows-Features\ WindowsMediaVersion` antes de iniciar o processo de instalação para confirmar se o valor existe e não está vazio.

- **/nodesktopexperience**

O recurso Enhanced Desktop Experience não está mais disponível. Esta opção (e configuração de política) é ignorada, se especificada.

Válido somente ao instalar um VDA de SO multissessão. Impede a ativação do recurso Enhanced Desktop Experience. Esse recurso também é controlado com a configuração de política Enhanced Desktop Experience Citrix.

- **/noreboot**

Impede uma reinicialização após a instalação. O VDA não pode ser usado até que seja reinicializado.

- **/noresume**

Por padrão, quando uma reinicialização de máquina é necessária durante uma instalação, o instalador continua automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso é útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/physicalmachine**

Use esse argumento junto com `/remotepc` para instalação do RemotePC. Caso contrário, o VDA pode não se comportar conforme o esperado em determinados cenários do usuário.

- **/portnumber** *porta*

Válido somente quando a opção `/reconfig` é especificada. Número da porta a ativar para comunicações entre o VDA e o Controller. A porta configurada anteriormente é desabilitada, a menos que seja a porta 80.

- **/proxyconfig** “*endereço ou caminho do arquivo PAC*”

Se você planeja usar o protocolo Rendezvous com o Gateway Service, o VDA Upgrade Service etc. em seu ambiente e tem um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Somente proxies HTTP são aceitos. O endereço ou o caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para obter detalhes do recurso, consulte [Protocolo Rendezvous](#).

- Formato do endereço proxy: `http://<url-or-ip>:<port>`
- Formato de arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** ou **/passive**

Nenhuma interface de usuário aparece durante a instalação. A única evidência do processo de instalação e configuração está no Gerenciador de Tarefas do Windows. Se esta opção for omitida, a interface gráfica será iniciada.

- **/reconfigure**

Personaliza as configurações de VDA definidas anteriormente quando usadas com as opções `/portnumber`, `/controllersou` `/enable_hdx_ports`. Se você especificar essa opção sem especificar também a opção `/quiet`, a interface gráfica para personalizar o VDA será iniciada.

- **/remotepc**

Válido somente para implantações de Remote PC Access (SO de sessão única) ou conexões agenciadas (SO multissessão). Exclui a instalação de quaisquer componentes adicionais (consulte as listas de componentes com as opções `/exclude` e `/includeadditional`).

Essa opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente a instalação destes componentes.

`/remotepc` não é compatível com a opção `/servervdi`.

- **/remove**

Remove os componentes especificados com a opção `/components`.

- **/remove\_appdisk\_ack**

Autoriza o instalador de VDA a desinstalar o plug-in AppDisks VDA se ele estiver instalado.

- **/remove\_pvd\_ack**

Autoriza o instalador de VDA a desinstalar o Personal vDisk se ele estiver instalado.

- **/removeall**

Remove o VDA. Ele não remove o aplicativo Citrix Workspace (se instalado).

- **/REMOVA TUDO COM CWA**

Remove o CWA junto com o VDA.

- **/sendexperiencemetrics**

Envia automaticamente análises coletadas durante a instalação, atualização ou remoção para a Citrix. Se essa opção for omitida (ou a opção `/disableexperiencemetrics` for especificada), as análises serão coletadas localmente, mas não enviadas automaticamente.

- **/servervdi**

Instala um VDA de SO de sessão única em uma máquina multissessão Windows suportada. Omita esta opção quando instalar um VDA de SO multissessão em uma máquina multissessão Windows.

Antes de usar essa opção, consulte [Server VDI](#).

Use esta opção somente com o instalador de VDA de produto completo.

- **`/site\_guid`** *guid*

Identificador Globalmente Exclusivo da Unidade Organizacional (UO) do Active Directory do site. Associa uma área de trabalho virtual a um site quando você estiver usando o Active Directory para descoberta (a atualização automática é o método de descoberta recomendado e o padrão). O GUID do site é uma propriedade do site exibida no Studio. Não especifique as opções `/site\_guide` e `/controllers`.

- **`/tempdir`** *diretório*

Diretório para manter os arquivos temporários durante a instalação. Padrão = c:\ Windows\Temp.

Esta opção não está disponível na interface gráfica.

- **`/virtualmachine`**

Válido somente ao instalar um VDA em uma VM. Substitui a detecção pelo instalador de uma máquina física, onde as informações do BIOS passadas para as VMs fazem com que elas apareçam como máquinas físicas.

Esta opção não está disponível na interface gráfica.

- **`/xendesktopcloud`**

Indica que o VDA está instalado em uma implantação do Citrix DaaS (Citrix Cloud).

## Exemplos de instalação de um VDA

### Instalar um VDA com o instalador de produto completo:

O comando a seguir instala um VDA de SO de sessão única e o aplicativo Citrix Workspace no local padrão em uma VM. Este VDA será usado como uma imagem e usa o MCS para provisionar VMs. O VDA será registrado inicialmente com o Controller no servidor chamado `Contr-Main` no domínio `mydomain`. O VDA usará a camada de personalização do usuário e a Assistência Remota do Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,  
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /  
includeadditional "camada de personalização do usuário"/mastermcsimage  
/enable_remote_assistance
```

### Instale um VDA de SO de sessão única com o instalador autônomo `VDAWorkstationCoreSetup`:

O comando a seguir instala um Core Services VDA em um SO de sessão única para uso em um Remote PC Access ou implantação VDI. O aplicativo Citrix Workspace e outros serviços não principais não são instalados. O endereço de um Controller é especificado e as portas no Serviço do Firewall do Windows serão abertas automaticamente. O administrador lidará com as reinicializações.

```
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, descritas em Opções de linha de comando para instalar um VDA.

- `/reconfigure` (necessário ao personalizar um VDA)
- `/h` ou `/help`
- `/quieto`
- `/noreboot`
- `/controllers`
- `/portnumber porta`
- `/enable_hdx_ports`

## Solucionar problemas de VDAs

- Na tela do Studio de um grupo de entrega, a entrada **Installed VDA version** no painel **Details** pode não refletir 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 Servidor de Impressão Universal

A opção a seguir é válida com o comando `XenDesktopPrintServerSetup.exe`.

- `/enable_upsserver_port`

Quando esta opção não for especificada, o instalador exibe a página de **Firewall** a partir da interface gráfica. Selecione **Automatically** para que o instalador adicione automaticamente as regras de

firewall do Windows, ou **Manually** para permitir que o administrador configure manualmente o firewall.

Depois de 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 acesso privado seguro

As opções a seguir são válidas com:

1. Instalador do CVAD: `XenDesktopSPASetup.exe`
2. Instalador local do SPA: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable\_spa\_ports**

Abre 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 habilitado. Se estiver usando um firewall diferente (ou se não estiver usando um firewall), você deve configurar o firewall manualmente. Para obter informações sobre portas, consulte [Network ports](#).

- **/nosql**

Impede a instalação do Microsoft SQL Server Express no servidor em que você está instalando o Secure Private Access. Se esta opção for omitida, o SQL Server Express é instalado para uso como o banco de dados do site.

- **/help ou /h ou/?**

Exibe a ajuda do comando

- **/noreboot**

Impede uma reinicialização após a instalação. O Secure Private Access não pode ser usado até depois 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.

- **/remove**

Remove o acesso privado seguro.

Para obter mais detalhes sobre as opções, consulte [Secure Private Access installer](#).



## Mais informações

Para obter informações sobre como a Citrix relata o resultado das instalações de componentes, consulte [Códigos de retorno de instalação da Citrix](#).

## Instale o Web Studio

January 24, 2025

### 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 de [a interface](#) do Citrix DaaS Studio, o Web Studio moderniza sua experiência de gerenciamento fornecendo uma experiência nativa na web.

Você pode implantar o Web Studio em qualquer servidor Windows com o Internet Information Service (IIS) instalado. Há duas opções de implantação:

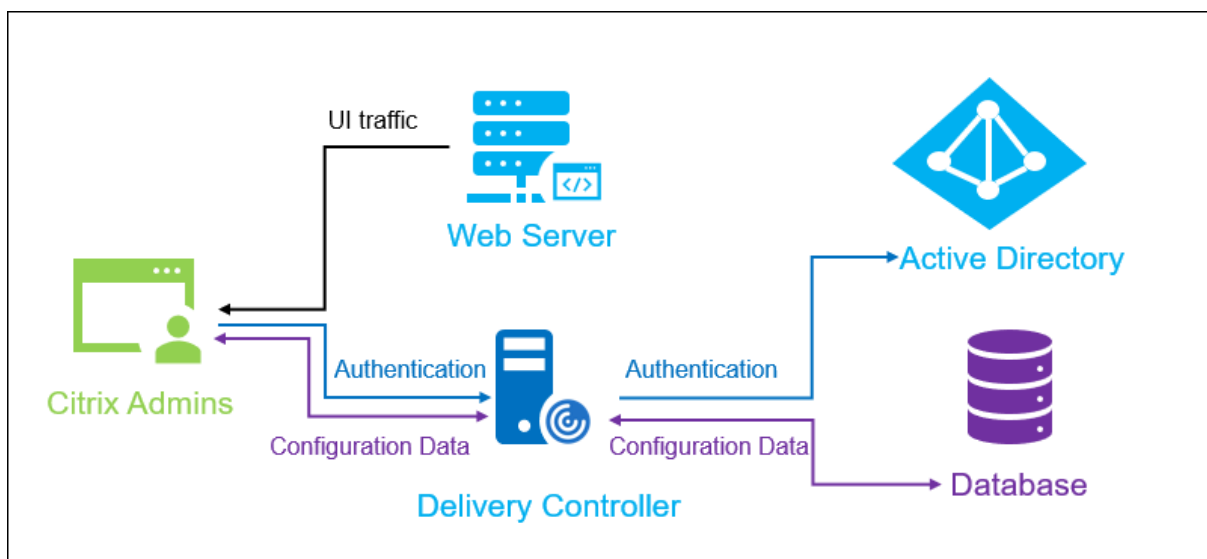
- Instalado em um servidor dedicado:

Para ambientes maiores em que o desempenho e a escalabilidade são essenciais, recomendamos instalar o Web Studio em um servidor dedicado. Opcionalmente, esse servidor também pode hospedar o Diretor.

- Integrado com um controlador de entrega:

Para implantações rápidas e ambientes mais simples, instale o Web Studio diretamente em um Delivery Controller. Essa abordagem é ideal para implantações menores, nas quais 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. Instale o Web Studio.
2. Configure um site.
3. Adicione controladores de entrega ao Web Studio para gerenciamento.
4. Faça login no Web Studio.

Para configurar uma implantação do Web Studio com balanceamento de carga, consulte [neste artigo](#).

## Novos recursos disponíveis no Web Studio

Veja o artigo [What's new](#).

## Requisitos do sistema

Sistemas operacionais compatíveis:

- Servidor Windows 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 compatíveis:

- Microsoft Edge 92
- Firefox ESR (versão de suporte estendido) 90

- Google Chrome 92
- Safári 14

A resolução de tela ideal recomendada para visualização do 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 versões posteriores.

Para implantações anteriores à 2212, primeiro atualize para 2212 e depois instale o Web Studio.

## Limitações conhecidas

Se você usa o Web Studio e o Citrix Studio de forma intercambiável, considere a seguinte limitação: Um modelo criado no Web Studio não é mostrado 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). Qualquer alteração no nome padrão do site resultará em falhas na instalação.

## Instale o Web Studio

As informações a seguir são um complemento à orientação em [Instalar componentes principais](#). Para instalar o Web Studio:

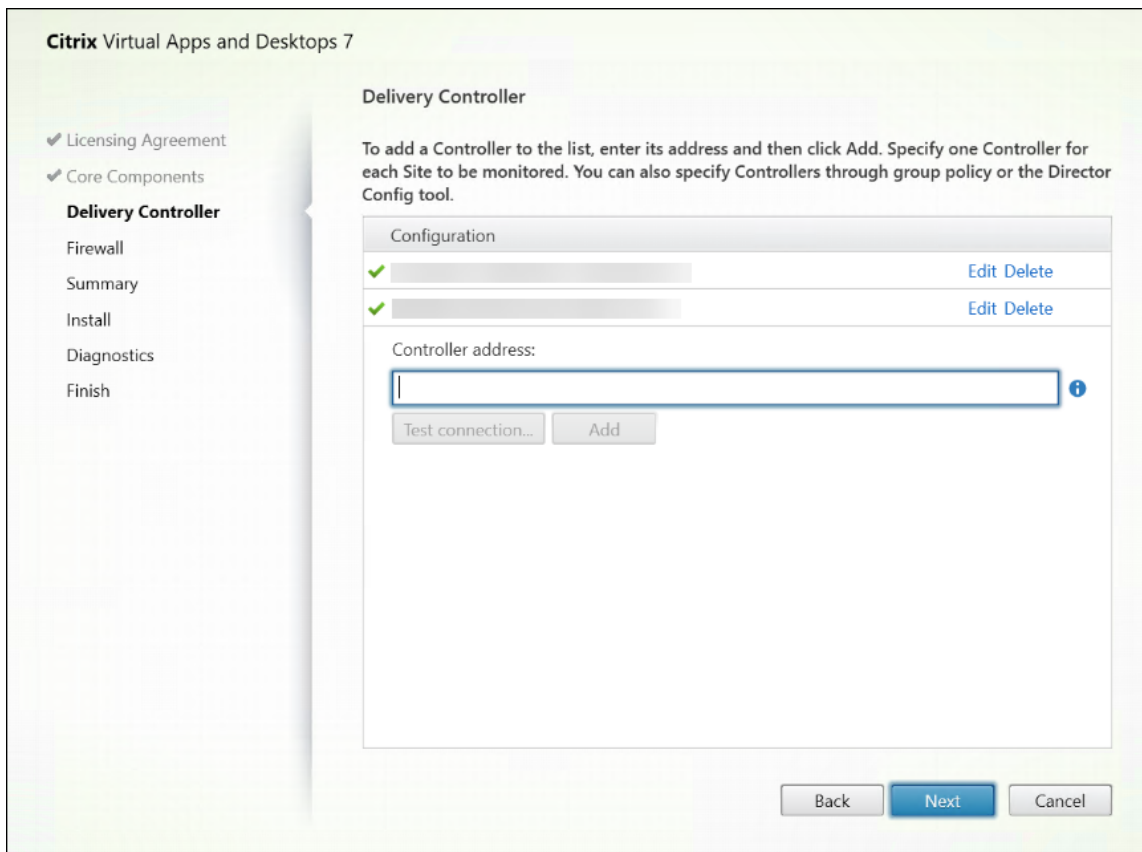
- Instale o Web Studio usando o instalador ISO completo do produto para Citrix Virtual Apps and Desktops. O instalador ISO verifica os pré-requisitos, instala os componentes ausentes, configura o site do Web Studio (no Delivery Controller, se incluído na instalação do Delivery Controller) e executa a 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 é solicitado a digitar o endereço de um Delivery Controller.

### Nota:

- 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 retornará para outros Delivery Controllers.

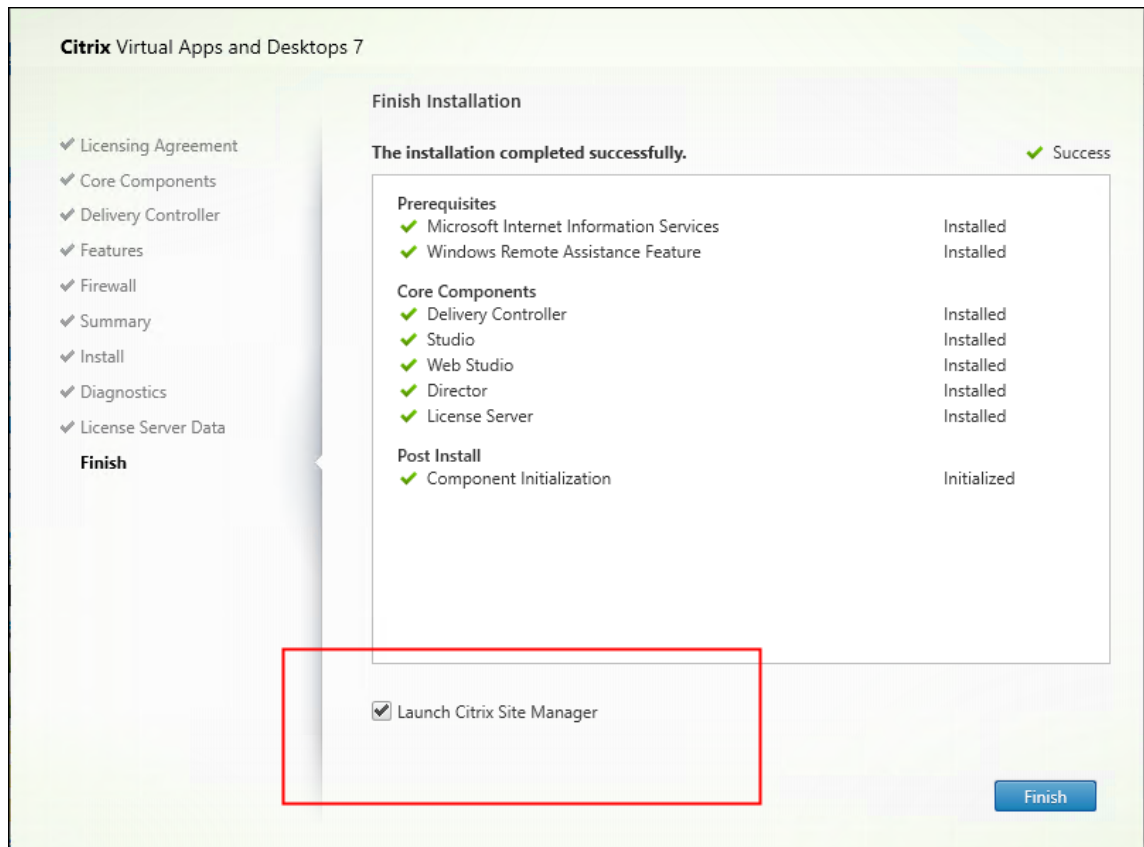
- Se o Director tiver sido selecionado em **Core Components** e instalado, os Delivery Controllers que você adicionar aqui serão usados tanto para o Web Studio quanto para o Director.
- Se você não tiver o certificado de confiança público externo configurado e não quiser solicitar o certificado de uma CA corporativa, basta configurar o FQDN do seu Delivery Controller.
- Se você tiver o certificado de confiança público externo e puder configurar o DNS público para seu Delivery Controller, poderá digitar o nome DNS como o endereço do Delivery Controller.
- Se você puder solicitar o certificado de sua CA corporativa e especificar seu DNS pessoal, poderá adicionar seu DNS pessoal como endereço do Delivery Controller.



- Para proteger as comunicações entre o navegador e o servidor web e entre o navegador e o Delivery Controller, a criptografia TLS deve estar habilitada no site do IIS que hospeda o Web Studio e no Delivery Controller. Se nenhum certificado TLS estiver 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 estiver configurado, o instal-

ador não fará nenhuma alteração. Para obter mais informações sobre criptografia TLS, consulte [Proteger uma implantação do Web Studio \(opcional\)](#).

- Na página **Finish**, a caixa de seleção **Launch Site Manager** é marcada por padrão para que o Citrix Site Manager seja aberto automaticamente. Para iniciá-lo mais tarde, abra o menu Iniciar do seu desktop 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](#).



**Nota:**

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 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 defina suas configurações da seguinte forma:
  - Na página **Introdução**, digite um nome para o site.
  - A página **Databases** contém seleções para configurar o site, monitorar e configurar bancos de dados de log. Para obter mais informações, consulte [Etapa 3. Bancos de dados](#).
  - Na página **Licensing**, 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 **Summary**, verifique todas as configurações e clique em **Submit**.

O endereço IP deste Controlador é adicionado automaticamente ao site.

**Nota:**

O usuário que cria um site se torna administrador completo do site. Para obter mais informações, consulte [Administração delegada](#).

Se você instalar um novo Controller depois de criar um site, deverá adicionar o Controller ao site. As etapas detalhadas são as seguintes:

1. Execute o Citrix Site Manager neste novo controlador.
2. Selecione **Ingressar em um site existente**.
3. Digite o endereço de um controlador que já foi adicionado ao site.
4. Clique em **Enviar**.

## Adicione controladores de entrega ao Web Studio para gerenciamento

Use a ferramenta de configuração do Studio para adicionar os Delivery Controllers ao Web Studio para gerenciamento. Essa 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 deseja gerenciar com o Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Execute o seguinte comando do PowerShell:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

**Nota:**

- A ferramenta requer permissões de administrador do computador.
- As alterações na configuração do Delivery Controller podem não entrar em vigor imediatamente devido às configurações de cache no servidor IIS. Para obter efeito imediato, acesse o servidor Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegue até Página Inicial > Sites > Site Padrão e selecione **Reiniciar** no painel Gerenciar site.
- Para ver 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 ao servidor do Web Studio e aos Delivery Controllers por meio do navegador da web. Fornecemos a opção de configurar o servidor do Web Studio como proxy para Delivery Controllers. Como resultado, você se conecta somente ao servidor do Web Studio ao gerenciar sua implantação.

Esta seção orienta você a configurar um servidor Web Studio como proxy para Delivery Controllers. Presumimos que o Web Studio e o Delivery Controllers estejam 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 ativar o modo proxy para o Web Studio, siga estas etapas:

1. No servidor Web Studio, execute o Windows PowerShell como administrador.
2. Execute o comando a seguir para substituir `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"
```

**Nota:**

Se você tiver uma implantação do Web Studio com balanceamento de carga, substitua `fqdn_of_webstudio_machine` pelo FQDN do servidor do balanceador de carga (também conhecido como servidor virtual). Para obter mais informações, consulte [Configurar uma implantação do Web Studio com balanceamento de carga](#).

Para desativar o modo proxy para o Web Studio, execute este comando do PowerShell:

```
1 `& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --  
  disableproxy`
```

**Nota:**

Como prática recomendada, recomendamos que você proteja sua implantação do Web Studio usando um certificado de confiança público externo ou um certificado de uma Autoridade Certificadora (CA) corporativa. Para obter mais informações, consulte [Proteger uma implantação do Web Studio](#).

## Faça login no Web Studio

O site do Web Studio está localizado em <https://<address of the server hosting Web Studio>/Citrix/Studio>.

Para fazer login no Web Studio, abra o menu Iniciar do seu desktop e selecione **Citrix > Citrix Web Studio**. Os administradores com permissões para o Web Studio devem ser usuários do domínio Active Directory. Ao fazer login no Web Studio, considere os seguintes cenários:

- Se você ainda não especificou controladores de entrega para o site. Você será solicitado a especificar um Delivery Controller para ter acesso temporário ao Web Studio.
- Se os Delivery Controllers especificados estiverem atualmente inacessíveis, você não poderá fazer login no Web Studio. Teste suas conexões para se certificar de que esses Delivery Controllers estejam acessíveis. Ou especifique um Delivery Controller alternativo para que você tenha acesso temporário ao Web Studio.

## Próximas etapas

1. [Instale VDAs](#)
2. Use o Web Studio para fornecer 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 VDAs

November 5, 2024



**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 estão assinados. Os binários assinados indicam que eles são validados por certificados gerados pela Citrix ou por certificados autênticos de terceiros.

Existem dois tipos de VDAs para máquinas Windows: VDA para SO multissessão e VDA para SO de sessão única. (Para obter informações sobre máquinas VDAs para Linux, consulte a documentação do [Linux Virtual Delivery Agent](#).)

Antes de iniciar uma instalação, revise [Preparar para instalar](#) e conclua todas as tarefas de preparação.

Antes de instalar VDAs, instale os componentes principais. Você também pode criar o site antes de instalar VDAs.

Este artigo descreve a sequência do assistente de instalação ao instalar um VDA. Equivalentes de linhas 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 do produto completo:

1. Se você ainda não baixou o ISO do produto:
  - Use as credenciais da sua conta da 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 na 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.

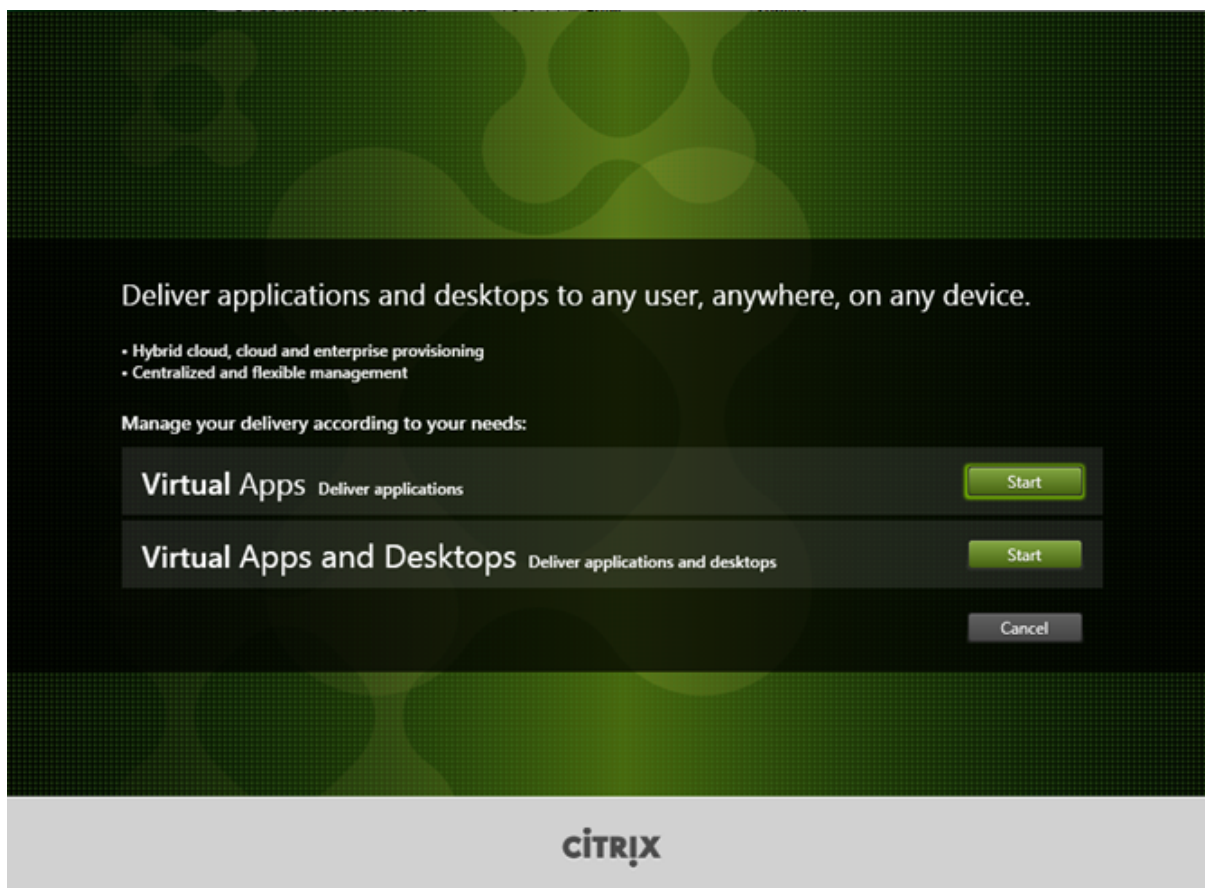
O assistente de instalação é iniciado.

Se você estiver usando um pacote autônomo:

1. Use as credenciais da sua conta da Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o pacote apropriado:
  - [VDAServerSetup\\_2402.exe](#): Sistema operacional multissessão VDA *versão*
  - [VDAWorkstationSetup\\_2402.exe](#): OS VDA de sessão única *versão*

- [VDAWorkstationCoreSetup\\_2402.exe](#): OS Core Services de sessão única VDA versão
2. Clique com o botão direito no pacote e escolha **Executar como administrador**.  
O assistente de instalação é iniciado.

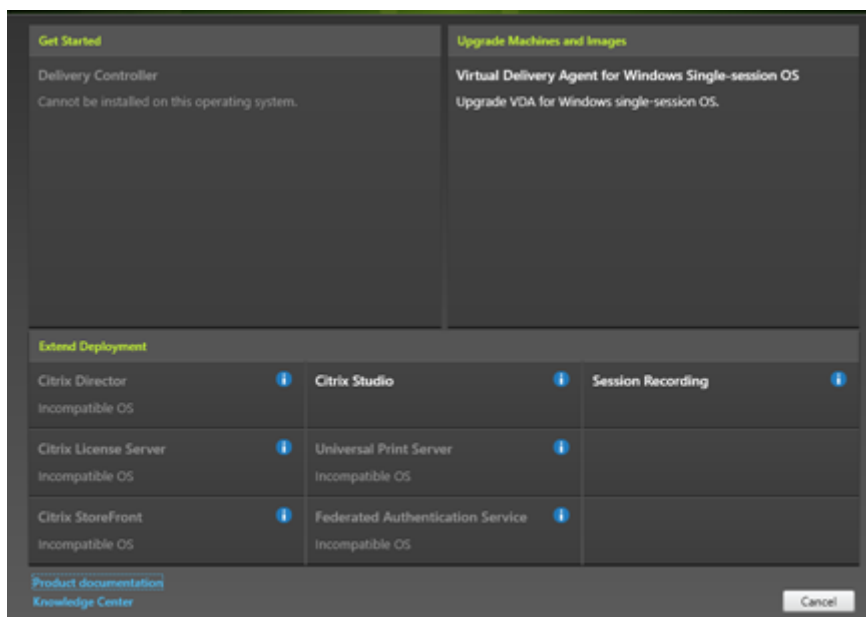
## Etapa 2. Escolha qual produto instalar



Clique em **Start** 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 será exibida.)

Opção de linha de comando: `/xenapp` para instalar o Citrix Virtual Apps. O Citrix Virtual Desktops é instalado se essa opção for omitida.

### Etapa 3. Seleção o VDA

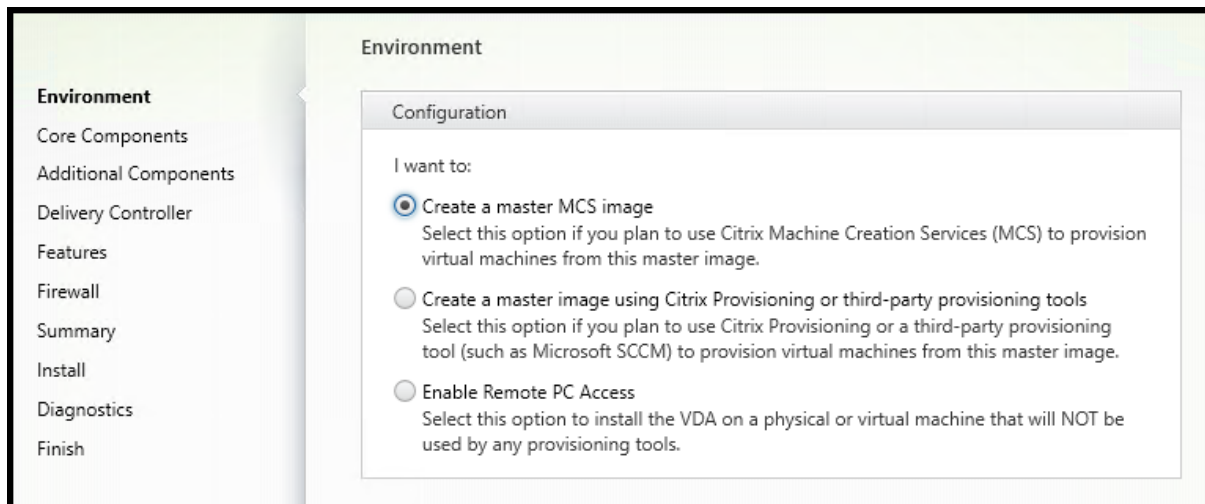


Selecione a entrada **Virtual Delivery Agent**. O instalador sabe se ele está sendo executado em um sistema operacional de sessão única ou multissessão, senso assim oferece apenas o tipo de VDA apropriado.

Por exemplo, quando você executa o instalador em uma máquina Windows Server 2019, a opção de VDA para SO multissessão está disponível. A opção VDA para SO de sessão única não é oferecida.

Se você tentar instalar (ou atualizar para) um Windows VDA em um sistema operacional que não é compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem orientará você sobre como obter informações sobre as opções.

## Etapa 4. Especifique como o VDA será usado



Na página **Environment**, especifique como você planeja usar o VDA, indicando se você usa essa máquina como uma imagem para provisionar mais máquinas.

A opção escolhida afeta quais ferramentas do Citrix Provisioning são instaladas automaticamente (se houver) e os valores padrão na página Componentes adicionais do instalador do VDA.

Vários MSIs (provisionamento e outros) são instalados automaticamente quando você instala um VDA. A única maneira de impedir sua instalação é com a opção `/exclude` em uma instalação por linha de comando.

Escolha uma das seguintes opções:

- **Create a master MCS image:** selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar Machine Creation Services para provisionar VMs. Esta opção instala o Machine Identity Service. Esta é a opção padrão.

Opção de linha de comando: `/mastermcsimage` ou `/masterimage`

### Importante:

A mídia de instalação ou a imagem ISO deve ser montada localmente. A montagem de uma imagem ISO fora de uma unidade de rede para fins de instalação de software não é suportada.

- **Create a master image using Citrix Provisioning or third-party provisioning tools:** selecione esta opção para instalar um VDA em uma imagem de VM, se você planeja usar o Citrix Provisioning ou ferramentas de provisionamento de terceiros (como o Microsoft System Center Configuration Manager) para provisionar VMs.

Opção de linha de comando: `/masterpvsimage`

- (Aparece somente em máquinas com sistema operacional multissessão) **Habilitar conexões intermediadas com um servidor:** Selecione essa opção para instalar um VDA em uma máquina física ou virtual que não será usada como imagem para provisionar outras máquinas.

Opção de linha de comando: `/remotepc`

- (Aparece apenas em máquinas de SO de sessão única) **Enable Remote PC Access:** selecione esta opção para instalar um VDA em uma máquina física para usar com o Remote PC Access.

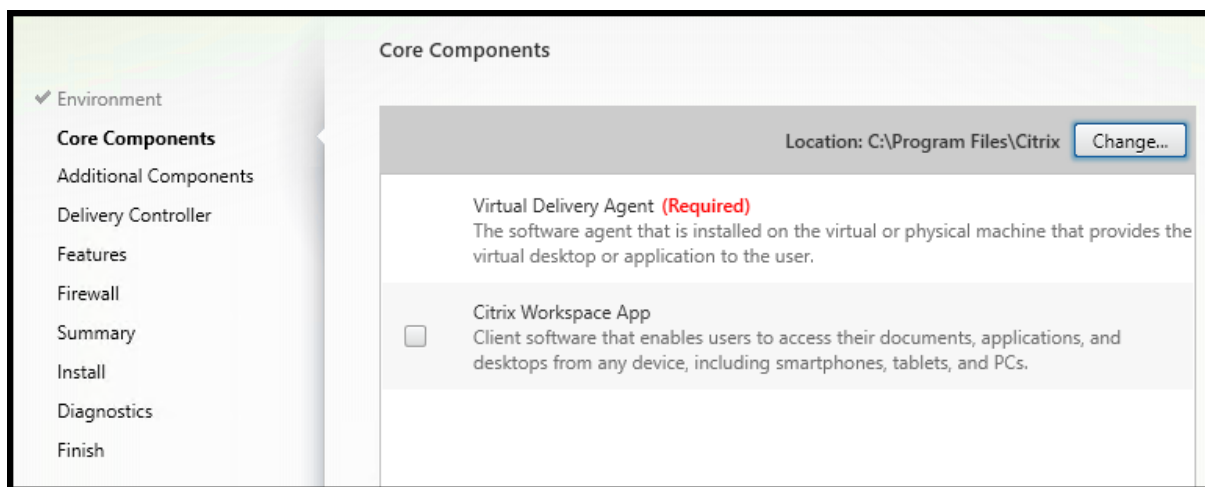
Opção de linha de comando: `/remotepc`

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 para instalar e o local de instalação



Na página **Core components**:

- **Localização:** 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 as permissões `execute` para o serviço de rede.
- **Components:** por padrão, o aplicativo Citrix Workspace para Windows não é instalado com o VDA. Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`, o aplicativo Citrix Workspace para Windows nunca será instalado, portanto, essa caixa de seleção não será exibida.

Clique em **Avançar**.

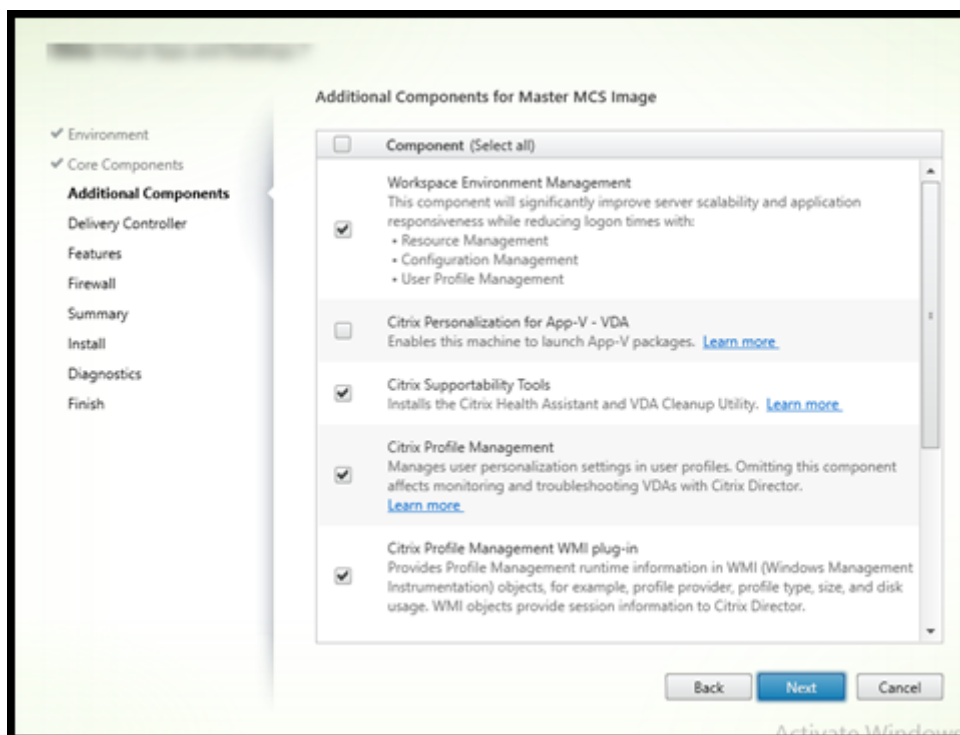
Opções de linha de comando: `/installdir`, `/components vda`, `plugin` para instalar o VDA e o aplicativo Citrix Workspace para Windows

### Observação:

Você pode optar por instalar, atualizar ou desinstalar o aplicativo Citrix Workspace durante a instalação, atualização ou desinstalação de um VDA nos seguintes cenários:

- Durante a instalação do VDA, você pode optar por instalar o aplicativo Citrix Workspace. Por padrão, o aplicativo Citrix Workspace não é instalado durante a instalação do VDA.
- Durante uma atualização do VDA, se o aplicativo Citrix Workspace ainda não estiver instalado no VDA, você poderá optar por instalar o aplicativo Citrix Workspace.
- Durante uma atualização do VDA, se a versão do aplicativo Citrix Workspace puder ser atualizada, a opção de atualizar o aplicativo Citrix Workspace será exibida.
- Durante a desinstalação do VDA, você pode optar por não desinstalar o aplicativo Citrix Workspace. Por padrão, o aplicativo Citrix Workspace é desinstalado durante a desinstalação do VDA.

## Etapa 6. Instale componentes adicionais



A página **Componentes adicionais** contém caixas de seleção para ativar ou desativar a instalação de outros recursos e tecnologias com o VDA. Em uma instalação por linha de comando, você pode usar a opção `/exclude` ou `/includeadditional` para omitir ou incluir expressamente um ou mais componentes disponíveis.

A tabela a seguir indica a configuração padrão dos itens nessa página. A configuração padrão depende da opção selecionada na página **Environment**.

Página Additional Components	Página Environment: “Master image with MCS” ou “Master image with Citrix Provisioning” selecionado	Página Environment: “Enable brokered connections to server”(para SO multissessão) ou “Remote PC Access”(para SO de sessão única) selecionado
Citrix Personalization for App-V - VDA	Não selecionado	Não selecionado
User Personalization Layer	Não selecionado	Não é mostrado 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 and Restore	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.

Marque 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 usar aplicativos de pacotes do 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 permitir a instalação de componentes, `/exclude “Citrix Personalization for App-V — VDA”` para impedir a instalação de componentes.

- **Citrix User Personalization Layer:** instala o MSI para a camada de personalização do usuário. Para obter detalhes, consulte [Camada de personalização do usuário](#).



Este componente aparece somente ao instalar um VDA em um computador Windows 10 de sessão única.

Opção de linha de comando: `/includeadditional "Camada de personalização do usuário"` para habilitar a instalação do componente, `/exclude "Camada de personalização do usuário"` 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 [Profile Management](#).

Excluir Citrix Profile Management da instalação afeta o monitoramento e a solução de problemas de VDAs com o Citrix Director. Nas páginas **User details** e **End Point**, o painel **Personalization** e o painel **Logon Duration** falham. Nas páginas **Dashboard** e **Trends**, o painel **Average Logon Duration** exibe dados somente para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de gerenciamento de perfil de usuário de terceiros, a Citrix recomenda que você instale e execute o Citrix Profile Management Service. A ativação do Citrix Profile Management Service não é necessária.

Opção de linha de comando: `/includeadditional "Citrix Profile Management"` para permitir a instalação de componentes, `/exclude "Citrix Profile Management"` para impedir a instalação de componentes.

- **Plug-in WMI do Citrix Profile Management:** Esse 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 do disco). Objetos WMI fornecem informações da sessão ao Director.

Opção de linha de comando: `/includeadditional "Citrix Profile Management WMI Plug-in"` para permitir a instalação de componentes, `/exclude "Citrix Profile Management WMI Plug-in"` para impedir a instalação de componentes.

- **VDA Upgrade Agent:** aplicável apenas a implantações do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Permite que o VDA participe do [recurso VDA Upgrade](#). Você pode usar esse recurso para atualizar os VDAs de um catálogo a partir do console de gerenciamento, imediatamente ou em um horário agendado. Se esse agente não estiver instalado, você poderá atualizar um VDA executando o instalador do VDA na máquina.

Opções de linha de comando: `/includeadditional "Citrix VDA Upgrade Agent"` para permitir a instalação de componentes, `/exclude "Citrix VDA Upgrade Agent"` para impedir a instalação de componentes.

- **Cache de gravação MCSIO para otimização de armazenamento:** Instala o driver de E/S Citrix MCS. 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 permitir a instalação de componentes, `/exclude "Citrix MCS IODriver"` para impedir a instalação de componentes.

- **Configuração de proxy:** Instale este componente se você planeja usar o protocolo Rendezvous com o Gateway Service, o VDA Upgrade Service etc. em seu ambiente e tiver um proxy não transparente em sua rede para conexões de saída, especifique o proxy aqui. Somente proxies HTTP são aceitos.

Se você instalar esse componente, especifique o endereço do proxy ou caminho do arquivo PAC na página **Rendezvous Proxy Configuration**. Para obter detalhes do recurso, consulte [Protocolo Rendezvous](#).

Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para ativar a instalação de componentes, `/exclude "Citrix Rendezvous V2"` para impedir a instalação de componentes.

- **Citrix Backup and Restore:** Se a instalação ou atualização de um VDA falhar, esse componente poderá retornar a máquina a um backup que foi feito antes da instalação ou atualização.

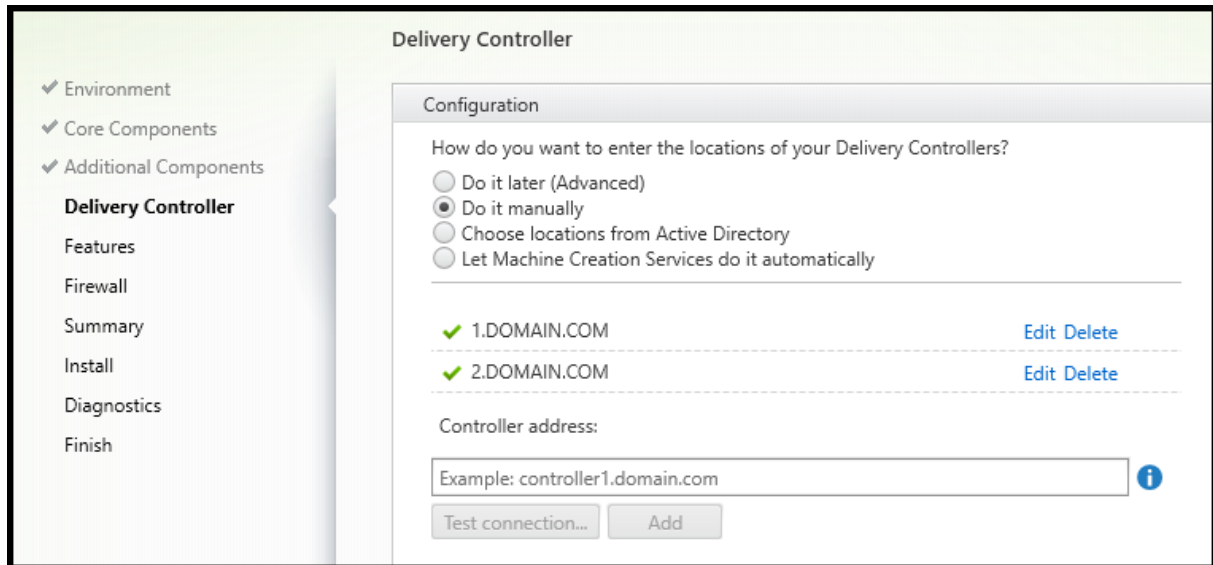
Certifique-se de que os pré-requisitos da Microsoft sejam atendidos conforme mencionado em [Prepare-se para instalar](#).

Opção de linha de comando: `/includeadditional "Citrix Backup and Restore"` para permitir a instalação de componentes, `/exclude "Citrix Backup and Restore"` para impedir a instalação de componentes.

**Observação:**

Se a otimização de armazenamento do MCS estiver ativada, o backup ou a restauração do sistema operacional Windows Server ou desktop poderão falhar. Para resolver isso, desative a opção de otimização de armazenamento MCS no metainstalador.

## 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 (**Do it manually**). O VDA não pode se registrar com um Controller até que tenha a informação. Se um VDA não puder se registrar, os usuários não poderão acessar aplicativos e áreas de trabalho nesse VDA.

- **Do it manually:** (padrão) incorpore o FQDN de um Controller instalado e clique em **Add**. Se você instalou mais Controllers, adicione seus endereços.
- **Do it later (Advanced):** se escolher esta opção, o assistente solicitará que você confirme que deseja fazer isso antes de continuar. Para especificar endereços posteriormente, você pode executar novamente o instalador ou usar a política de grupo da Citrix. O assistente também o lembra na página **Summary**.
- **Choose locations from Active Directory:** válido somente quando a máquina é associada a um domínio e o usuário é um usuário do domínio.
- **Use o token WebSocket (prévia técnica):** Cria um VDA WebSocket. O WebSocketToken é para o token necessário.
- **Let Machine Creation Services do it automatically:** válido somente ao usar o MCS para provisionar máquinas.

Clique em **Avançar**. Se selecionou **Do it later (Advanced)**, você será solicitado a confirmar que especificará os endereços do Controller posteriormente.

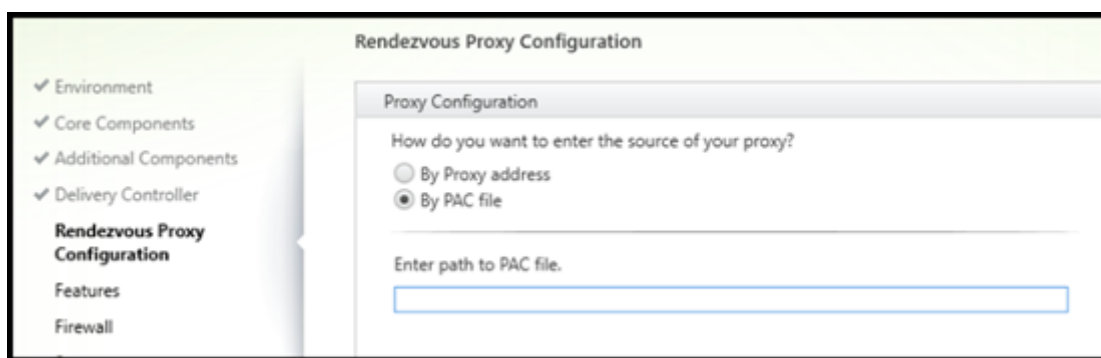
Outras considerações:

- 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 substituem as configurações fornecidas durante a instalação.

- O registro bem-sucedido do VDA exige que as portas de firewall usadas para se comunicar com o Controller estejam abertas. Essa ação é ativada por padrão na página **Firewall** do assistente.
- Depois de especificar as localizações 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 [VDA registration](#).

Opção de linha de comando: `/controllers`

## Etapa 8. Configuração de proxy



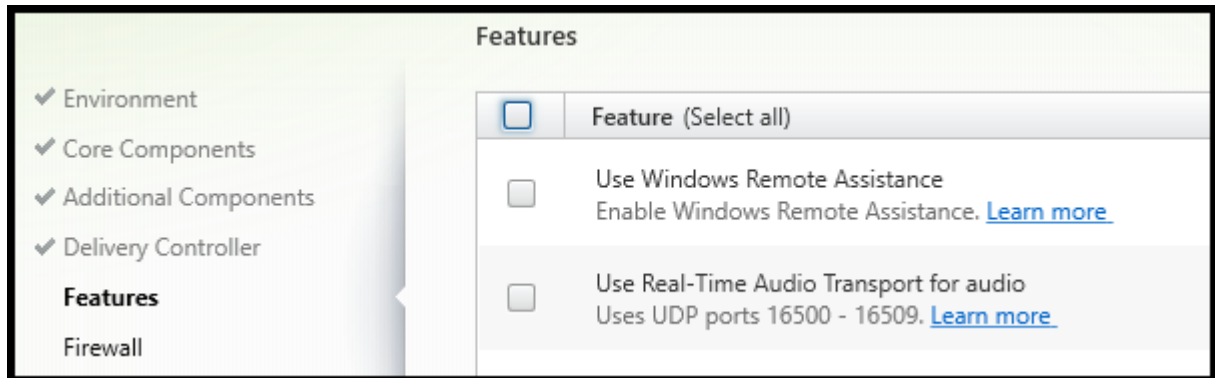
A página **Proxy Configuration** aparece somente se você tiver ativado a caixa de seleção **Proxy Configuration** na página **Additional Components**.

1. Selecione se você especificará a origem do proxy por endereço proxy ou caminho do arquivo PAC.
2. Especifique o endereço proxy ou o caminho do arquivo PAC.
  - Formato do endereço proxy: `http://<url-or-ip>:<port>`
  - Formato de arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

O firewall da porta proxy deve estar aberto para que o teste de conexão seja realizado. Se não for possível estabelecer uma conexão com o proxy, você pode decidir se deseja continuar com a instalação do VDA.

Opção de linha de comando: `/proxyconfig`

## Etapa 9. Ativar ou desativar recursos



Na página **Features**, use as caixas de seleção para ativar ou desativar os recursos que deseja usar.

- **Use Windows Remote Assistance:** quando este recurso está ativado, a Assistência Remota do Windows é usada com o recurso de sombreamento do usuário do Director. A Assistência Remota do Windows abre as portas dinâmicas no firewall. (Padrão = desativado)

Opção de linha de comando: `/enable_remote_assistance`

- **Use Real-Time Audio Transport for audio:** ative este recurso se Voice-over-IP for amplamente utilizado em sua rede. O recurso reduz a latência e melhora a resiliência de áudio em redes com perdas. Ele permite que os dados de áudio sejam transmitidos usando o transporte RTP sobre UDP. (Padrão = desativado)

Opção de linha de comando: `/enable_real_time_transport`

- **Use screen sharing:** Quando ativado, as portas usadas pelo compartilhamento de tela são abertas no firewall do Windows. (Padrão = desativado)

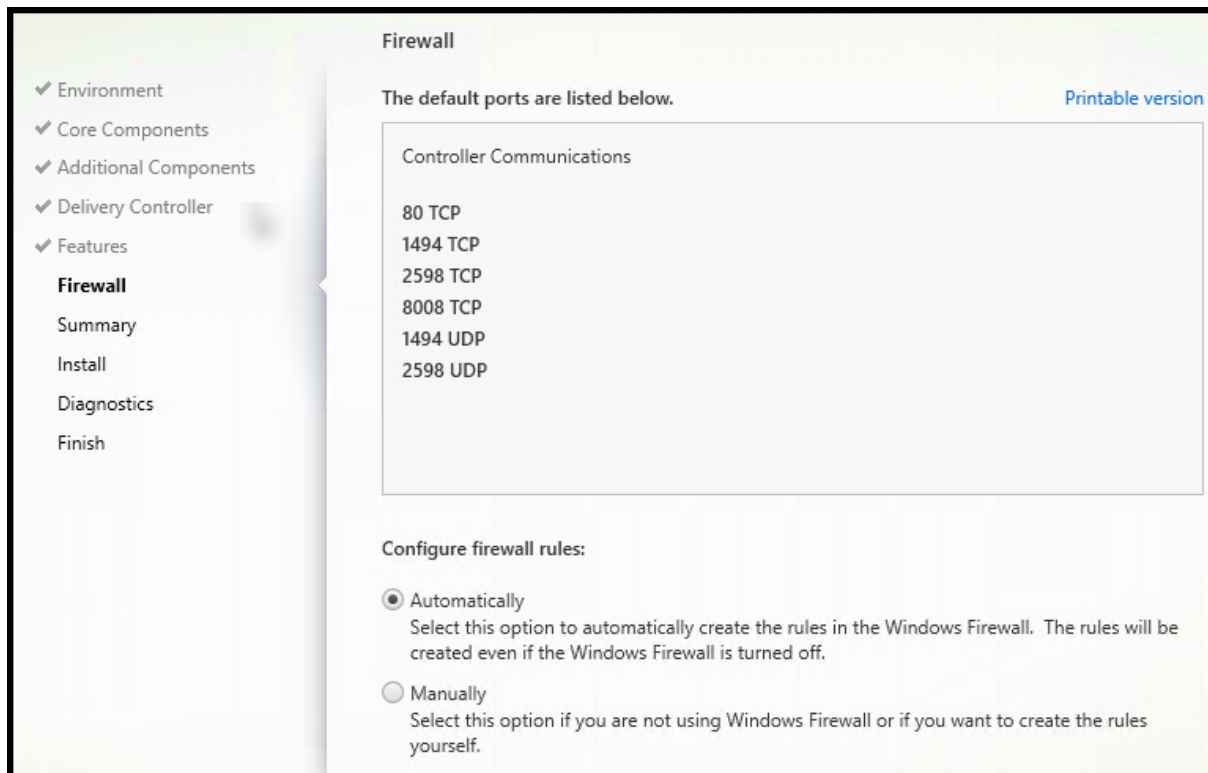
Opção de linha de comando: `/enable_ss_ports`

- **Is this VDA installed on a VM in a cloud:** essa configuração ajuda a Citrix a identificar corretamente os locais de recursos para implantações de VDA no local e de serviço (Citrix Cloud) para fins de telemetria. Esse recurso não tem impacto na utilização do lado do cliente. Ative essa configuração se a sua implantação usar Citrix DaaS (Padrão = desativada).

Opção de linha de comando: `/xendesktopcloud`

Clique em **Avançar**.

## Etapa 10. Portas de firewall

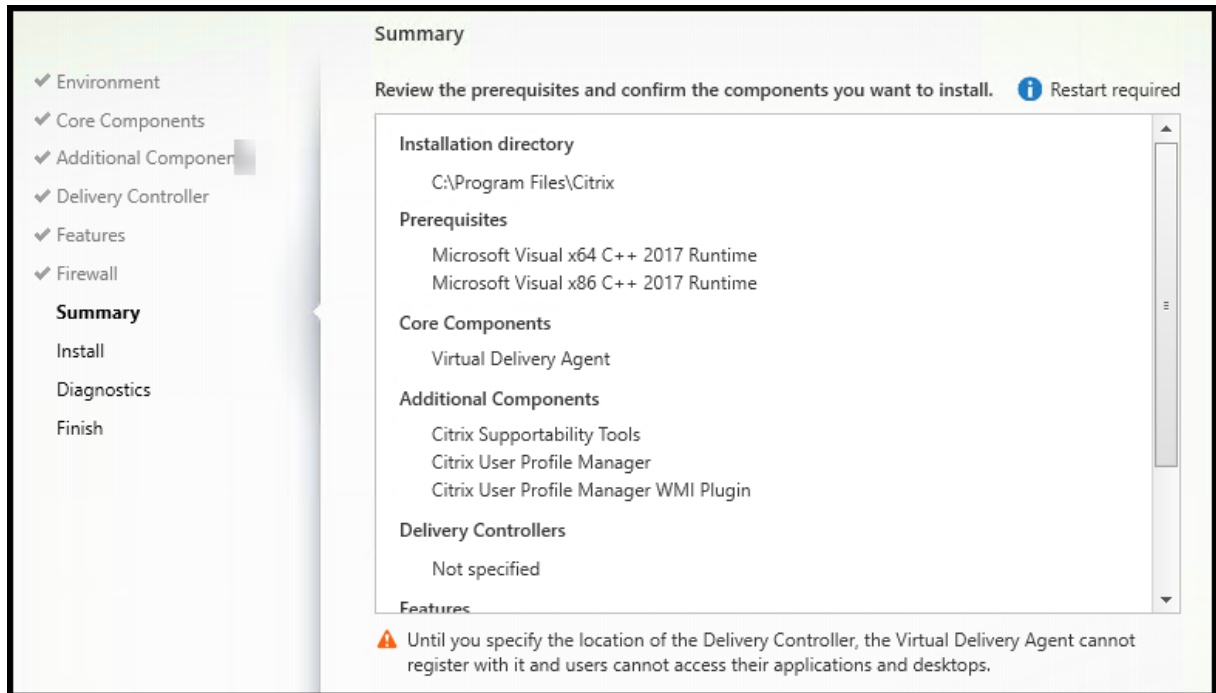


Na página **Firewall**, por padrão, as portas são abertas automaticamente se o Serviço do Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Essa configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte [Network ports](#).

Clique em **Avançar**.

Opção de linha de comando: `/enable_hdx_ports`

## Etapa 11. Verifique os pré-requisitos e confirme a instalação

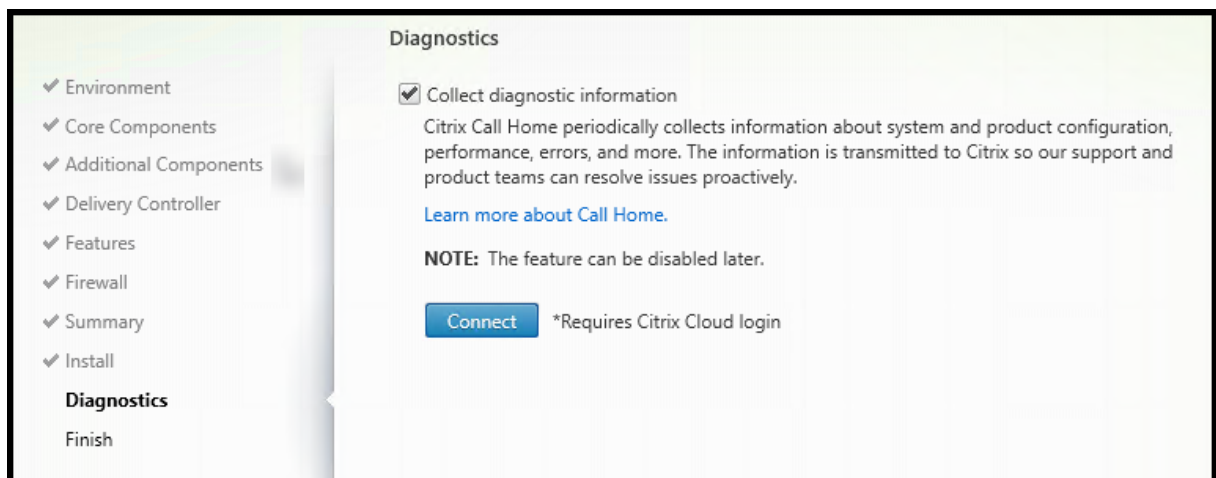


A página **Summary** lista o que será instalado. Use o botão **Back** para retornar às páginas anteriores do assistente e alterar as seleções.

Quando estiver pronto, clique em **Install**.

Se os pré-requisitos ainda não estiverem instalados ou ativados, a máquina poderá reinicializar uma ou mais vezes. Consulte [Prepare-se para instalar](#).

## Etapa 12. Diagnóstico



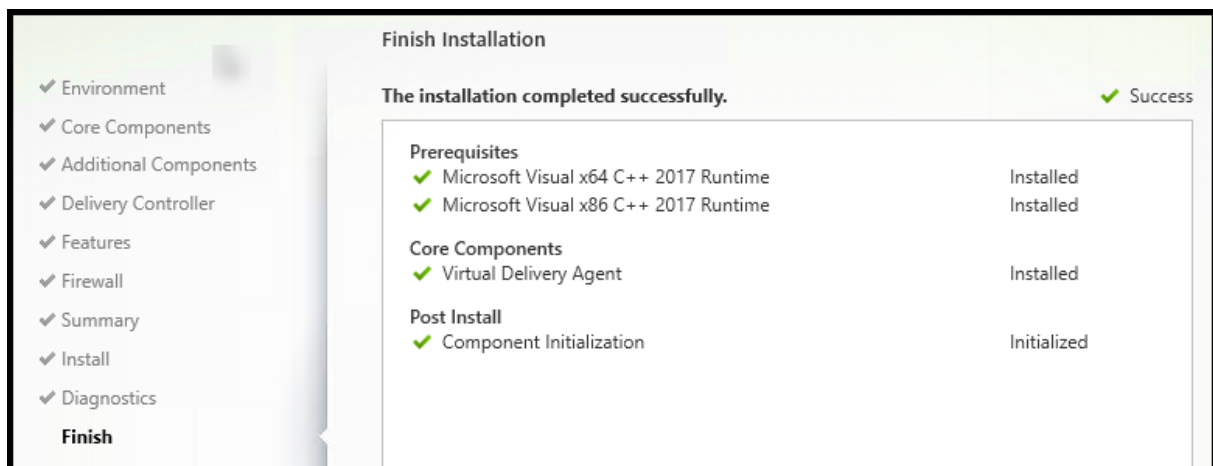
Na página **Diagnostics**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), clique em **Connect**. Quando solicitado, insira as credenciais da sua conta da Citrix.

Depois que suas credenciais forem validadas (ou se você optar por não participar), clique em **Next**.

Ao usar o instalador do produto completo, se você clicar em **Connect** na página **Diagnostics** sem primeiro selecionar **Collect diagnostic information**, depois de fechar a caixa de diálogo **Connect to Citrix Insight Services**, o botão **Next** fica desativado. Você não consegue se mover para a próxima página. Para reativar o botão **Next**, marque e desmarque imediatamente **Collect diagnostic information**.

Para obter mais informações, consulte [Call Home](#).

### Etapa 13. Conclua a instalação



A página **Finish** mostra marcas de seleção verdes para todos os pré-requisitos e componentes que foram instalados e inicializados com êxito.

Clique em **Finish**. Por padrão, a máquina é reiniciada automaticamente. Embora você possa desativar a reinicialização automática, o VDA não pode ser usado até que a máquina seja reiniciada.

### 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 disso, o Studio o guiará para criar um catálogo de máquinas e, em seguida, um grupo de entrega. Veja:

- [Crie 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.

Depois de instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Veja [CTX224676](#). O artigo CTX contém o pacote de download, além de instruções sobre como instalar e usar o Citrix Optimizer.

## Personalizar um VDA

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 **Customize Virtual Delivery Agent Settings**. Quando o instalador for iniciado, você pode alterar:
  - Endereços do Controller
  - Porta TCP/IP para registrar no Controller (padrão = 80)
  - Se as portas do Firewall do Windows devem ser abertas automaticamente

## Solucionar problemas

- Para obter informações sobre como a Citrix relata os resultados das instalações de componentes, consulte [Códigos de retorno de instalação da Citrix](#).
- Na tela do Studio de um grupo de entrega, a entrada **Installed VDA version** no painel **Details** pode não refletir 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](#).



## Limitação conhecida

Quando você usa o aplicativo Citrix Workspace para Windows versão 1912 ou anterior, a sessão é interrompida após algum tempo. Esse problema foi corrigido nas versões mais recentes LTSR e CR do aplicativo Citrix Workspace. Para obter mais informações sobre as versões de lançamento suportadas, consulte [Aplicativo Citrix Workspace para Windows/Citrix Receiver for Windows Long Term Service Releases](#).

## Instale VDAs usando o SCCM

January 24, 2025

### Visão geral

O Microsoft Endpoint Configuration Manager, antigo System Center Configuration Manager (SCCM), é um produto Windows que permite o gerenciamento, a implantação e a segurança de dispositivos e aplicativos em uma empresa.

#### Nota:

O artigo a seguir descreve apenas recomendações com base em como a Citrix testou o ambiente. Você pode personalizar essas etapas de acordo com suas necessidades. A Citrix não é responsável por nenhuma atualização ou ajuste necessário para atender às necessidades do cliente.

### Recomendações

- Para implantar com sucesso um Virtual Delivery Agent (VDA) usando SCCM ou ferramentas similares de distribuição de software, a Citrix recomenda usar o instalador [VDA em uma sequência de etapas](#).
- A Citrix não recomenda usar o VDA Cleanup Utility como parte de uma instalação ou atualização do VDA. Use o VDA Cleanup Utility somente no caso limitado em que o instalador do VDA falhou anteriormente.

### Antes de começar

O número necessário de reinicializações 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 anteriormente bloqueados por outros processos podem precisar de atualizações, forçando uma reinicialização extra.
- Alguns componentes opcionais no instalador do VDA (como o Citrix Profile Management e o Citrix Files) podem exigir uma reinicialização.
- Quando você atualiza um VDA, a máquina na qual ele está instalado deve estar no modo de manutenção, sem sessões.
- Quando uma instalação de VDA é executada pela primeira vez em uma máquina, o instalador de VDA que está sendo usado é copiado nessa máquina. Para obter mais informações sobre a instalação do VDA, consulte [Installers](#).

O **SCCM Task Sequencer** gerencia todas as reinicializações necessárias.

## Etapas principais para implantar o VDA usando o SCCM

As etapas a seguir descrevem como implantar o VDA usando o SCCM na máquina virtual.

1. [Instale o VDA](#).
2. [Crie uma unidade organizacional \(OU\)](#).
3. Verifique as máquinas.
4. Use o VDA para distribuir conteúdo.

### Etapa 1: instalar o VDA

Depois de identificar todos os pré-requisitos, use **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 instaladores de VDA, consulte [Installers](#).

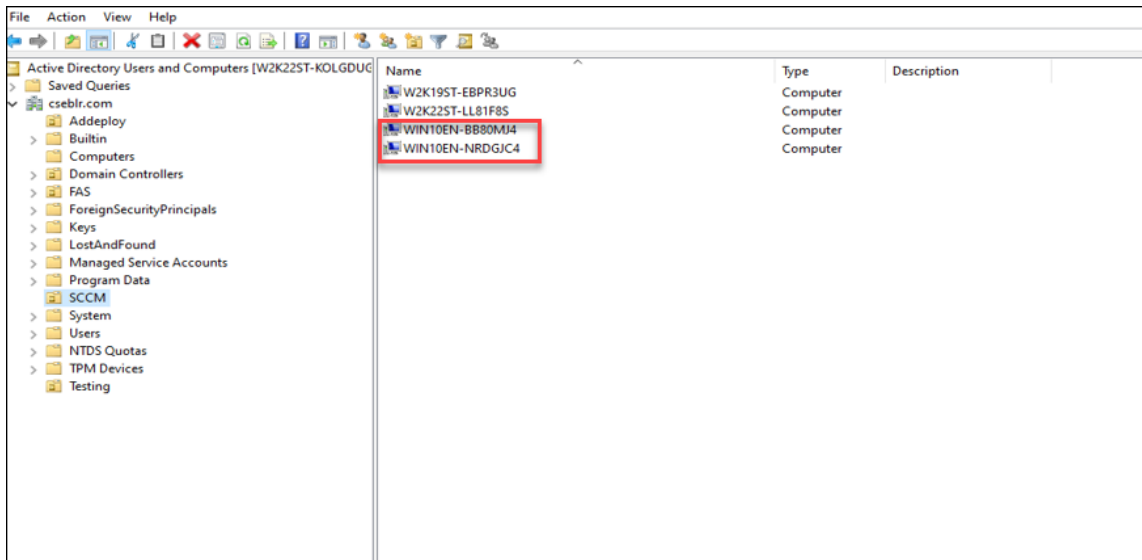
#### Nota:

Quando você atualiza um VDA, a máquina na qual ele está instalado deve estar no modo de manutenção, sem sessões.

2. Quando uma instalação de VDA é executada pela primeira vez em uma máquina, o instalador de VDA que está sendo usado é copiado nessa máquina.
  - Quando você usa um instalador de VDA diferente de `VDAWorkstationCoreSetup_XXXX.exe`, o instalador de 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. A localização do diretório do instalador do VDA também é armazenada 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`: Suprime a reinicialização automática do instalador do VDA. O SCCM aciona reinicializações quando necessário.
  - `/NORESUME`: Normalmente, quando é necessário reiniciar durante a instalação, o instalador do VDA define uma chave de registro `runonce` (`\ 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 pode monitorar a instalação e capturar o código de saída.


## **Etapa 2: criar uma unidade organizacional (OU)**

1. Crie duas máquinas virtuais unidas ao domínio que você deseja adicionar à OU. Quando as máquinas virtuais são criadas inicialmente, elas estão na pasta **Computers** . 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 marque a caixa de seleção **Habilitar Active Directory System Discovery** para ativar a descoberta automática das máquinas virtuais recém-criadas.



4. Clique no ícone  para selecionar novos contêineres.
5. Na seção **Location**, adicione o caminho \*\* em que suas máquinas virtuais do SCCM estão localizadas.
6. Vá para `\ Administration\ Overview\ Site Configuration\ Sites` e clique com o botão direito do mouse no SCCM VDA.
7. Selecione **Configurações de instalação do cliente > Instalação push do cliente**. A janela **Client Push Installation Properties** é aberta.
8. Depois que as VMs estiverem definidas como **Enabled**, você poderá ver a lista de VMs conforme ilustrado nas imagens a seguir.

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	x86 Unknown Computer...	No			CSE	
	x64 Unknown Computer...	No			CSE	
	WIN10EN-NRDGJ4	Yes			CSE	Active
	WIN10EN-8880M4	No			CSE	
	W2K22ST-LLS1F85	Yes			CSE	Active
	W2K19ST-EBPR3UG	No			CSE	
	W2K19ST-6CBDO9Q	Yes			CSE	Active
	TSVDA-SCCM19	Yes			CSE	Active
	SCCM-VDA	Yes			CSE	Active
	Provisioning Device(Pro...	No			CSE	
	2019-SCCM	No			CSE	

**Create Package and Program Wizard**

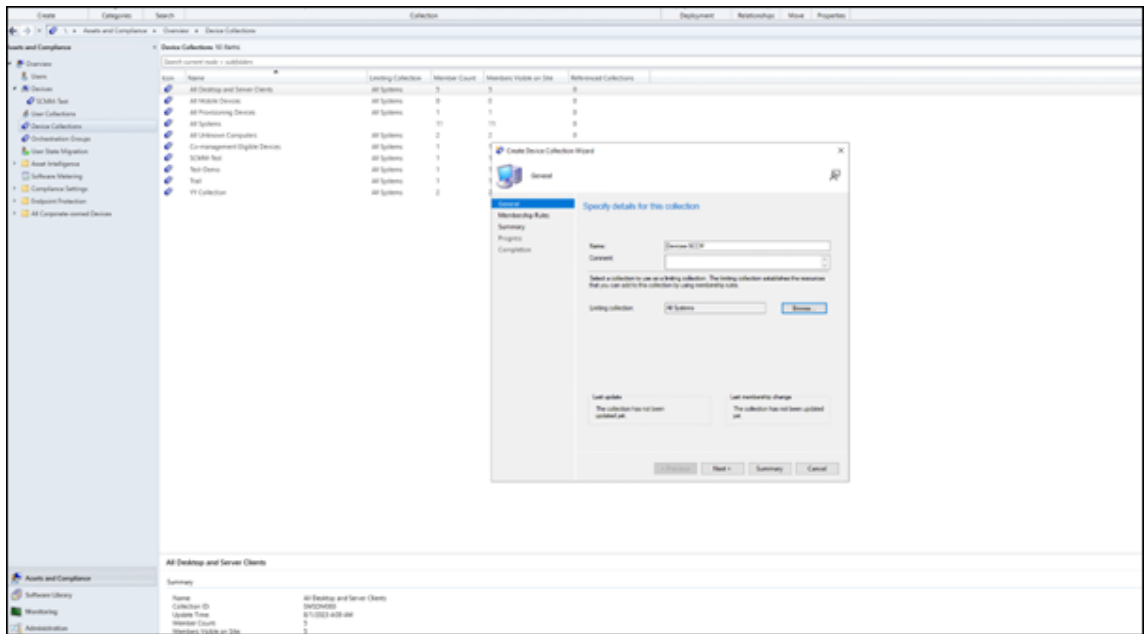
**Program Type**

Choose the program type that you want to create

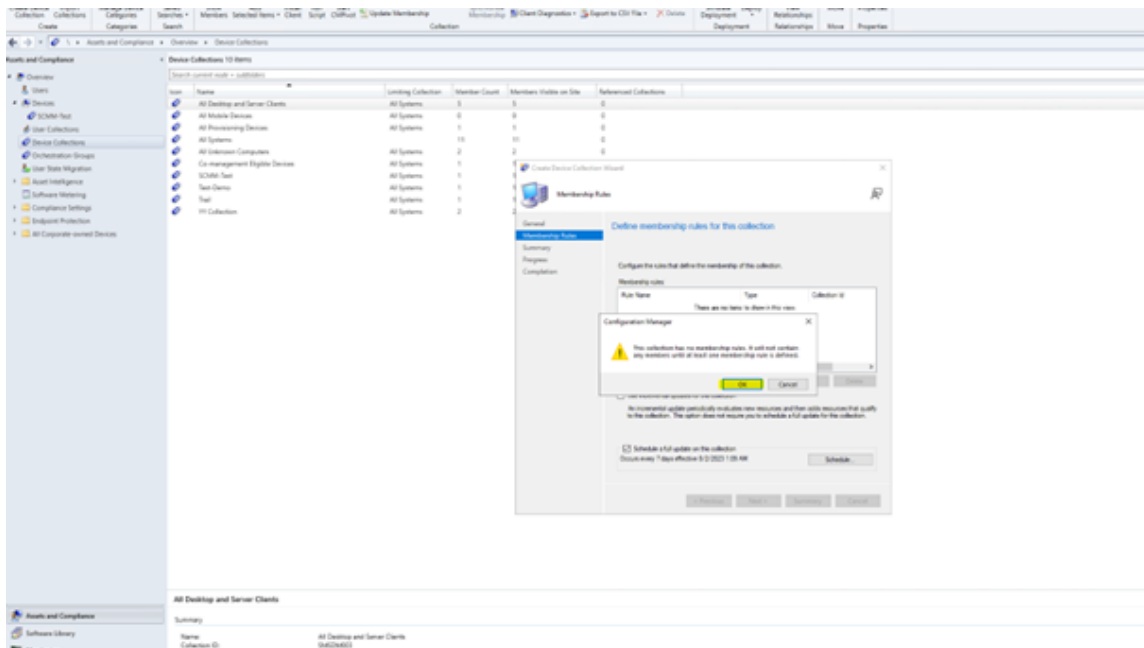
- Standard program  
Create a program for a client computer.
- Program for device  
Create a program for a device.
- Do not create a program  
Create a package, but do not create a program. You can use the Create Program Wizard to add a program later.

< Previous   **Next >**   Summary   Cancel

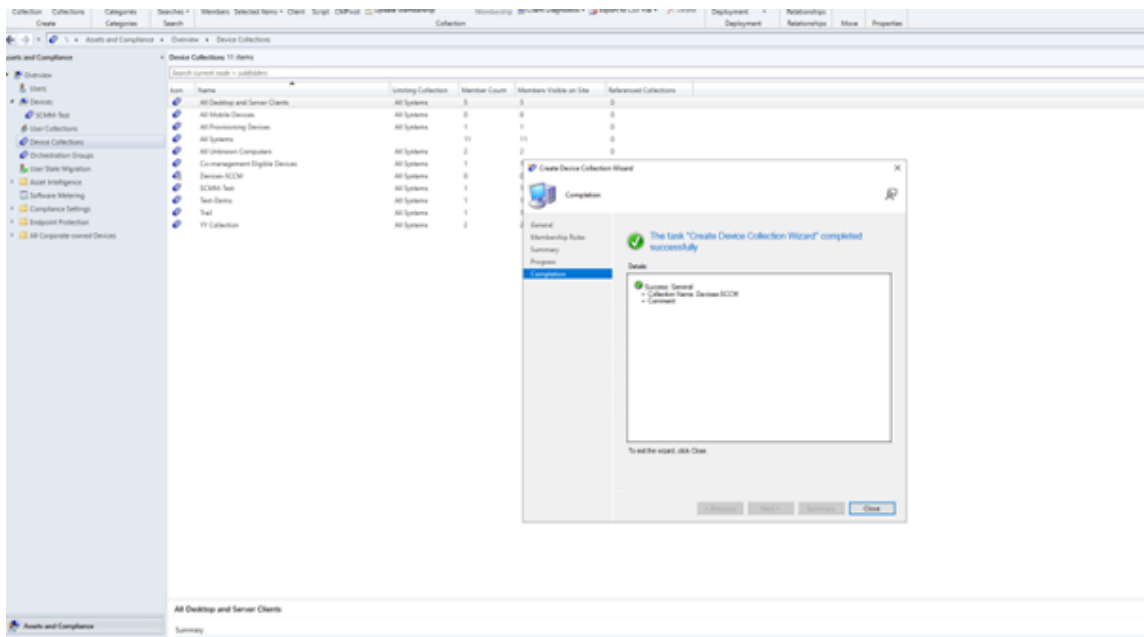
9. Crie a coleção de dispositivos **\*\* para criar a OU. Digite o nome\*\*** do nome da coleção.



10. Siga as instruções do assistente.

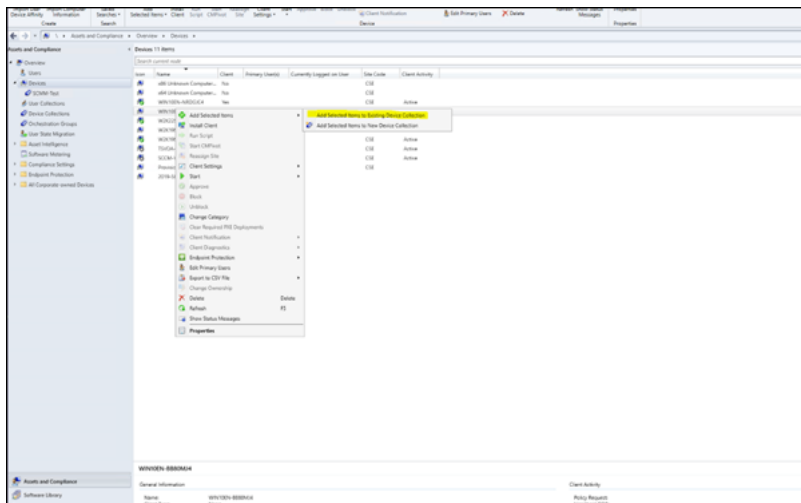


A OU é criada.

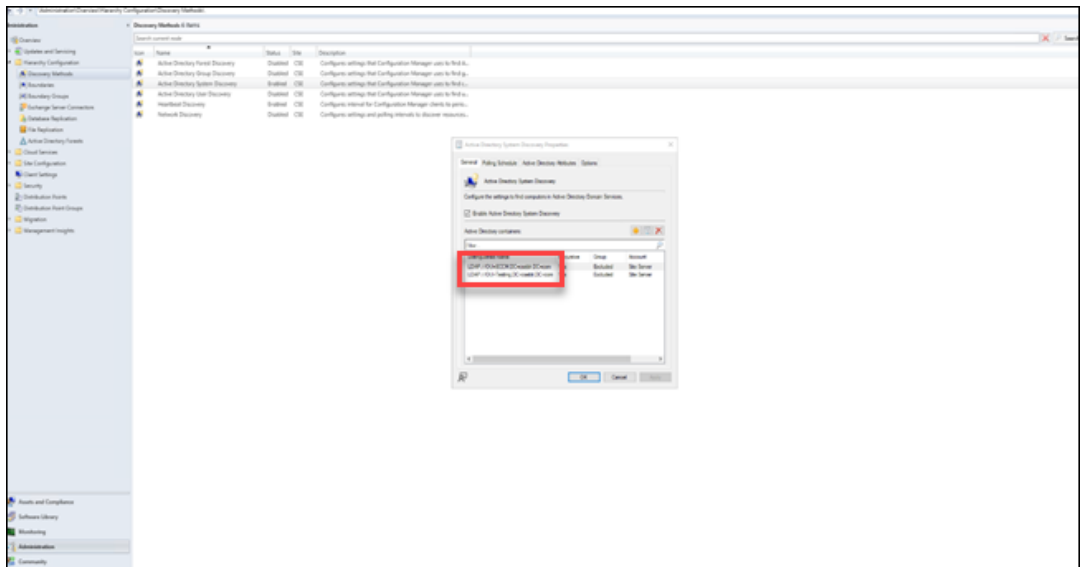


11. Adicione as VMs criadas à coleção de dispositivos recém-criada.

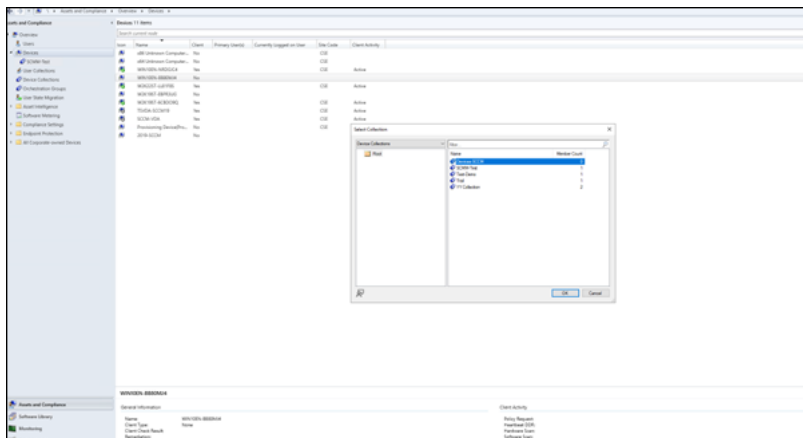
- a) Clique com o botão direito na VM. Selecione **Adicionar itens selecionados > Adicionar itens selecionados à coleção de dispositivos existentes**.



- b) Na janela **Select Collection**, selecione o nome do dispositivo necessário. Neste exemplo, é **Devices-SCCM**.

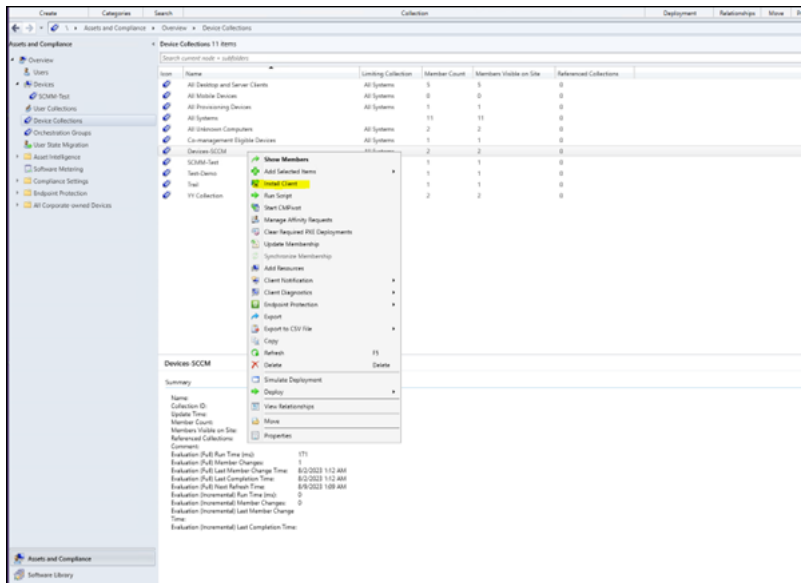


Devices-SCCM está listado em **Assets and Compliance > Visão geral > Device Collections**.

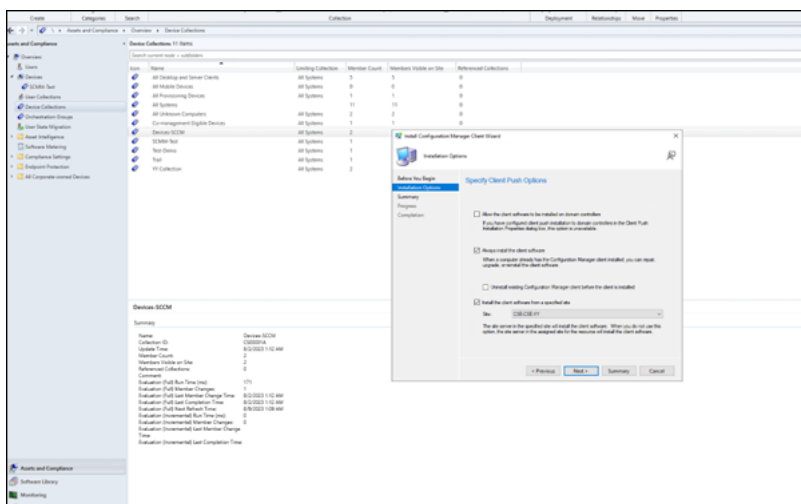


12. Selecione **Instalar o cliente** no coletor de dispositivos.

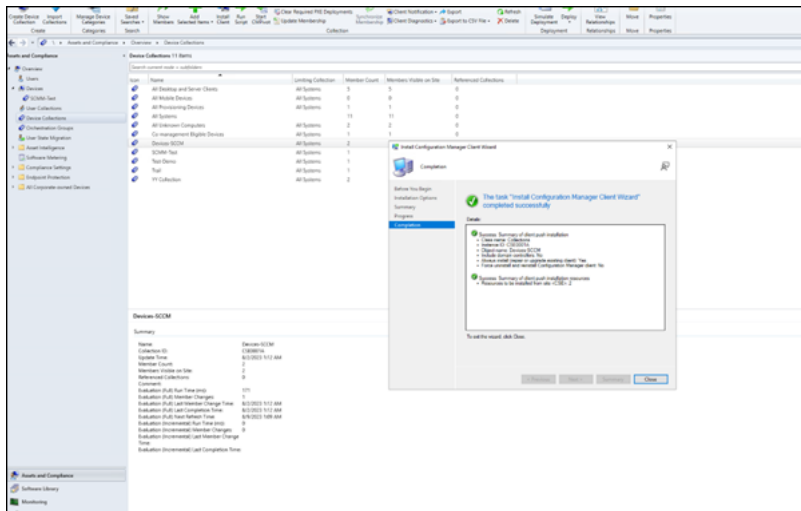




13. Selecione a instalação necessária **Site**.



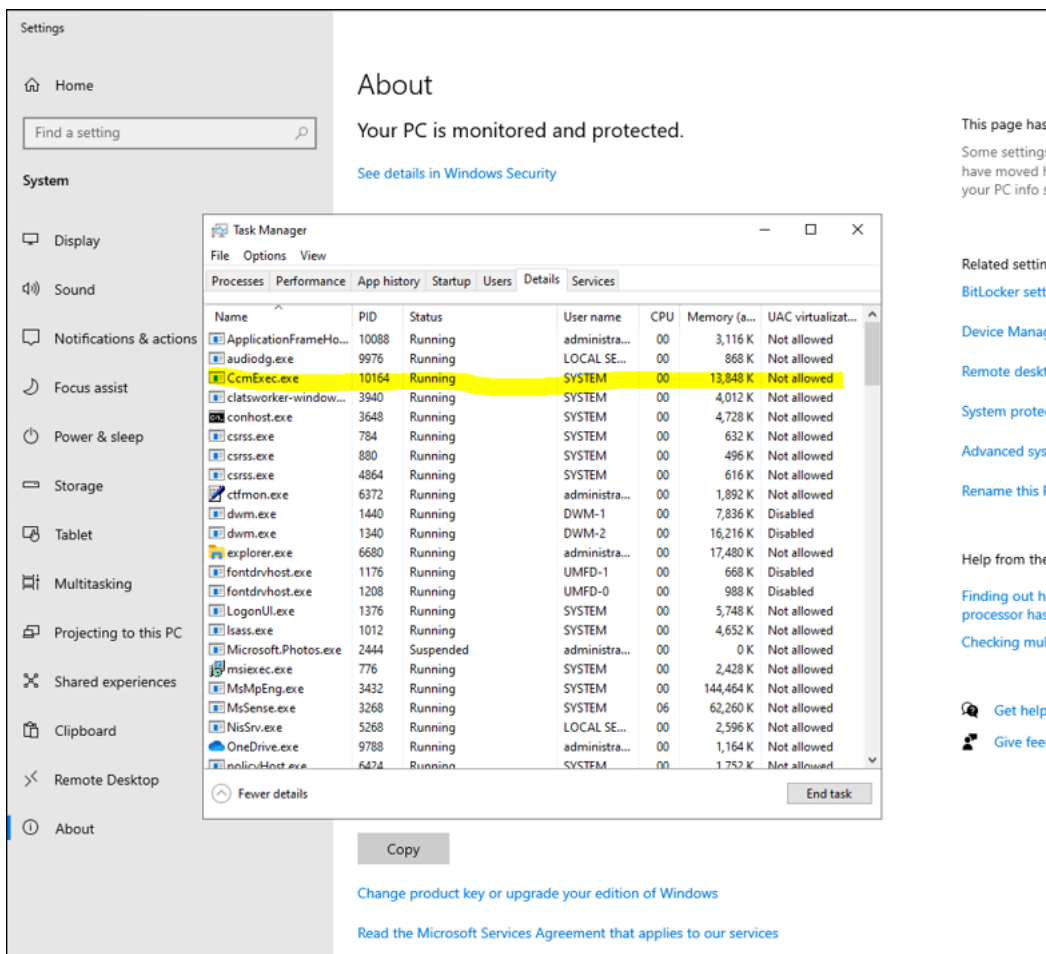
14. Siga as instruções do assistente. **O Assistente de Instalação do Cliente do Configuration Manager** foi concluído com êxito.



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.

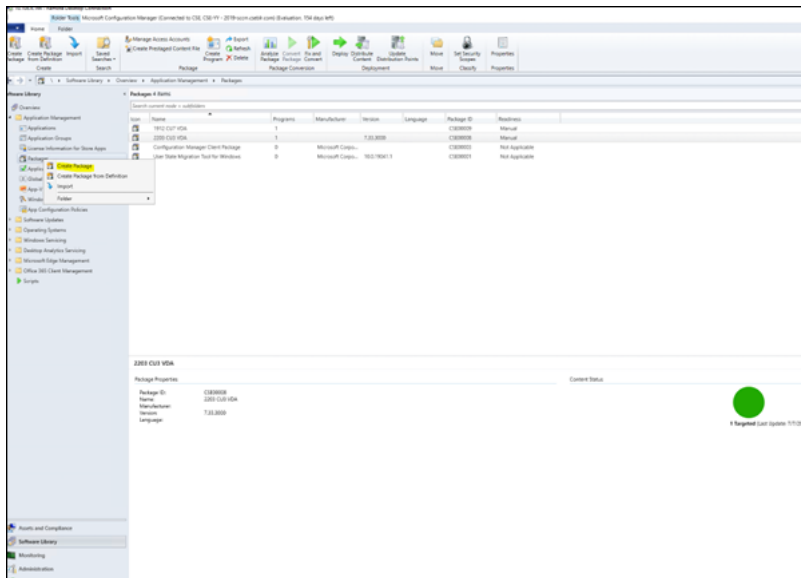
#### Etapa 4: use o VDA para distribuir conteúdo

As etapas a seguir descrevem como você pode usar o VDA implantado para distribuir conteúdo nas máquinas virtuais associadas.

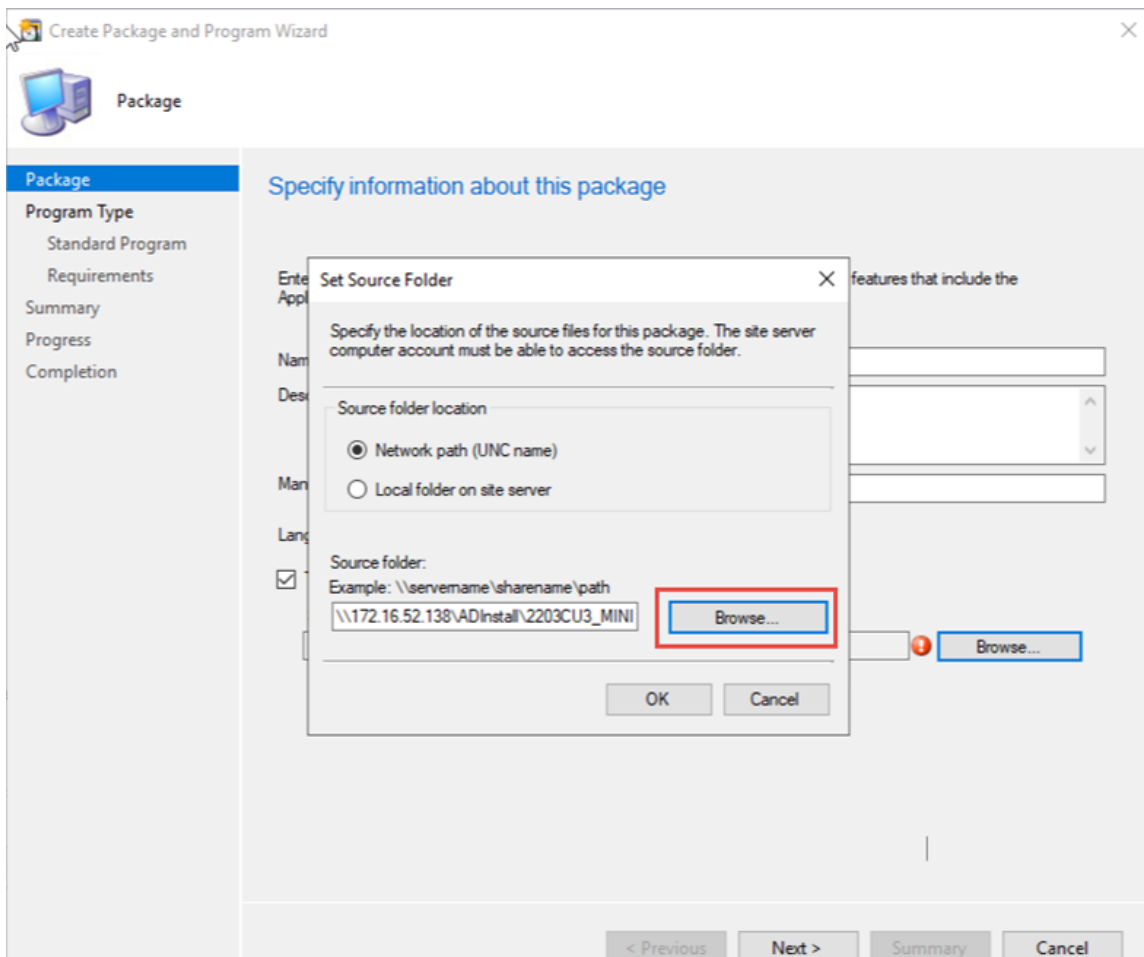
1. Crie um pacote
2. Distribuir conteúdo

#### Crie um pacote

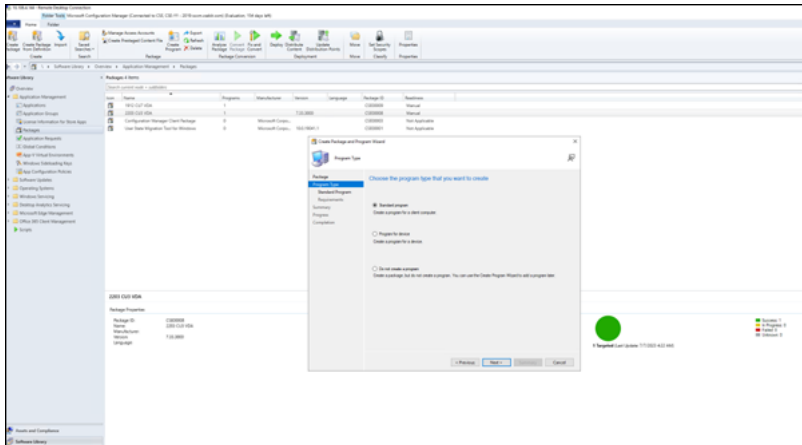
1. Para criar um pacote, clique com o botão direito do mouse no VDA desejado e clique em **Criar pacote**.



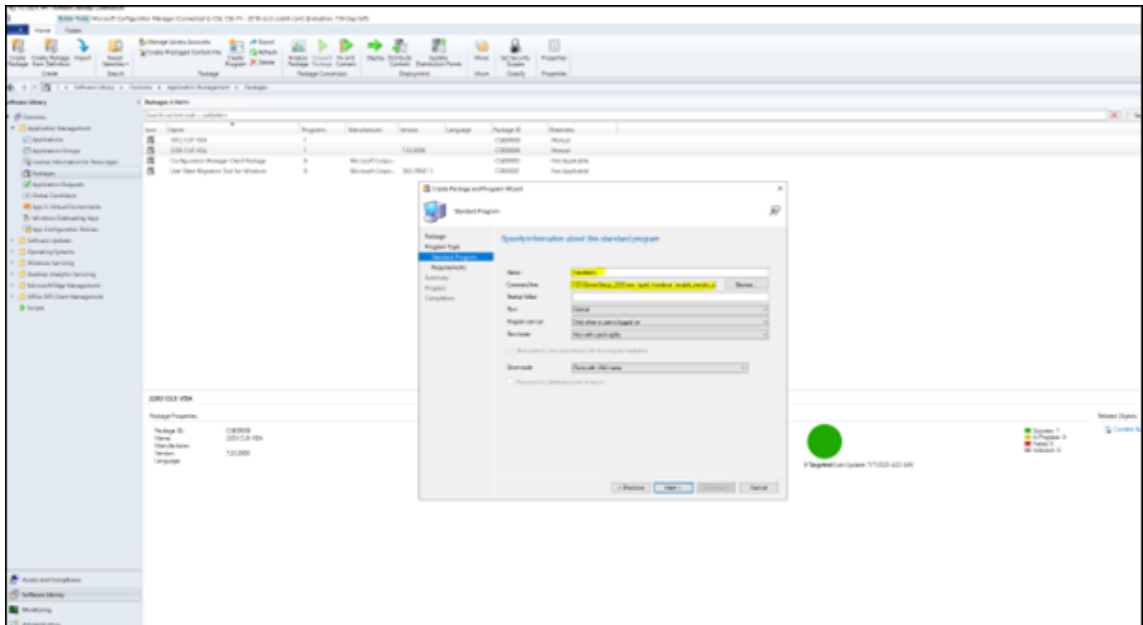
2. Especifique a localização dos arquivos de origem desse pacote clicando em **Procurar**.



3. Selecione o tipo de pacote que você deseja.

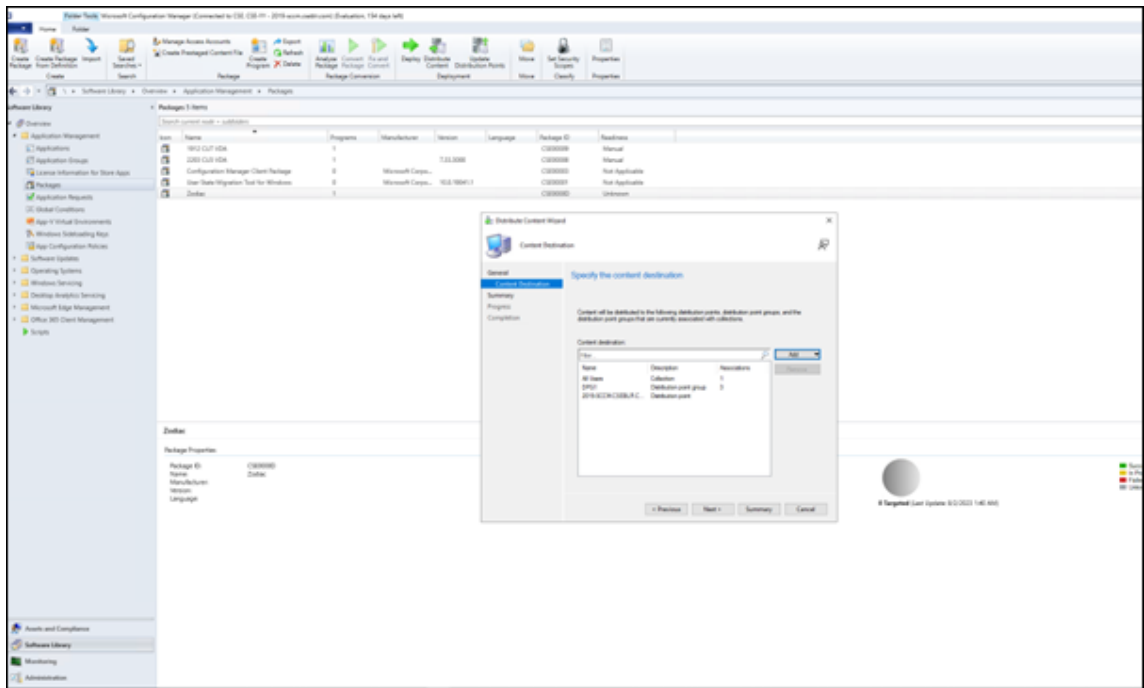


4. Digite o pacote **Name** e **Command line**.

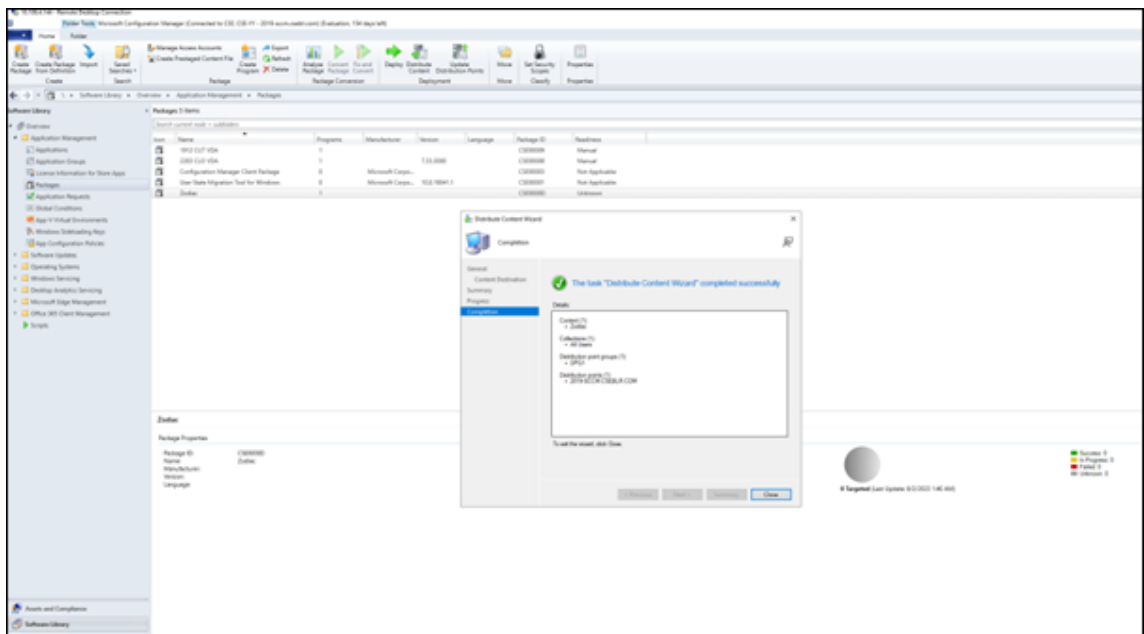


5. Clique em **Próximo**.

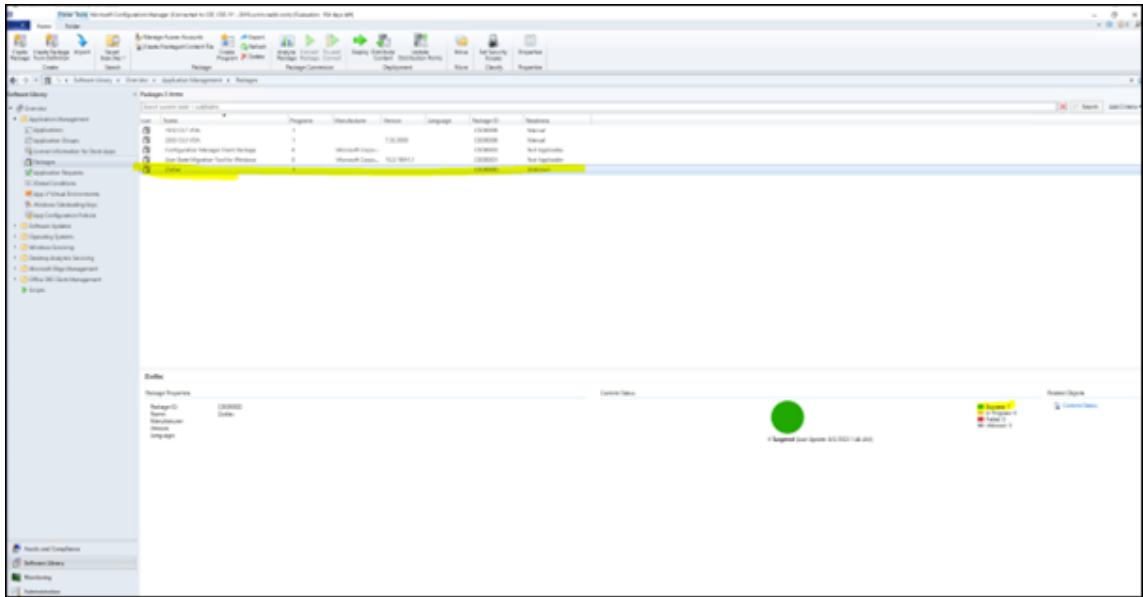




4. Verifique se o pacote (neste exemplo, *Zodiac*) está disponível para implantação.



A imagem a seguir ilustra que o pacote está disponível para implantação.

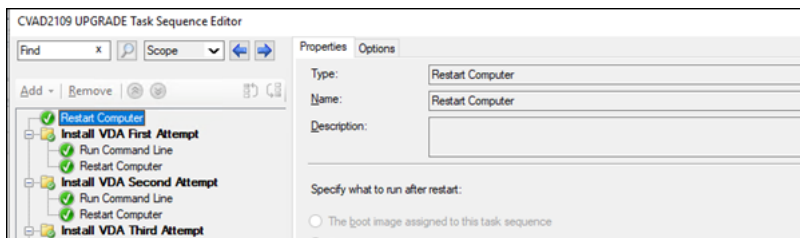


Para obter informações detalhadas, consulte [Implantar e gerenciar conteúdo para o Configuration Manager](#) na documentação da Microsoft.

## Exemplo de sequência de instalação usando SCCM

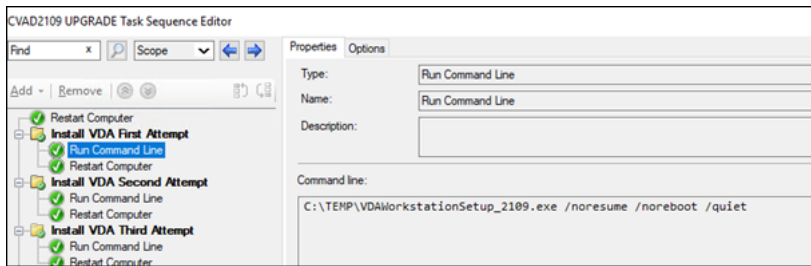
O exemplo a seguir mostra a sequência de instalação.

1. **Reinicie o computador:** Prepare a máquina reiniciando-a.



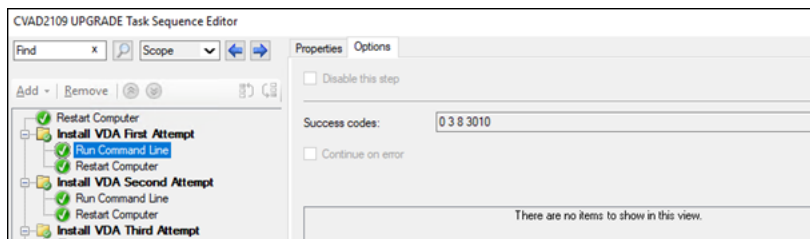
2. **Instale o VDA na primeira tentativa:** Inicie a instalação do VDA.
  - a) Adicione as opções `/quiet`, `/noreboot` /`noresume` às suas opções de linha de comando.
  - b) Execute o instalador de VDA de sua escolha (imagem local ou um dos instaladores mínimos).



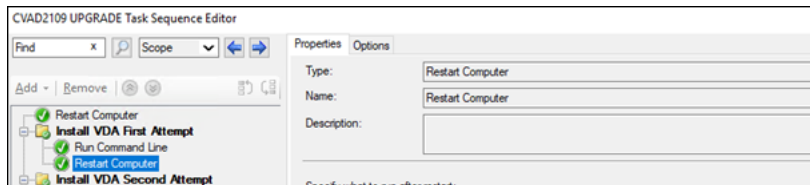


c) O SCCM deve capturar o código de devolução.

- Se o código de retorno for 0 ou 8, a instalação estará concluída e será necessário reiniciar.

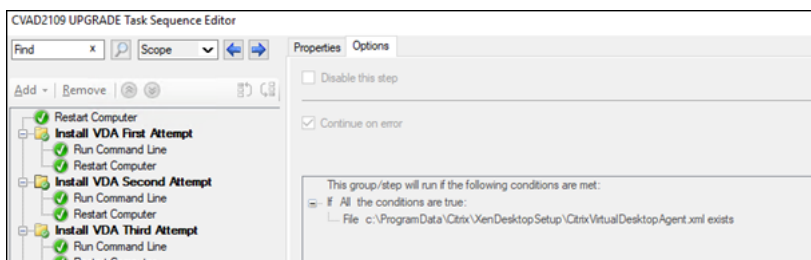


- Se o código de retorno for 3, reinicie a máquina e passe o controle para **Install VDA Second Attempt**.



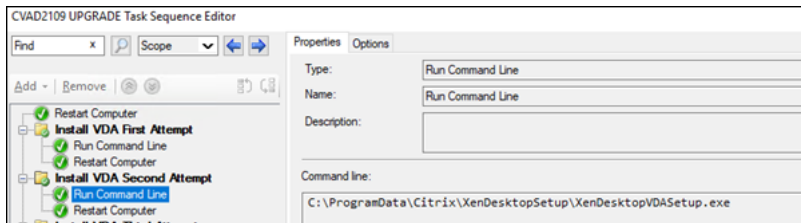
### 3. Instale o VDA Second Attempt: Continue a instalação do VDA.

- a) Depois de **Install VDA First Attempt** se o arquivo %programdata%\ Citrix\ XeNDesktopSetup\ CitrixVirtualDesktopAgent.xml existir, a instalação não será concluída e deverá ser continuada após a conclusão da reinicialização.



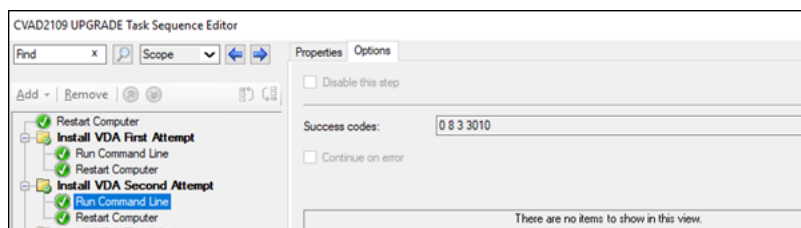
- b) **Install VDA Second Attempt** se repete até que o arquivo %programdata%\ Citrix\ XeNDesktopSetup\ CitrixVirtualDesktopAgent.xml não exista ou um código de retorno diferente de 0 ou 8 seja retornado. Trate qualquer outro código de retorno como um erro e INSTALL VDA SECOND ATTEMPT deve reportar um erro e parar.

- c) Retome a instalação do VDA executando o instalador de VDA apropriado (`XenDesktopVdaSetup.exe` na maioria dos casos, ou `XenDesktopRemotePCSetup.exe` se `VDAWorkstationCoreSetup.exe` foi usado) no diretório do arquivo `%programdata%\Citrix\XenDesktopSetup\` sem linha de comando parâmetros. (O instalador do VDA usa os parâmetros salvos durante a primeira execução do instalador.)



- d) Fique atento ao código de retorno do instalador do VDA.

- 0 ou 8: sucesso, instalação concluída, reinicialização necessária.



- 3: A instalação não está completa. Reinicie a máquina e repita `INSTALL VDA SECOND ATTEMPT` 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 `INSTALL VDA SECOND ATTEMPT` deve reportar um erro e terminar.

Para obter mais informações sobre códigos de devolução, consulte [Códigos de devolução de instalação da Citrix](#).

## Exemplos de comandos de instalação do VDA

As opções de instalação disponíveis variam, dependendo do instalador usado. Consulte os artigos a seguir para obter detalhes das opções de linha de comando.

- [Instale VDAs](#)
- [Instale usando a linha de comando](#)

## Comandos de instalação para acesso remoto ao 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 dedicada

- 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
```

## Conexão com a AWS

November 5, 2024

[Criar e gerenciar conexões e recursos](#) descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem da AWS.

#### Observação:

Antes de criar uma conexão com a AWS, você precisa primeiro concluir a configuração da sua conta da AWS como um local de recursos. Veja [Ambientes de nuvem da AWS](#).

### Criar uma conexão

Quando você cria 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 chaves que contém esses valores da AWS e depois importá-los. Você também deve fornecer a região, a zona de disponibilidade, o nome da VPC, os endereços de sub-rede, o nome do domínio, o nome dos grupos de segurança e as credenciais.
- O arquivo de credenciais para a conta raiz da AWS (recuperado do console da AWS) não está formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão da

AWS. Portanto, o gerenciamento do Citrix Virtual Apps and Desktops não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Verifique se você está usando os arquivos de credenciais do AWS Identity Access Management (IAM).

**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 servidor proxy ou do firewall e verifique se o seguinte endereço pode ser contatado: [https://\\*.amazonaws.com](https://*.amazonaws.com).

### Valores padrão de conexão do host

Quando você cria conexões de host em ambientes de nuvem da AWS, os seguintes valores padrão são exibidos:

---

Opção	Absoluto	Porcentagem
Ações simultâneas (todos os tipos)	125	100
Máximo de novas ações por minuto	125	

---

Por padrão, o MCS oferece suporte a 100 operações de provisionamento simultâneas.

### URL do ponto de extremidade de serviço

#### URL do ponto de extremidade do serviço de zona padrão

Quando você usa MCS, uma nova conexão da AWS é adicionada com uma chave de API e um segredo de API. Com essas informações, juntamente com a conta autenticada, o MCS consulta a AWS sobre as zonas suportadas usando a chamada de API do EC2 da AWS: DescribeRegions. A consulta é feita usando uma URL genérica do EC2 Service Endpoint <https://ec2.amazonaws.com/>. Use o MCS para selecionar a zona para a conexão na lista de zonas suportadas. A URL do ponto de extremidade de serviço preferencial da AWS é selecionada automaticamente para a zona. No entanto, depois de criar a URL do ponto de extremidade de serviço, você não pode mais definir ou modificar a URL.

### Definir permissões do IAM

Use as informações nesta seção para definir as permissões do IAM para o Citrix Virtual Apps and Desktops na AWS. O serviço IAM da Amazon permite contas com vários usuários, que podem ser organizados em grupos. Os usuários podem ter permissões diferentes para controlar sua capacidade de

realizar operações associadas à conta. Para obter mais informações sobre permissões do IAM, consulte [Referência de política JSON do IAM](#).

Para aplicar a política de permissões do IAM a um novo grupo de usuários:

1. Faça login no console de gerenciamento da AWS e selecione o serviço **IAM** na lista suspensa.
2. Selecione **Create a New Group of Users**.
3. Digite um nome para o novo grupo de usuários e selecione **Continue**.
4. Na página **Permissions**, selecione **Custom Policy**. Selecione **Select**.
5. Digite um nome para a **Permissions policy**.
6. Na seção **Policy Document**, insira as permissões relevantes.

Depois de inserir as informações da política, selecione **Continue** para concluir o grupo de usuários. Os usuários do grupo recebem permissões para executar somente as ações necessárias para o Citrix Virtual Apps and Desktops.

**Importante:**

Use o texto de política fornecido no exemplo anterior para listar as ações que o Citrix Virtual Apps and Desktops usa para executar ações em uma conta da AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar mais restrições aos recursos.

## Definir permissões do IAM

Defina as permissões na seção **IAM** do AWS Management Console:

1. No painel **Summary**, selecione a guia **Permissions**.
2. Selecione **Add permissions**.

**Identity and Access Management (IAM)**

Dashboard

Access management

Groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID:

Users >

## Summary

User ARN: am:aws:iam::

Path: /

Creation time: 2019-07-17 09:59 EST

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (2 policies applied)

Add permissions

Policy name

Attached from group

- Billing
- AdministratorAccess

Permissions boundary (not set)

Na tela **Add Permissions to**, conceda permissões:

Add permissions to

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies

Policy name	Type	Used as
AdministratorAccess	Job function	Permissions policy (8)
AlexaForBusinessDeviceSetup	AWS managed	None
AlexaForBusinessFullAccess	AWS managed	None
AlexaForBusinessGatewayExecution	AWS managed	None
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
AlexaForBusinessReadOnlyAccess	AWS managed	None
AmazonAPIGatewayAdministrator	AWS managed	None
AmazonAPIGatewayInvokeFullAccess	AWS managed	None

Use o seguinte como exemplo na guia **JSON**:

## Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

Import managed policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:CreateTags",
9         "ec2:DeleteTags",
10        "ec2:DescribeTags",
11        "ec2:PutObjectTagging",
12        "ec2:PutBucketTagging"
13      ],
14      "Resource": "*"
15    },
16    {
17      "Sid": "VisualEditor1",
18      "Effect": "Allow",
19      "Action": "iam:PassRole",
20      "Resource": "arn:aws:iam:*:role/*"
21    }
22  ]
23 }

```

Character count: 304 of 6,144.

Cancel

Review policy

**Dica:**

O exemplo de JSON observado talvez não inclua todas as permissões para o seu ambiente. Consulte [How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS](#) para obter mais informações.

**Permissões necessárias da AWS**

Esta seção contém a lista completa de permissões da AWS.

**Observação:**

A permissão `iam:PassRole` é necessária somente para `role_based_auth`.

**Criar uma conexão de host**

Uma nova conexão de host é adicionada usando as informações da AWS.

```

1 {
2
3   "Versão": "2012-10-17",
4   "Declaração": [
5     {

```

```
6
7     "Ação": [
8         "ec2:DescribeAvailabilityZones",
9         "ec2:DescribeImages",
10        "ec2:DescribeInstances",
11        "ec2:DescribeInstanceTypes",
12        "ec2:DescribeSecurityGroups",
13        "ec2:DescribeSubnets",
14        "ec2:DescribeVpcs",
15        "ec2:DescribeRegions",
16        "ec2:DescribeSnapshots",
17        "ec2:DescribeLaunchTemplates"
18    ],
19    "Efeito": "Permitir",
20    "Recurso": "*"
21 }
22
23 ]
24 }
```

### Gerenciamento de energia de VMs

As instâncias de máquina estão ligadas ou desligadas.

```
1 {
2
3     "Versão": "2012-10-17",
4     "Declaração": [
5         {
6
7             "Ação": [
8                 "ec2:AttachVolume",
9                 "ec2:CreateVolume",
10                "ec2>DeleteVolume",
11                "ec2:DescribeInstances",
12                "ec2:DescribeVolumes",
13                "ec2:DetachVolume",
14                "ec2:StartInstances",
15                "ec2:StopInstances"
16            ],
17            "Efeito": "Permitir",
18            "Recurso": "*"
19        }
20    ]
21 }
22 }
```



## Criar, atualizar ou excluir VMs

Um catálogo de máquinas é criado, atualizado ou excluído com VMs provisionadas como instâncias da AWS.

```
1 {
2
3   "Versão" : "2012-10-17",
4   "Declaração" : [
5     {
6
7       "Ação" : [
8         "ec2:AttachVolume" ,
9         "ec2:AssociateIAMInstanceProfile" ,
10        "ec2:AuthorizeSecurityGroupEgress" ,
11        "ec2:AuthorizeSecurityGroupIngress" ,
12        "ec2:CreateImage" ,
13        "ec2:CreateLaunchTemplate" ,
14        "ec2:CreateSecurityGroup" ,
15        "ec2:CreateTags" ,
16        "ec2:CreateVolume" ,
17        "ec2>DeleteVolume" ,
18        "ec2:Describe Account Attributes" ,
19        "ec2:Describe Availability Zones" ,
20        "ec2:Describe IAM InstanceProfile Associations" ,
21        "ec 2:DescribeImages" ,
22        "ec2:DescribeInstances" ,
23        "ec2:DescribeInstanceTypes" ,
24        "ec2:DescribeLaunchTemplates" ,
25        "ec2:DescribeLaunchTemplateVersions" ,
26        "ec2:DescribeNetwork Interfaces" ,
27        "ec2:DescribeRegions" ,
28        "ec2:DescribeSecurityGroups" ,
29        "ec2:DescribeSnapshots" ,
30        "ec2:DescribeSubnets" ,
31        "ec2:DescribeTags" ,
32        "ec2:DescribeVolumes" ,
33        "ec2:DescribeVPCs" ,
34        "ec2:DetachVolume" ,
35        "ec2:DisassociateIAM InstanceProfile" ,
36        "ec2:RunInstances" ,
37        "ec2:StartInstances" ,
38        "ec2:StopInstances" ,
39        "EC2:Encerrar Instâncias"
40      ],
41      "Effect" : "Permitir" ,
42      "Recurso" : "*"
43    }
44  ,
45    {
46
47      "Ação" : [
48        "ec2:AuthorizeSecurityGroupEgress" ,
```

```

49         " ec2:AuthorizeSecurityGroupIngress " ,
50         " ec2:CreateSecurityGroup " ,
51         " ec2>DeleteSecurityGroup " ,
52         " ec2:RevokeSecurityGroupEgress " ,
53         " ec2:revokeSecurityGroupIngress "
54     ],
55     " Effect " : " Permitir " ,
56     " Recurso " : " * "
57 }
58 ,
59 {
60
61     " Ação " : [
62         " s3:CreateBucket " ,
63         " s3>DeleteBucket " ,
64         " S3:PutBucketACL " ,
65         " S3:PutBucketTagging " ,
66         " S3:PutObject " ,
67         " S3:getObject " ,
68         " S3>DeleteObject " ,
69         " s3:PutObjectTagging "
70     ],
71     " Effect " : " Allow " ,
72     " Resource " : " Arn:aws:s3: ::citrix* "
73 }
74 ,
75 {
76
77     " Ação " : [
78         " ebs:startSnapshot " ,
79         " ebs:getSnapshotBlock " ,
80         " ebs:putSnapshotBlock " ,
81         " ebs:completeSnapshot " ,
82         " ebs:listSnapshotBlocks " ,
83         " ebs:listChangedBlocks " ,
84         " ec2:createSnapshot "
85     ],
86     " Efeito " : " Permitir " ,
87     " Recurso " : " * "
88 }
89
90 ]
91 }

```

**Observação:**

A seção do EC2 relacionada aos grupos de segurança só é necessária se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Feito isso, essas permissões não serão necessárias.

**Upload e download direto do disco** O upload direto do disco elimina o requisito do volume worker para o provisionamento do catálogo de máquinas e, em vez disso, usa APIs públicas fornecidas pela AWS. Essa funcionalidade reduz o custo associado a contas extras de armazenamento e a complexidade para manter as operações do volume worker.

**Observação:**

O suporte para o volume worker foi preterido.

As seguintes permissões devem ser adicionadas à política:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:ExcluirInstantâneo`
- `ec2:DescribeLaunchTemplates`

**Importante:**

- Você pode adicionar uma VM aos catálogos de máquinas existentes sem nenhuma operação do volume worker, como volume worker AMI e volume worker VM.
- Se você excluir um catálogo existente que usava o volume worker antes, todos os artefatos, incluindo os relacionados ao volume worker, serão excluídos.

### Criptografia do EBS dos volumes criados

O EBS pode criptografar automaticamente volumes recém-criados se a AMI estiver criptografada ou se o EBS estiver configurado para criptografar todos os novos volumes. No entanto, para implementar a funcionalidade, as seguintes permissões devem ser incluídas na política do IAM.

```
1 {
2
3     "Versão": "2012-10-17",
4     "Declaração": [
5         {
6
7             "Efeito": "Permitir",
8             "Ação": [
9                 "kms:CreateGrant",
10                "kms:Decrypt",
11                "kms:DescribeKey",
```

```

12         "kms:GenerateDataKeyWithoutPlainText",
13         "kms:ReEncryptTo",
14         "kms:ReEncryptFrom"
15     ],
16     "Recurso": "*"
17 }
18
19 ]
20 }

```

**Observação:**

As permissões podem ser limitadas a chaves específicas, incluindo um bloco Resource e Condition a critério do usuário. Por exemplo, **Permissões do KMS com condição:**

```

1 {
2
3     "Versão": "2012-10-17",
4     "Declaração": [
5         {
6
7             "Efeito": "Permitir",
8             "Ação": [
9                 "kms:CreateGrant",
10                "kms:Decrypt",
11                "kms:DescribeKey",
12                "kms:GenerateDataKeyWithoutPlainText",
13                "kms:ReEncryptTo",
14                "kms:ReEncryptFrom"
15            ],
16            "Recurso": [
17                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-a123b4cd56ef"
18            ],
19            "Condição": {
20
21                "Bool": {
22
23                    "kms:GrantIsForAWSResource": true
24                }
25            }
26        }
27    ]
28 }
29
30 ]
31 }

```

A declaração de política de chaves a seguir é a política de chaves padrão completa para chaves do KMS que é necessária para permitir que a conta use políticas do IAM para delegar permissão para todas as ações (kms: \*) na chave do KMS.

```
1 {
2
3   "Sid": "Habilitar políticas do IAM",
4   "Efeito": "Permitir",
5   "Principal": {
6
7     "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10  "Ação": "kms:",
11  "Recurso": ""
12 }
```

Para obter mais informações, consulte a [documentação oficial do AWS Key Management Service](#).

### Autenticação baseada na função do IAM

As seguintes permissões são adicionadas para oferecer suporte à autenticação baseada em função.

```
1 {
2
3   "Versão": "2012-10-17",
4   "Declaração": [
5     {
6
7       "Efeito": "Permitir",
8       "Ação": "iam:PassRole",
9       "Recurso": "arn:aws:iam::*:role/*"
10    }
11  ]
12 }
13 }
```

### Política de permissões mínimas do IAM

O JSON a seguir pode ser usado para todos os recursos atualmente suportados. Você pode criar conexões de host, criar, atualizar ou excluir VMs, e fazer o gerenciamento de energia usando essa política. A política pode ser aplicada aos usuários conforme explicado nas seções Definir permissões do IAM ou você também pode usar a autenticação baseada em funções usando a chave de segurança **role\_based\_auth** e a chave secreta.

#### Importante:

Para usar **role\_based\_auth**, primeiro configure a função do IAM desejada 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 usa a autenticação baseada em função.

```
1 {
2
3     "Versão" : " 2012-10-17",
4     "Declaração" : [
5         {
6
7             "Ação" : [
8                 "ec2:AttachVolume" ,
9                 "ec2:AssociateIAMInstanceProfile" ,
10                "ec2:AuthorizeSecurityGroupEgress" ,
11                "ec2:AuthorizeSecurityGroupIngress" ,
12                "ec2:CreateImage" ,
13                "ec2:CreateLaunchTemplate" ,
14                "ec2:CreateNetwork Interface" ,
15                "ec2:CreateTags" ,
16                "ec2:CreateVolume" ,
17                "ec2>DeleteLaunchTemplate" ,
18                "ec2>DeleteNetwork Interface" ,
19                "ec2>DeleteSecurityGroup" ,
20                "ec2>DeleteSnapshot" ,
21                "EC2:Ec2>DeleteSnapshot" Excluir tags" ,
22                "ec2>DeleteVolume" ,
23                "ec2:Cancelar registro da imagem" ,
24                "ec2:Descreva os atributos da conta" ,
25                "ec2:Descreva as zonas de disponibilidade" ,
26                "ec2:Descreva associações de perfil de instância do
                IAM" ,
27                "ec2:DescribeImages" ,
28                "ec2:DescribeInstances" ,
29                "ec2:Descreva os tipos de instância" ,
30                "ec2:DescribeLaunchTemplates" ,
31                "ec2:DescribeLaunchTemplateVersions" ,
32                "ec2:DescribeNetwork Interfaces" ,
33                "ec2:DescribeRegions" ,
34                "ec2:DescribeSecurityGroups" ,
35                "ec2:DescribeSnapshots" ,
36                "ec2:DescribeSubnets" ,
37                "ec2:DescribeTags" ,
38                "ec2: DescribeVolumes" ,
39                "ec2:DescribeVPCs" ,
40                "ec2:DetachVolume" ,
41                "ec2:DisassociateIAM InstanceProfile" ,
42                "ec2:RebootInstances" ,
43                "ec2:RunInstances" ,
44                "ec2:StartInstances" ,
45                "ec2:StopInstances" ,
46                "ec2:Encerrar Instâncias"
47            ],
48            "Effect" : " Permitir" ,
49            "Recurso" : "*"
50        }
51    ]
52 }
```

```
51 ,
52   {
53
54     "Ação" : [
55       "ec2:AuthorizeSecurityGroupEgress" ,
56       "ec2:AuthorizeSecurityGroupIngress" ,
57       "ec2:CreateSecurityGroup" ,
58       "ec2>DeleteSecurityGroup" ,
59       "ec2:RevokeSecurityGroupEgress" ,
60       "ec2:RevokeSecurityGroupIngress"
61     ],
62     "Effect" : "Allow" ,
63     "Resource" : "*"
64   }
65 ,
66   {
67
68     "Action" : [
69       "S3:CreateBucket" ,
70       "s3>DeleteBucket" ,
71       "S3>DeleteObject" ,
72       "s3:getObject" ,
73       "s3:putBucketAcl" ,
74       "s3:putObject" ,
75       "s3:putBucketTagging" ,
76       "s3:putObjectTagging"
77     ],
78     "Effect" : "Allow" ,
79     "Resource" : "arn:aws:s3: ::citrix*"
80   }
81 ,
82   {
83
84     "Action" : [
85       "ebs:startSnapshot" ,
86       "ebs:getSnapshotBlock" ,
87       "ebs:putSnapshotBlock" ,
88       "ebs:completeSnapshot" ,
89       "ebs:listSnapshotBlocks" ,
90       "ebs:listChangedBlocks" ,
91       "ec2:createSnapshot"
92     ],
93     "Effect" : "Permitir" ,
94     "Recurso" : "*"
95   }
96 ,
97   {
98
99     "Efeito" : "Permitir" ,
100    "Ação" : [
101      "kms:createGrant" ,
102      "kms:decrypt" ,
103      "kms:describeKey" ,
```

```
104         " kms:generateDataKeyWithoutPlaintext " ,
105         " kms:generateDataKey " ,
106         " kms:reencryptTo " ,
107         " kms:reencryptFrom "
108     ],
109     " Resource " : " * "
110 }
111 ,
112 {
113
114     " Effect " : " Allow " ,
115     " Action " : " iam:passRole " ,
116     " Resource " : " arn:aws:iam: *:role/* "
117 }
118
119 ]
120 }
```

#### Observação:

- A seção do EC2 relacionada a SecurityGroups só será necessária se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Feito isso, essas permissões não serão necessárias.
- A seção KMS só é necessária ao usar a criptografia de volume do EBS.
- A seção de permissão iam:PassRole é necessária somente para **role\_based\_auth**.
- Permissões específicas de nível de recurso podem ser adicionadas em vez de acesso total com base em seus requisitos e ambiente. Consulte os documentos da AWS [Demystifying EC2 Resource-Level Permissions](#) e [Access management for AWS resources](#) para obter mais detalhes.

#### O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte [Criar catálogos de máquinas](#)
- Para obter informações específicas da AWS, consulte [Criar um catálogo da AWS](#)

#### Mais informações

- [Conexões e recursos](#)
- [Criar catálogos de máquinas](#)



## Conexão com o Microsoft Azure

January 24, 2025

### Nota:

Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência ao Azure Active Directory, Azure AD ou AAD agora se refere ao Microsoft Entra ID.

[Criar e gerenciar conexões e recursos](#) descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Azure Resource Manager.

### Nota:

Antes de criar uma conexão com o Microsoft Azure, você deve concluir a configuração da sua conta do Azure como um local de recurso. Veja [Ambientes de nuvem do Microsoft Azure Resource Manager](#).

## Crie diretores de serviços e conexões

Antes de criar conexões, você deve configurar os principais de serviço que as conexões usam para acessar os recursos do Azure. Você pode criar uma conexão de duas maneiras:

- Crie um principal de serviço e uma conexão juntos usando o Web Studio
- Crie uma conexão usando um principal de serviço criado anteriormente

Esta seção mostra como concluir essas tarefas:

- [Crie um principal de serviço e uma conexão usando o Web Studio](#)
- [Crie um principal de serviço usando o PowerShell](#)
- [Obtenha o segredo do aplicativo no Azure](#)
- [Crie uma conexão usando um principal de serviço existente](#)

## Considerações

- A Citrix recomenda usar o Service Principal 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 a ela as permissões necessárias. Para conexões futuras, você ainda deve se autenticar, mas o Azure lembra seu consentimento anterior e não exige a solicitação 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. Há dois tipos de contas que você deve conhecer: “Trabalho ou escola” e “conta pessoal da Microsoft”. Consulte [CTX219211](#) para obter detalhes.
- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, pode haver complicações se o usuário já tiver recebido acesso de convidado a um dos recursos do diretório. Nesse caso, eles podem ter uma entrada de espaço reservado no diretório que não lhes concede as permissões necessárias, e um erro é retornado. Corrija isso removendo os recursos do diretório e adicionando-os de volta explicitamente. No entanto, use essa opção com cuidado, pois ela tem efeitos não intencionais para outros recursos que a conta possa acessar.
- Há um problema conhecido em que determinadas contas são detectadas como convidadas do diretório quando, na verdade, são membros. Configurações como essa geralmente ocorrem com contas de diretório estabelecidas mais antigas. Solução alternativa: adicione uma conta ao diretório, que usa o valor de associação adequado.
- Os grupos de recursos são simplesmente contêineres de recursos e podem conter recursos de outras regiões além de sua própria região. Isso pode ser potencialmente confuso se você espera 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 de que você precisa. Isso exige alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientações sobre a capacidade do espaço de endereço.

## Crie um principal de serviço e uma conexão usando o Web Studio

### Importante:

Esse 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 diretores de serviço dão às conexões acesso aos recursos do Azure. Quando você se autentica no Azure para criar um serviço principal, 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 nesse caso) usa o segredo do cliente para se autenticar no Azure AD.

Antes de começar, verifique se você atendeu a esses 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 globais de administrador, administrador de aplicativos ou desenvolvedor de aplicativos para autenticação. Essas permissões podem ser revogadas após a criação da conexão com o host. Para obter mais informações sobre funções, consulte [Funções integradas 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 **Próximo**.
3. Na página **Connection Details**, insira seu ID de assinatura do Azure e um nome para a conexão. Depois de inserir o ID da assinatura, o botão **Criar novo** é ativado.

**Nota:**

O nome da conexão pode conter de 1 a 64 caracteres e não pode conter somente espaços em branco nem os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' .`

4. Selecione **Criar novo** e, em seguida, digite o nome de usuário e a senha da conta do Azure Active Directory.
5. Selecione **Fazer login**.
6. Selecione **Aceitar** para conceder ao Citrix Virtual Apps and Desktops as permissões listadas. O Citrix Virtual Apps and Desktops cria um principal de serviço que permite gerenciar os recursos do Azure em nome do usuário especificado.
7. Depois de selecionar **Aceitar**, você retornará à página **Connection** no assistente.

**Nota:**

Depois de se autenticar com sucesso no Azure, os botões **Criar novo** e **Usar** existentes 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 **Connection Details**, selecione **Next**.

**Nota:**

Você não pode prosseguir para a próxima página até se autenticar com êxito no Azure e consentir em conceder as permissões necessárias.

9. Configure os recursos para a conexão. Os recursos abrangem a região e a rede.

- Na página **Região**, selecione uma região.
- Na página **Network**, faça o seguinte:
  - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. O nome de um recurso não pode conter somente 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, emparelhar o nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver redes virtuais, retorne a essa página e selecione uma região que tenha redes virtuais.

10. Na página **Summary**, veja um resumo das configurações e selecione **Finish** para concluir sua configuração.

**Exibir o ID do aplicativo** Depois de criar uma conexão, você pode ver o ID do aplicativo que a conexão usa para acessar os recursos do Azure.

Na lista **Adicionar conexão e recursos**, selecione a conexão para ver os detalhes. A guia **Details** mostra a ID do aplicativo.

### Crie um principal de serviço usando o PowerShell

Para criar um principal de serviço usando o PowerShell, conecte-se à sua assinatura do Azure Resource Manager e use os cmdlets do PowerShell fornecidos nas seções a seguir.

Certifique-se de ter esses itens prontos:

- **SubscriptionID:** Azure Resource Manager `SubscriptionID` para a assinatura em que 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.

```
1 `Connect-AzAccount`
```

1. Selecione a assinatura do Azure Resource Manager na qual você deseja criar o principal do serviço.

```
Get-AzSubscription -SubscriptionId $subscriptionId | Select-  
AzSubscription
```

2. Crie o aplicativo em seu locatário do AD.

```
$AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
```

3. Crie um diretor de serviço.

```
New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
```

4. Atribua uma função ao diretor do 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 essa ID ao criar a conexão do host.

### Obtenha o segredo do aplicativo no Azure

Para criar uma conexão usando um principal de serviço existente, primeiro você deve obter o ID do aplicativo e o segredo do principal de serviço no portal do Azure.

As etapas detalhadas são as seguintes:

1. Obtenha a ID do aplicativo \*\* no Web Studio ou usando o PowerShell.
2. Entre no portal do Azure.
3. No Azure, selecione **Azure Active Directory**.
4. Em **Registros de aplicativos** no Azure AD, selecione seu aplicativo.
5. Vá para **Certificates & secrets**.
6. Clique em **Client secrets**.

### Crie uma conexão usando um principal de serviço existente

Se você já tiver um principal de serviço, poderá usá-lo para criar uma conexão usando o Web Studio.

Certifique-se de ter esses itens prontos:

- ID da assinatura
- ActiveDirectoryID (ID do inquilino)
- ID do aplicativo

- Segredo do aplicativo

Para obter mais informações, consulte [Obtenha o segredo do aplicativo](#).

- Data de expiração secreta

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 **Próximo**.
3. Na página **Connection Details** , insira seu ID de assinatura do Azure e um nome para a conexão.

**Nota:**

O nome da conexão pode conter de 1 a 64 caracteres e não pode conter somente espaços em branco nem os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' .`

4. Selecione **Usar existente**. Na janela **Detalhes do diretor 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 avançar além desta página até fornecer detalhes válidos.

- **ID de assinatura**. Insira seu ID de assinatura do Azure. Para obter sua ID de assinatura, entre no portal do Azure e navegue até **Assinaturas > Visão geral**.
- **ID do Active Directory** (ID do inquilino). 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 se autenticar no Azure AD. Recomendamos que você altere as chaves regularmente para fins de segurança. Certifique-se de salvar a chave porque você não pode recuperá-la posteriormente.
- **Data de validade secreta**. Insira a data após a qual o segredo do aplicativo expira. Você recebe um alerta no console antes que a chave secreta expire. No entanto, se a chave secreta expirar, você receberá erros.

**Nota:**

Por motivos de segurança, o período de expiração não pode ser superior a dois anos

a partir de agora.

- **URL de autenticação.** Esse campo é preenchido automaticamente e não é editável.
- **URL de gerenciamento.** Esse campo é preenchido automaticamente e não é editável.
- **Sufixo de armazenamento.** Esse 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/>. Essa é uma URL de solicitação para as 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/](https://*.core.windows.net/). Esse (\*) é um caractere curinga para o sufixo de armazenamento. Por exemplo, <https://demo.table.core.windows.net/>.

5. Depois de selecionar **Salvar**, você retorna à página **Connection Details**. Selecione **Próximo** para continuar na próxima página.
6. Configure os recursos para a conexão. Os recursos abrangem a região e a rede.
  - Na página **Região**, selecione uma região.
  - Na página **Network**, faça o seguinte:
    - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. O nome de um recurso não pode conter somente 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, emparelhar o nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver redes virtuais, retorne a essa página e selecione uma região que tenha redes virtuais.
7. Na página **Summary**, veja um resumo das configurações e selecione **Finish** para concluir sua configuração.

## Gerencie conexões e diretores de serviços

Esta seção detalha como você pode gerenciar conexões e diretores de serviços:

- Definir as configurações de limitação do Azure

- Habilitar o compartilhamento de imagens no Azure
- Adicionar inquilinos compartilhados a uma conexão usando o Web Studio
- Implemente o compartilhamento de imagens usando o PowerShell
- Gerencie o segredo do aplicativo e a data de expiração secreta

### Definir as configurações de limitação do Azure

O Azure Resource Manager limita as solicitações de assinaturas e locatários, roteando o tráfego com base em limites definidos, de acordo com as necessidades específicas do provedor. Consulte [Throttling Resource Manager requests](#) no site da Microsoft para obter mais informações. Existem limites para assinaturas e locatários, onde o gerenciamento de muitas máquinas pode se tornar problemático. Por exemplo, uma assinatura contendo muitas máquinas pode apresentar problemas de desempenho relacionados às operações de energia.

#### Dica:

Para obter mais informações, consulte [Melhorando o desempenho do Azure com os Serviços de Criação de Máquinas](#).

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 ativar ou desativar as VMs em grandes assinaturas, por exemplo, aquelas que contêm 1.000 VMs:

- Operações simultâneas absolutas: 500
- Máximo de novas operações por minuto: 2000
- Simultaneidade máxima de operações: 500

Use o Web Studio para configurar as operações do Azure para uma determinada conexão do Azure:

1. No Web Studio, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão.
3. No assistente **Editar conexão**, selecione **Avançado**.
4. Na página **Advanced**, use as opções de configuração para especificar o número de ações simultâneas e o máximo de novas ações por minuto, além de outras opções de conexão.



**Edit Connection**  
Azure-08

Connection Properties  
Advanced  
Scopes

**Advanced**  
Use these settings to specify a maximum number of simultaneous actions (or concurrent machines) per hosting connection. For simultaneous actions, specify both settings. The lower value overrides the higher value. [Learn more](#)

	Absolute	Percentage (%)
Simultaneous actions (all types): ?	500	100
Maximum new actions per minute:	2000	

Connection options:

Use this setting only when Citrix Technical Support or the product documentation makes the recommendation.

Save Apply Cancel

O MCS suporta no máximo 500 operações simultâneas por padrão. Como alternativa, você pode usar o SDK remoto do PowerShell para definir o número máximo de operações simultâneas.

Use a propriedade **PowerShell** , `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações simultâneas de provisionamento do Azure. Ao usar essa propriedade, considere:

- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` usando o comando do 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:

- Compartilhe imagens dentro de um inquilino (em todas as assinaturas)
- Compartilhe imagens entre inquilinos

**Compartilhe imagens dentro de um inquilino (em todas as assinaturas)** Para selecionar uma imagem na Galeria de Computação do Azure que pertença a uma assinatura diferente, a imagem deve ser compartilhada com o principal de serviço (SPN) dessa assinatura.

Por exemplo, se houver um serviço principal (SPN 1), configurado no Studio como:

Serviço principal: SPN 1

Assinatura: assinatura 1

Inquilino: inquilino 1

A imagem está em uma assinatura diferente, que é configurada no Studio como:

Assinatura: assinatura 2

Inquilino: inquilino 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 a SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em funções (RBAC) do Azure. O Azure RBAC é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o Azure RBAC, consulte o documento da Microsoft [O que é o controle de acesso baseado em funções do Azure \(Azure RBAC\)](#). Para conceder acesso, você atribui funções aos diretores de serviço no escopo do grupo de recursos com a função de Colaborador. Para atribuir funções do Azure, você deve ter a permissão `microsoft.authorization/roleAssignments/write`, como administrador de acesso de usuário ou proprietário. Para obter mais informações sobre o compartilhamento de 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 os comandos do PowerShell, Selecione uma imagem de uma assinatura diferente.

**Compartilhe imagens entre inquilinos** Para compartilhar imagens entre locatários com a Galeria de Computação do Azure, crie um registro de aplicativo.

Por exemplo, se houver dois inquilinos (inquilino 1 e inquilino 2) e você quiser compartilhar sua galeria de imagens com o inquilino 1, então:

1. Crie um registro de inscrição para o Tenant 1. Para obter mais informações, consulte [Criar o registro do aplicativo](#).
2. Dê ao Tenant 2 acesso ao aplicativo solicitando um login usando um navegador. Substitua `Tenant2 ID` pela ID de inquilino do Tenant 1. Substitua `ID do aplicativo (cliente)` pelo ID do aplicativo do registro do aplicativo que você criou. Quando terminar de fazer as substituições, cole o URL em um navegador e siga as instruções de login para entrar no Tenant 2. Por exemplo:

```
1 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 Tenant 2](#).

3. Conceda ao aplicativo acesso ao grupo de recursos Tenant 2. Faça login como Tenant 2 e conceda ao registro do aplicativo acesso ao grupo de recursos que tem a imagem da galeria. Para obter mais informações, consulte [Autenticar solicitações entre inquilinos](#).

Para criar um catálogo usando uma imagem de um locatário diferente usando os comandos do PowerShell:

1. Atualize as propriedades personalizadas da conexão de hospedagem com IDs de inquilino compartilhados.
2. Selecione uma imagem de um inquilino diferente.

### **Adicionar inquilinos compartilhados a uma conexão usando o Web Studio**

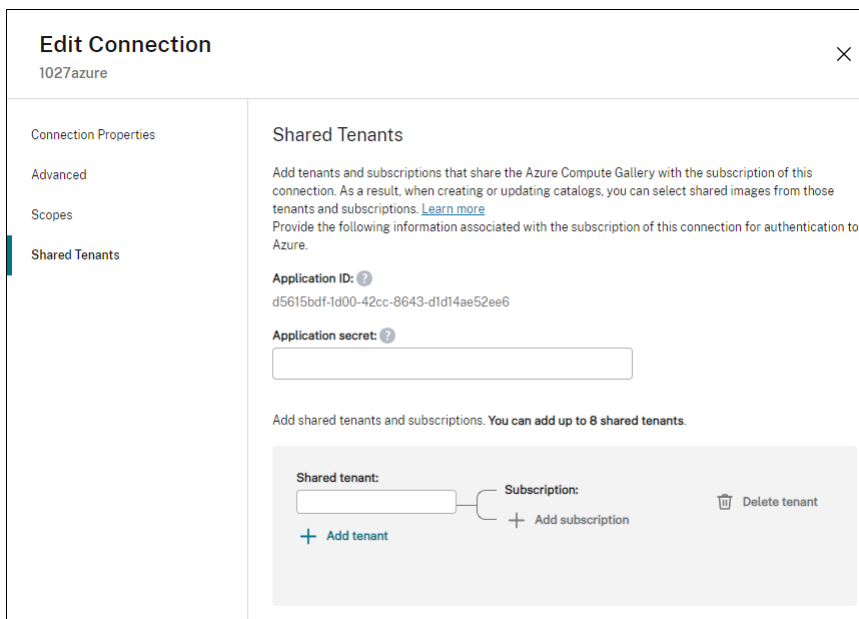
Ao criar ou atualizar catálogos de máquinas no Web Studio, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas por meio da Galeria de Computação do Azure). O recurso exige que você forneça informações compartilhadas de inquilino e assinatura para conexões de host associadas.

#### **Nota:**

Verifique se você definiu as configurações necessárias no Azure para permitir o compartilhamento de imagens entre inquilinos. Para obter mais informações, consulte [Compartilhar imagens entre inquilinos](#).

Conclua as seguintes etapas para uma conexão:

1. No Web Studio, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar conexão** na barra de ação.



3. Em **Shared Tenants**, 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 se 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 inquilinos compartilhados e 8 assinaturas para cada inquilino.

4. Ao terminar, selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

## Implemente o compartilhamento de imagens usando o PowerShell

Esta seção orienta você nos processos de compartilhamento de imagens usando o PowerShell:

- Selecione uma imagem de uma assinatura diferente
- Atualize as propriedades personalizadas da conexão de hospedagem com IDs de inquilino compartilhados
- Selecione uma imagem de um inquilino diferente

**Selecione uma imagem de uma assinatura diferente** Você pode selecionar uma imagem na Galeria de Computação do Azure que pertença a uma assinatura compartilhada diferente no mesmo locatário do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, a Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.

2. Liste todas as assinaturas compartilhadas em um localatário.

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\  
sharedsubscription.folder"
```

3. Selecione uma assinatura compartilhada e liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\  
abc123.sharedsubscription"
```

4. Selecione um grupo de recursos e liste todas as galerias desse grupo de recursos.

```
1 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.

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\  
abc123.sharedsubscription\xyz.resourcegroup\testgallery.  
gallery"
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões dessa definição de imagem.

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\  
abc123.sharedsubscription\xyz.resourcegroup\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 remoto do PowerShell, consulte <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>.

**Atualize as propriedades personalizadas da conexão de hospedagem com IDs de inquilino compartilhados** Use `Set-Item` para atualizar as propriedades personalizadas da conexão de hospedagem com IDs de inquilino e IDs de assinatura compartilhados. Adicione uma propriedade `SharedTenants` em `CustomProperties`. O formato do `Shared Tenants` é:

```
1 [ {  
2   "Tenant": "94367291-119e-457c-bc10-25337231f7bd", "Subscriptions": [ "7  
bb42f40-8d7f-4230-a920-be2781f6d5d9" ] } ]
```

```

3  ,{
4  "Tenant": "50e83564-c4e5-4209-b43d-815c45659564", "Subscriptions": ["06
      ab8944-6a88-47ee-a975-43dd491a37d0"] }
5  ]

```

Por exemplo:

```

1  Set-Item -CustomProperties "<CustomProperties xmlns='http://schemas.
      citrix.com/2014/xd/machinecreation' xmlns:xsi='http://www.w3.org
      /2001/XMLSchema-instance'"
2  <Property xsi:type='StringProperty' Name='SubscriptionId' Value='
      123' />
3  <Property xsi:type='StringProperty' Name='ManagementEndpoint'
      Value='https://management.azure.com/' />
4  <Property xsi:type='StringProperty' Name='AuthenticationAuthority'
      Value='https://login.microsoftonline.com/' />
5  <Property xsi:type='StringProperty' Name='StorageSuffix' Value='
      core.windows.net' />
6  <Property xsi:type='StringProperty' Name='TenantId' Value='123
      abc' />
7  <Property xsi:type='StringProperty' Name='SharedTenants' Value='
      '[ {
8  'Tenant':'123abc', 'Subscriptions':['345', '567'] }
9  ]'` />
10 </CustomProperties>"
11 -LiteralPath @("XDHyp:\Connections\azure") -PassThru -UserName "
      advc345" -SecurePassword
12 $psd

```

#### Nota:

Você pode adicionar mais de um inquilino. Cada inquilino pode ter mais de uma assinatura.

**Selecione uma imagem de um inquilino diferente** Você pode selecionar uma imagem na Galeria de Computação do Azure que pertença a um locatário diferente do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, a Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.
2. Liste todas as assinaturas compartilhadas.

```

1  Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.
      folder

```

3. Selecione uma assinatura compartilhada e liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

```

1  Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription

```

4. Selecione um grupo de recursos e liste todas as galerias desse grupo de recursos.

```
1 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.

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.  
sharedsubscription\xyz.resourcegroup\efg.gallery
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões dessa definição de imagem.

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.  
sharedsubscription\xyz.resourcegroup\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 remoto do PowerShell, consulte <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>.

## Gerencie o segredo do aplicativo e a data de expiração secreta

Certifique-se de alterar o segredo do aplicativo para uma conexão antes que o segredo expire. Você recebe um alerta no Web Studio antes que a chave secreta expire.

**Crie um segredo de aplicativo no Azure** Você pode criar um segredo de aplicativo para uma conexão por meio do portal do Azure.

1. Selecione **Azure Active Directory**.
2. Em **Registros de aplicativos** no Azure AD, selecione seu aplicativo.
3. Vá para **Certificates & secrets**.
4. Clique em **Segredos do cliente > Novo segredo do cliente**.
5. Forneça uma descrição do segredo e especifique uma duração. Quando terminar, selecione **Adicionar**.

**Nota:**

Certifique-se de salvar o segredo do cliente porque você não pode recuperá-lo mais tarde.

6. Copie o valor secreto do cliente e a data de validade.
7. No Web Studio, edite a conexão correspondente e substitua o conteúdo no campo **Application secret** e **Secret expiration date** pelos valores que você copiou.

**Alterar a data de expiração secreta** Você pode usar o Web Studio para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

1. No assistente **Adicionar conexão e recursos**, clique com o botão direito do mouse em uma conexão e clique em **Editar conexão**.
2. Na página **Connection Properties**, clique em **Data de expiração secreta** para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

## Permissões necessárias do Azure

Esta seção contém as permissões mínimas e gerais necessárias para o Azure.

### Permissões mínimas

As permissões mínimas oferecem melhor controle de segurança. No entanto, os novos recursos que exigem permissões adicionais falham devido ao uso apenas de permissões mínimas.

**Criação de uma conexão de host** Adicione uma nova conexão de host usando as informações obtidas do Azure.

```
1 "Microsoft.Network/virtualNetworks/read",
2 "Microsoft.Compute/virtualMachines/read",
3 "Microsoft.Compute/disks/read",
```

**Gerenciamento de energia de VMs** Ligue ou desligue as instâncias da máquina.

```
1 "Microsoft.Compute/virtualMachines/read",
2 "Microsoft.Resources/subscriptions/resourceGroups/read",
3 "Microsoft.Compute/virtualMachines/deallocate/action",
4 "Microsoft.Compute/virtualMachines/start/action",
5 "Microsoft.Compute/virtualMachines/restart/action",
```



**Criação, atualização ou exclusão de VMs** Crie um catálogo de máquinas e, em seguida, adicione, exclua, atualize máquinas e exclua o catálogo de máquinas.

A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é gerenciada em disco ou quando os instantâneos estão localizados na mesma região da conexão de hospedagem.

```
1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Resources/deployments/validate/action",
3 "Microsoft.Compute/virtualMachines/read",
4 "Microsoft.Compute/virtualMachines/write",
5 "Microsoft.Compute/virtualMachines/delete",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/snapshots/read",
8 "Microsoft.Compute/snapshots/write",
9 "Microsoft.Compute/snapshots/delete",
10 "Microsoft.Compute/snapshots/beginGetAccess/action",
11 "Microsoft.Compute/snapshots/endGetAccess/action",
12 "Microsoft.Compute/disks/read",
13 "Microsoft.Compute/disks/write",
14 "Microsoft.Compute/disks/delete",
15 "Microsoft.Compute/disks/beginGetAccess/action",
16 "Microsoft.Compute/disks/endGetAccess/action",
17 "Microsoft.Network/virtualNetworks/read",
18 "Microsoft.Network/virtualNetworks/subnets/join/action",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/networkSecurityGroups/read",
21 "Microsoft.Network/networkSecurityGroups/write",
22 "Microsoft.Network/networkSecurityGroups/delete",
23 "Microsoft.Network/networkSecurityGroups/join/action",
24 "Microsoft.Network/networkInterfaces/read",
25 "Microsoft.Network/networkInterfaces/write",
26 "Microsoft.Network/networkInterfaces/delete",
27 "Microsoft.Network/networkInterfaces/join/action",
```

Você precisa das seguintes permissões extras com base nas permissões mínimas para os seguintes recursos:

- Se a imagem mestre for um VHD em uma conta de armazenamento localizada na mesma região da conexão de hospedagem:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
```

- Se a imagem mestre for uma ImageVersion da Galeria de Imagens Compartilhada:

```
1 "Microsoft.Compute/galleries/read",
2 "Microsoft.Compute/galleries/images/read",
3 "Microsoft.Compute/galleries/images/versions/read",
```

- Se a imagem mestre for um disco gerenciado, os instantâneos, ou VHD, estão em uma região diferente da região da conexão de hospedagem:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 "Microsoft.Storage/storageAccounts/write",
4 "Microsoft.Storage/storageAccounts/delete",
```

- Se você usa o grupo de recursos gerenciado pela Citrix:

```
1 "Microsoft.Resources/subscriptions/resourceGroups/write",
2 "Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- Se você colocar a imagem mestre na Galeria de Imagens Compartilhada:

```
1 "Microsoft.Compute/galleries/write",
2 "Microsoft.Compute/galleries/images/write",
3 "Microsoft.Compute/galleries/images/versions/write",
4 "Microsoft.Compute/galleries/read",
5 "Microsoft.Compute/galleries/images/read",
6 "Microsoft.Compute/galleries/images/versions/read",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/versions/delete",
```

- Se você usa o suporte de host dedicado do Azure:

```
1 "Microsoft.Compute/hostGroups/read",
2 "Microsoft.Compute/hostGroups/write",
3 "Microsoft.Compute/hostGroups/hosts/read",
```

- Se você usar a criptografia do lado do servidor (SSE) com chaves gerenciadas pelo cliente (CMK):

```
1 "Microsoft.Compute/diskEncryptionSets/read",
```

- Se você implantar VMs usando modelos ARM (perfil de máquina):

```
1 "Microsoft.Resources/deployments/write",
2 "Microsoft.Resources/deployments/operationstatuses/read",
3 "Microsoft.Resources/deployments/read",
4 "Microsoft.Resources/deployments/delete",
```

- Se você usar a especificação de modelo do Azure como um perfil de máquina:

```
1 "Microsoft.Resources/templateSpecs/read",
2 "Microsoft.Resources/templateSpecs/versions/read",
```

**Criação, atualização e exclusão de máquinas com disco não gerenciado** A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é VHD e usa o grupo de recursos conforme fornecido pelo administrador:

```
1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Storage/storageAccounts/delete",
```

```
3 "Microsoft.Storage/storageAccounts/listKeys/action",
4 "Microsoft.Storage/storageAccounts/read",
5 "Microsoft.Storage/storageAccounts/write",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/virtualMachines/delete",
8 "Microsoft.Compute/virtualMachines/read",
9 "Microsoft.Compute/virtualMachines/write",
10 "Microsoft.Resources/deployments/validate/action",
11 "Microsoft.Network/networkInterfaces/delete",
12 "Microsoft.Network/networkInterfaces/join/action",
13 "Microsoft.Network/networkInterfaces/read",
14 "Microsoft.Network/networkInterfaces/write",
15 "Microsoft.Network/networkSecurityGroups/delete",
16 "Microsoft.Network/networkSecurityGroups/join/action",
17 "Microsoft.Network/networkSecurityGroups/read",
18 "Microsoft.Network/networkSecurityGroups/write",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/virtualNetworks/read",
21 "Microsoft.Network/virtualNetworks/subnets/join/action"
```

### Permissão geral

A função de colaborador tem acesso total para gerenciar todos os recursos. Esse conjunto de permissões não impede que você obtenha novos recursos.

O conjunto de permissões a seguir fornece a melhor compatibilidade no futuro, embora inclua mais permissões do que o necessário com o conjunto de recursos atual:

```
1 "Microsoft.Compute/diskEncryptionSets/read",
2 "Microsoft.Compute/disks/beginGetAccess/action",
3 "Microsoft.Compute/disks/delete",
4 "Microsoft.Compute/disks/endGetAccess/action",
5 "Microsoft.Compute/disks/read",
6 "Microsoft.Compute/disks/write",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/read",
10 "Microsoft.Compute/galleries/images/versions/delete",
11 "Microsoft.Compute/galleries/images/versions/read",
12 "Microsoft.Compute/galleries/images/versions/write",
13 "Microsoft.Compute/galleries/images/write",
14 "Microsoft.Compute/galleries/read",
15 "Microsoft.Compute/galleries/write",
16 "Microsoft.Compute/hostGroups/hosts/read",
17 "Microsoft.Compute/hostGroups/read",
18 "Microsoft.Compute/hostGroups/write",
19 "Microsoft.Compute/snapshots/beginGetAccess/action",
20 "Microsoft.Compute/snapshots/delete",
21 "Microsoft.Compute/snapshots/endGetAccess/action",
22 "Microsoft.Compute/snapshots/read",
23 "Microsoft.Compute/snapshots/write",
```

```
24 "Microsoft.Compute/virtualMachines/deallocate/action",
25 "Microsoft.Compute/virtualMachines/delete",
26 "Microsoft.Compute/virtualMachines/read",
27 "Microsoft.Compute/virtualMachines/restart/action",
28 "Microsoft.Compute/virtualMachines/start/action",
29 "Microsoft.Compute/virtualMachines/write",
30 "Microsoft.Network/networkInterfaces/delete",
31 "Microsoft.Network/networkInterfaces/join/action",
32 "Microsoft.Network/networkInterfaces/read",
33 "Microsoft.Network/networkInterfaces/write",
34 "Microsoft.Network/networkSecurityGroups/delete",
35 "Microsoft.Network/networkSecurityGroups/join/action",
36 "Microsoft.Network/networkSecurityGroups/read",
37 "Microsoft.Network/networkSecurityGroups/write",
38 "Microsoft.Network/virtualNetworks/subnets/read",
39 "Microsoft.Network/virtualNetworks/read",
40 "Microsoft.Network/virtualNetworks/subnets/join/action",
41 "Microsoft.Resources/deployments/operationstatuses/read",
42 "Microsoft.Resources/deployments/read",
43 "Microsoft.Resources/deployments/validate/action",
44 "Microsoft.Resources/deployments/write",
45 "Microsoft.Resources/deployments/delete",
46 "Microsoft.Resources/subscriptions/resourceGroups/read",
47 "Microsoft.Resources/subscriptions/resourceGroups/write",
48 "Microsoft.Resources/subscriptions/resourceGroups/delete",
49 "Microsoft.Storage/storageAccounts/delete",
50 "Microsoft.Storage/storageAccounts/listKeys/action",
51 "Microsoft.Storage/storageAccounts/read",
52 "Microsoft.Storage/storageAccounts/write",
53 "Microsoft.Resources/templateSpecs/read",
54 "Microsoft.Resources/templateSpecs/versions/read",
```

## Configurar as permissões de conexão de host do Azure necessárias

Você pode configurar facilmente todas as permissões mínimas necessárias para uma conta principal de serviço ou de usuário no Azure vinculada a uma conexão de host para realizar todas as operações do MCS usando um modelo ARM. Esse modelo ARM automatiza o seguinte:

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

Você pode implantar esse modelo ARM usando o Portal do Azure ou os comandos do PowerShell. Para obter mais informações, consulte [Modelo ARM para operações CVAD](#).

## Para onde ir a seguir

- Se você estiver no processo inicial de implantação, consulte [Criar catálogos de máquinas](#)
- Para obter informações específicas do Azure, consulte [Criar um catálogo do Microsoft Azure](#)

## Mais informações

- [Conexões e recursos](#)
- [Crie catálogos de máquinas](#)

## Gerenciamento de imagens (prévia)

August 22, 2024

### Introdução

O processo de criação ou atualização do 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 do MCS diferentes. Essa implementação reduz significativamente os custos de armazenamento e tempo e simplifica o processo de implantação da VM e de atualização de imagens.

Os benefícios de usar essa funcionalidade de gerenciamento de imagens são:

- Gere imagens preparadas com antecedência sem criar um catálogo.
- Reutilize imagens preparadas em vários cenários, como criar e atualizar um catálogo.
- Reduza significativamente o tempo de criação ou atualização do catálogo.

#### Nota:

- Atualmente, esse recurso é aplicável aos ambientes de virtualização do Azure e da VMware.
- Você pode criar um catálogo de máquinas do 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:

- gerencie diferentes iterações ou atualizações em uma imagem específica.
  - mantenha várias versões de uma imagem para finalidades diferentes.
- *Agrupamento lógico* —Você pode criar várias definições de imagem para:
- agrupar logicamente versões de imagens com base em vários critérios, como projeto, departamento ou aplicativo e tipo de área de trabalho.
  - gerenciar imagens com mais eficiência dentro de uma organização.

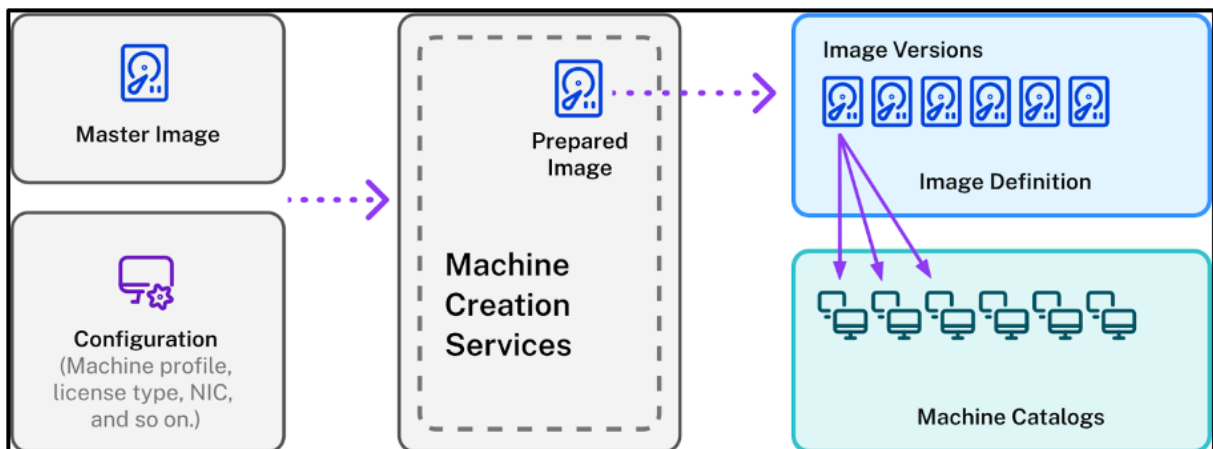
## O que é uma imagem preparada?

Com a funcionalidade de gerenciamento de imagens, o MCS separa a fase de masterização do fluxo de trabalho geral de criação ou atualização do catálogo e divide o processo em dois estágios:

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 do 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 do MCS quando você usa 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 que serve o sistema operacional
- outras informações sobre o uso da imagem.

Um catálogo não é criado a partir de uma definição de imagem, mas das versões de imagem que são criadas com base na definição de imagem.

*Versão da imagem:* as versões da imagem gerenciam as versões para a definição de imagem. Uma definição de imagem pode ter várias versões de imagem. Use as versões de imagem como imagens preparadas para criar ou atualizar um catálogo.

Como alternativa, se você quiser usar os comandos do PowerShell para criar um esquema de provisionamento para criar ou atualizar um catálogo, deverá criar uma especificação de versão de imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para seu ambiente.

## Participar do Tech Preview

Se você estiver interessado em participar do Tech Preview, forneça suas informações de contato [aqui](#).

Ajudaremos você a configurar o ambiente de teste e forneceremos suporte técnico, se necessário.

## Requisito

- Para a imagem mestre do Windows, somente imagens do VDA com a versão 2311 e posterior e o MCS/IO habilitado são permitidas.

## Limitações

Atualmente, o recurso não oferece suporte ao seguinte:

- Várias NICs no Azure
- Recurso de disco de dados persistente
- Hibernação para várias sessões
- Alteração do tipo de imagem

## Gerenciamento do ciclo de vida de imagens usando o Web Studio

O ciclo de vida da imagem quando você usa o Web Studio é:

1. Crie 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. Use uma versão de imagem como uma imagem preparada para criar catálogos.
4. Atualize um catálogo de máquinas com uma imagem preparada diferente.
5. Gerencie as definições e versões da imagem: edite o nome e a descrição das versões da imagem e a descrição de uma definição de imagem.
6. Exclua uma versão da imagem.

7. Exclua uma definição de imagem.

Como alternativa, você também pode gerenciar imagens usando o PowerShell. Consulte Gerenciamento do ciclo de vida de imagens 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 do MCS usando:

- O Web Studio
- Os comandos do PowerShell

### **Usar o Web Studio**

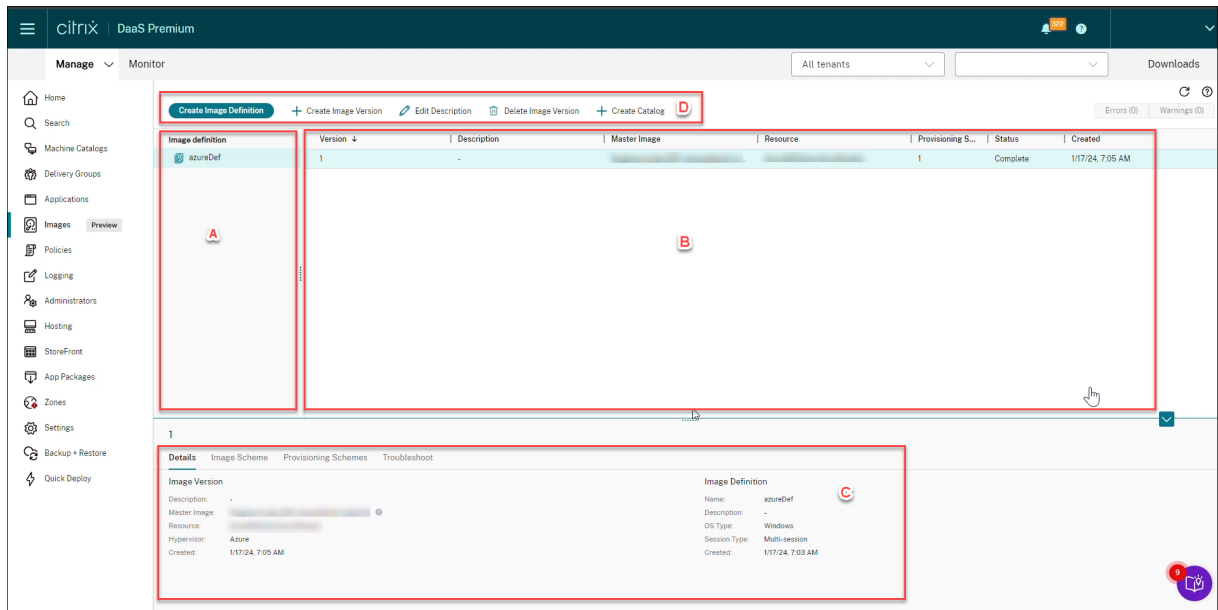
Veja os tópicos a seguir:

- Entender o nó Imagens
- Criar uma definição de imagem e uma 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 computadores
- Atualizar um catálogo de máquinas com uma imagem preparada diferente
- Gerenciar as definições e versões da imagem

### **Entender o nó Imagens**

Use o nó **Imagens** para criar e gerenciar imagens preparadas pelo MCS. Sua visão 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.
C	Detalhes	<ul style="list-style-type: none"> <li>A guia <b>Detalhes</b> exibe informações detalhadas sobre a definição ou versão de imagem selecionada, como                             <ul style="list-style-type: none"> <li>imagem mestre, recurso, hipervisor, nome da definição de imagem e versão de imagem, como <b>Criar versão da imagem</b>, <b>Editar descrição</b>, <b>Excluir versão da imagem</b> e <b>Criar catálogo</b>.</li> </ul> </li> <li>A guia <b>Esquema de imagem</b> exibe</li> </ul>
D	Barra de ação	Lista as ações que você pode realizar nas definições e versões de imagem, como <b>Criar versão da imagem</b> , <b>Editar descrição</b> , <b>Excluir versão da imagem</b> e <b>Criar catálogo</b> .

### Criar um catálogo de máquinas usando a imagem preparada

As principais etapas para criar um catálogo de máquinas do MCS usando a imagem preparada são:

1. Crie a definição de imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo.

- A guia **Esquemas de provisionamento** exibe o nome do esquema de

## Criar uma definição de imagem e uma versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. Entre no Web Studio e selecione o nó **Imagens**. Clique em **Avançar** na página de **introdução**.
2. Na página **Definição de imagem**, especifique o **Tipo de sistema operacional** e o **Tipo de sessão** para a definição de 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 selecione um perfil de máquina.

### Nota:

Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. (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.

### Nota:

Se você selecionar um perfil de máquina na página **Imagem**, o tipo de licença do perfil da máquina será pré-selecionado com base na configuração do perfil.

5. Na página **Especificações da máquina**:

- Para o Azure, selecione um tamanho de máquina. Se você selecionar um perfil de máquina na página **Imagem**, o tamanho da máquina do perfil da máquina será selecionado por padrão.
- Para a VMware, se você selecionar um perfil de máquina, poderá ver a contagem de CPUs virtuais derivada do perfil da máquina e ela permanecerá inalterável. Se você não selecionar um perfil de máquina, poderá ver somente 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 a 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 imutável.

### Nota:

Várias NICs não são permitidas no Azure.

7. (Somente para Azure) Na página **Configurações do 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 de imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição de imagem. Clique em **Finish**.

### **Criar versões de imagem**

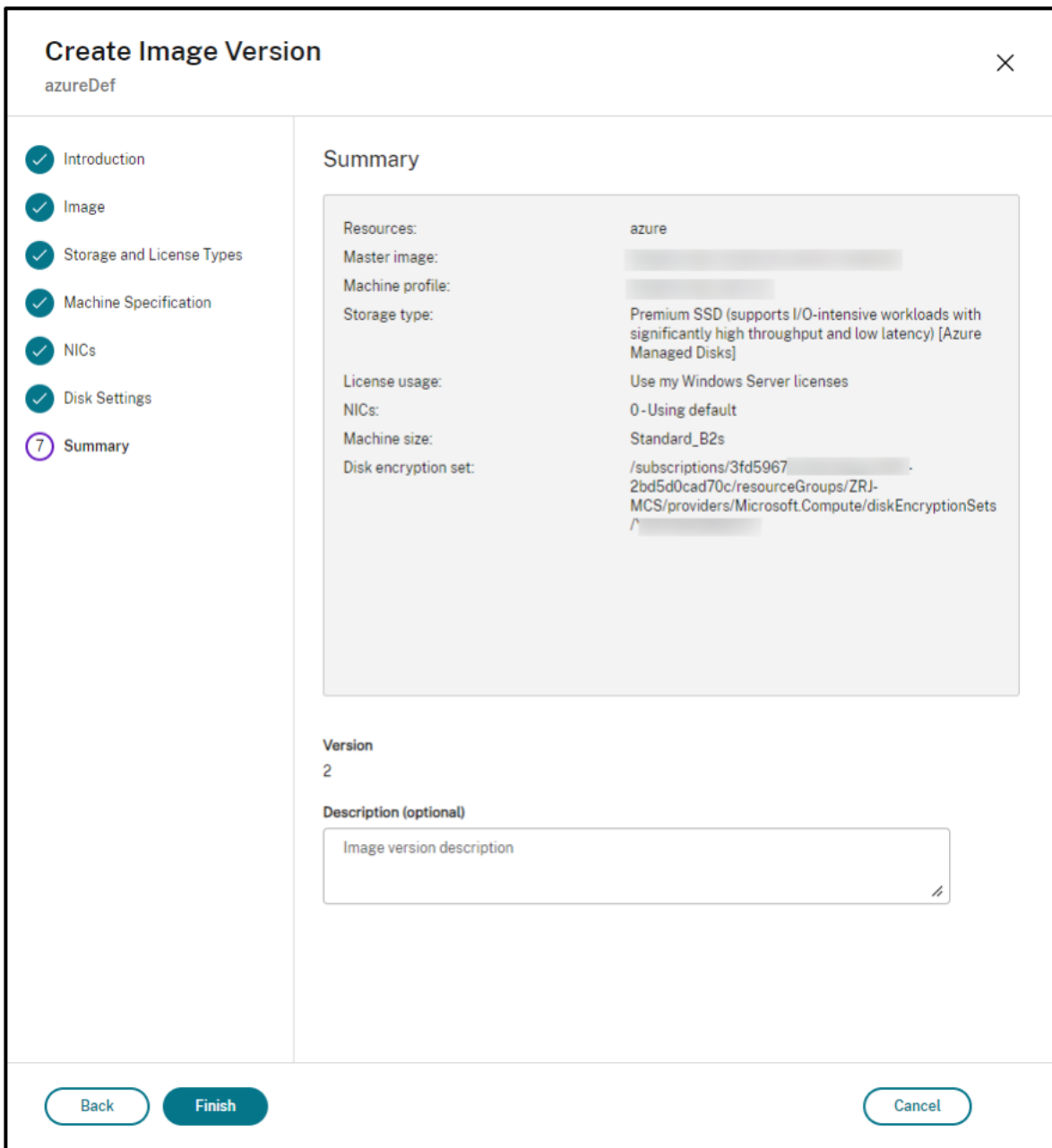
As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações em uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para finalidades diferentes.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

**Nota:**

A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá até o nó **Imagens**, selecione uma versão da imagem e selecione **Criar versão da imagem**.
2. Se você quiser que a configuração da versão de imagem seja diferente da versão inicial da imagem configurada, defina as configurações nas páginas **Imagem**, **Armazenamento e tipos de licença**, **Especificação da máquina**, **NICs** e **Configurações do disco** da caixa de diálogo **Criar versão da imagem**.
3. Adicione uma descrição para a versão da imagem. Clique em **Finish**.



### 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.

Como alternativa, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de computadores**, vinculando à opção de imagem preparada no fluxo de trabalho de criação do catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de computadores

Para criar um catálogo de máquinas do 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 de **introdução**.
2. Na página **Experiência de área de trabalho**, selecione a experiência de área de trabalho necessária.
3. Da página **Imagem** até a página **Configurações do disco**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. (Para Azure) Na página **Grupo de recursos**, você pode escolher criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos desse catálogo.
5. Conclua as configurações nas páginas a seguir.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Finish**.
7. Acesse o nó **Catálogos de computadores** para ver o catálogo de máquinas criado.

### **Criar um catálogo de máquinas a partir do nó Catálogos de computadores**

Para criar um catálogo de máquinas do MCS a partir do nó **Catálogos de computadores**, faça o seguinte:

1. Clique em **Catálogos de computadores** 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 da imagem de uma definição de imagem.
  - c) Clique no nome da versão da imagem. Para exibir 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. Defina as configurações nas páginas a seguir.
5. Na página **Configurações do 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 escolher criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos desse catálogo.
7. Conclua as configurações nas páginas a seguir.
8. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Finish**.

## Atualizar um catálogo de máquinas com uma imagem preparada diferente

Para atualizar um catálogo de máquinas do MCS existente com uma imagem preparada diferente, faça o seguinte:

1. Clique em **Catálogos de computadores** no painel de navegação esquerdo e selecione um catálogo de máquinas que você deseja atualizar. Clique com o botão direito do mouse e selecione **Alterar imagem preparada**.
2. Na página **Imagem**, selecione uma imagem preparada.
3. Na página **Estratégia de implantação**, selecione quando você deseja atualizar esse catálogo com a imagem preparada selecionada.
4. Na página **Resumo**, verifique os detalhes. Clique em **Finish**.

**Você pode ver o histórico das 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 da 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 da imagem para especificar a finalidade dessa versão da imagem.

Para editar uma versão da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão da imagem e selecione **Editar descrição**.

**Excluir uma versão da imagem** Para excluir uma versão da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão da imagem e selecione **Excluir versão da imagem**.

**Nota:**

Você não poderá excluir uma versão da imagem se ela for usada por um catálogo de máquinas.

**Excluir uma definição de imagem** Para excluir uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Excluir definição de imagem**.

**Nota:**

Você não poderá excluir uma definição de imagem se ela contiver uma versão da imagem.

**Gerenciamento do ciclo de vida de imagens usando o PowerShell** Se você quiser usar os comandos do PowerShell para criar um esquema de provisionamento, deverá criar uma especificação de versão da imagem preparada com base na especificação de versão da 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 da imagem. Você pode adicionar uma imagem existente no hipervisor como especificação de versão da imagem mestre ou criar uma especificação de versão da imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para seu ambiente. A especificação da versão da imagem preparada pode ser usada para vários esquemas de provisionamento.

O ciclo de vida de uma imagem durante o uso dos comandos do PowerShell é:

1. Crie uma imagem:
  - a) Crie uma definição de imagem.
  - b) Crie uma versão da imagem.
  - c) Adicione uma especificação de versão da imagem mestre.
  - d) Crie uma especificação de versão da imagem preparada.
2. Crie um catálogo de máquinas do MCS usando uma especificação de versão de imagem preparada:
  - a) Crie um catálogo de agentes.
  - b) Crie um pool de identidades.
  - c) Crie um esquema de provisionamento com o parâmetro da especificação de versão da imagem preparada `Uid` usando o comando `New-ProvScheme`.

- d) Vincule o catálogo de agentes ao esquema de provisionamento.
3. Crie VMs no catálogo de máquinas do MCS.
4. Altere a especificação da versão da imagem preparada de um esquema de provisionamento usando o comando `Set-ProvScheme`.
5. Gerencie as definições e versões de imagem: edite as versões e definições de imagem.
6. Exclua um catálogo de máquinas do MCS: a ordem de exclusão é: especificação da versão da imagem preparada > especificação da versão da imagem mestre > versão da imagem > definição de imagem. Antes de excluir a especificação da versão da imagem, certifique-se de que a especificação da versão da imagem preparada não esteja associada a nenhum catálogo de máquinas do MCS.

## Usar o PowerShell

Você pode fazer o seguinte usando os comandos do PowerShell:

- Criar uma imagem preparada
- Criar um catálogo usando a especificação de versão da imagem preparada
- Atualizar um catálogo usando uma especificação de versão da imagem preparada
- Excluir a definição da imagem, a versão da imagem e a especificação da versão da imagem preparada
- Gerenciar a definição e a versão de imagem
- Obter a definição de imagem, a versão da imagem, a especificação da versão da imagem preparada e os detalhes do esquema de provisionamento

## Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão da imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando o `Test-ProvImageDefinitionNameAvailable` command. Por exemplo,

```
1 Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string  
   []>
```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,



```
1 New-ProvImageDefinition -ImageDefinitionName image1 -OsType
  Windows -VdaSessionSupport MultiSession
```

3. Crie uma versão da imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
1 New-ProvImageVersion -ImageDefinitionName image1 -Description "
  version 1"
```

4. Adicione uma especificação de versão da imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
1 Add-ProvImageVersionSpec -ImageDefinitionName image1 -
  ImageVersionNumber 1 -HostingUnitName azure -MasterImagePath "
  XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
  resourcegroup\win2022-snapshot.snapshot"
```

**Nota:**

Você pode adicionar somente uma especificação de versão da imagem mestre a uma versão da imagem para uma unidade de hospedagem.

5. Crie uma especificação de versão da imagem preparada a partir da especificação de versão da imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
1 New-ProvImageVersionSpec
2 -SourceImageVersionSpecUid c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
  azureresourcegroup.resourcegroup\azure-vnet-eastus.
  virtualprivatecloud\dev.network"
5 -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
```

**Nota:**

Uma unidade de hospedagem e um tipo de preparação podem ter somente uma instância preparada.

**Exemplo do conjunto completo de comandos do Powershell para criar a definição de imagem, a versão da imagem e a especificação de versão da imagem preparada no Azure:**

```
1 $ImageDefintion = New-ProvImageDefinition
2 -ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
  MultiSession
3 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
  $ImageDefintion.ImageDefinitionName -Description "version 1"
```

```

4 $MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
  azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
5 $SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
  $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
  .ImageVersionNumber -HostingUnitName azure -MasterImagePath
  $MasterImagePath
6 $Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
  $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
7   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
  azureresourcegroup.resourcegroup\azure-vnet-eastus.
  virtualprivatecloud\dev.network" }
8   -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
9 Get-ProvTask -TaskId $Task.TaskId

```

**Exemplo do conjunto completo de comandos do Powershell para criar a definição de imagem, a versão da imagem e a especificação de versão da imagem preparada na VMware:**

```

1 $ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
  OsType Windows -VdaSessionSupport SingleSession
2 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
  $ImageDefintion.ImageDefinitionName -Description "version 1"
3 $MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
  master-snap.snapshot"
4 $SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
  $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
  .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
  $MasterImagePath
5 $Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
  $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
6   "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
7   -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
8 Get-ProvTask -TaskId $Task.TaskId

```

**Nota:**

- Todas as especificações da versão da imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão da imagem pode ter somente uma especificação de versão da imagem mestre e uma especificação de versão da imagem preparada.
- Todas as especificações da versão da imagem devem ter um perfil de máquina ou nenhuma das especificações da versão da imagem deve ter um perfil de máquina.
- Você não pode especificar um grupo de recursos ao criar uma especificação de versão da imagem.

## Criar um catálogo usando uma especificação de versão da imagem preparada

Crie um catálogo de máquinas do MCS a partir da especificação da versão da imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
1 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,

```
1 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 do Powershell para criar um catálogo no Azure:

```
1 $Catalog = New-BrokerCatalog -AllocationType "Random" -IsRemotePC
  $False -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
  PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
  SessionSupport "MultiSession"
2 $IdentityPool = New-AcctIdentityPool -AllowUnicode -Domain "azure.
  local" -IdentityPoolName "azurecatalog" -IdentityType "
  ActiveDirectory" -NamingScheme "azure##" -NamingSchemeType "Numeric
  " -Scope @()
3 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
  ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
  PreparationType -eq 'Mcs'"
4 $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 @{
5   "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
  azureresourcegroup.resourcegroup\azure-vnet-eastus.
  virtualprivatecloud\dev.network" }
6   -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
7 Get-ProvTask -TaskId $Task.TaskId
8 $ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
9 Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
.ProvisioningSchemeUid

```

**Exemplo do conjunto completo de comandos do Powershell para criar um catálogo na VMware:**

```

1 $Catalog = New-BrokerCatalog -AllocationType "Random" -IsRemotePC
$False -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
SessionSupport "MultiSession"
2 $IdentityPool = New-AcctIdentityPool -AllowUnicode -Domain "vmware.
local" -IdentityPoolName "vmwarecatalog" -IdentityType "
ActiveDirectory" -NamingScheme "vmware##" -NamingSchemeType "
Numeric" -Scope @()
3 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
PreparationType -eq 'Mcs'"
4 $Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{
5 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
6 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
7 Get-ProvTask -TaskId $Task.TaskId
8 $ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
9 Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
.ProvisioningSchemeUid

```

**Atualizar um catálogo usando uma especificação de versão da imagem preparada**

Você pode atualizar um catálogo usando o comando `Set-ProvSchemeImage`. Por exemplo,

```

1 Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
PurgeJobOnSuccess]

```

Ou,

```

1 Set-ProvSchemeImage -ProvisioningSchemeName <string> -
ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
] [-PurgeJobOnSuccess]

```

**Exemplo do conjunto completo de comandos do Powershell para atualizar um catálogo:**

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -  
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "  
    PreparationType -eq 'Mcs'"  
2 Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -  
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -  
    RunAsynchronously
```

### Excluir a definição da imagem, a versão da imagem e a especificação da versão da imagem preparada

Considere o seguinte antes de excluir uma definição de imagem, versão da imagem e especificação de versão da imagem preparada:

- Uma definição de imagem não poderá ser excluída se ela contiver qualquer versão da imagem.
- Uma versão da imagem não poderá ser excluída se ela contiver qualquer especificação de versão da imagem.
- Uma especificação de versão da imagem mestre não poderá ser excluída se for usada por qualquer outra especificação de versão da imagem preparada.
- Uma especificação de versão da imagem preparada não poderá ser excluída se for usada por qualquer esquema de provisionamento.

As etapas detalhadas são as seguintes:

1. Remova uma especificação de versão da imagem preparada. Por exemplo,

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -  
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "  
    PreparationType -eq 'Mcs'"  
2 Remove-ProvImageVersionSpec -ImageVersionSpecUid  
    $PreparedImageVersionSpec.ImageVersionSpecUid -  
    RunAsynchronously
```

#### Nota:

A especificação da versão da imagem principal só poderá ser excluída quando não há nenhuma especificação de versão da imagem preparada associada.

2. Remova a especificação da versão da imagem mestre. Por exemplo,

```
1 $MasterImageVersionSpec = Get-ProvImageVersionSpec -  
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "  
    PreparationType -eq 'None'"  
2 Remove-ProvImageVersionSpec -ImageVersionSpecUid  
    $PreparedImageVersionSpec.ImageVersionSpecUid -  
    RunAsynchronously
```

3. Remova uma versão da imagem. Por exemplo,

```
1 Remove-ProvImageVersion -ImageDefinitionName image1 -  
ImageVersionNumber 1
```

4. Remova uma definição de imagem. Por exemplo,

```
1 Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos do PowerShell:

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -  
ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "  
PreparationType -eq 'Mcs'"  
2 $Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid  
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously  
3 $MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName  
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"  
4 $Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid  
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously  
5 Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber  
1  
6 Remove-ProvImageDefinition -ImageDefinitionName image1
```

## Gerenciar a definição e a versão de imagem

Você pode renomear e editar uma definição de imagem e editar uma versão da imagem.

- Renomeie uma definição de imagem usando o comando `Rename-ProvImageDefinition`. Por exemplo:

```
1 Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -  
NewImageDefinitionName <string>
```

Ou,

```
1 Rename-ProvImageDefinition -ImageDefinitionName <string> -  
NewImageDefinitionName <string>
```

- Edite uma definição de imagem usando o comando `Set-ProvImageDefinition`. Por exemplo:

```
1 Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description  
<string>]
```

Ou,

```
1 Set-ProvImageDefinition -ImageDefinitionName <string> [-  
Description <string>]
```

- Edite uma versão da imagem usando o comando `Set-ProvImageVersion`. Por exemplo:

```
1 Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

Ou,

```
1 Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber <int> [-Description <string>]
```

### Obter a definição de imagem, a versão da imagem, a especificação da versão da imagem preparada e os detalhes do esquema de provisionamento

- Obtenha detalhes da definição de imagem usando o comando `Get-ProvImageDefinition`. Por exemplo:

```
1 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 versões da imagem em uma definição de imagem,

```
1 Get-ProvImageVersion -ImageDefinitionUid <Guid>
```

Ou,

```
1 Get-ProvImageVersion -ImageDefinitionName <string>
```

- Para obter detalhes da versão da imagem,

```
1 Get-ProvImageVersion -ImageVersionUid <Guid>
```

Ou,

```
1 Get-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber <int>
```

- Prepare a especificação da versão da imagem usando o comando `Get-ProvImageVersionSpec`. Por exemplo:

- Para listar todas as especificações da versão da imagem preparada em uma versão da imagem,

```
1 Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

- Para listar as especificações da versão da imagem mestre em uma especificação de versão da imagem preparada,

```
1 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,

```
1 Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx"'
```

- Para obter especificações de versão da imagem preparada com sucesso em uma versão da imagem,

```
1 Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
```

- Para obter um detalhe de especificação da versão da imagem preparada,

```
1 Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Obtenha detalhes do esquema de provisionamento usando o comando `Get-ProvScheme`. Por exemplo:

```
1 Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
```

- Prepare o histórico de especificações da versão da imagem de um esquema de provisionamento usando o comando `Get-ProvSchemeImageVersionSpecHistory`. Por exemplo:

```
1 Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
    <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
```

## Crie catálogos de máquinas

January 24, 2025



**Importante:**

A partir do Citrix Virtual Apps and Desktops 7 2006, se sua implantação atual usar qualquer uma das seguintes tecnologias, você poderá atualizar sua implantação para a versão atual somente após remover os itens de fim de vida útil (EOL) que usam essas tecnologias.

- VDIs 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 a 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 abrange somente 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 quiser usar conexões de host de nuvem pública para sua implantação, precisará da Licença de Direitos Híbridos para concluir sua nova instalação ou atualizar 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 é interrompida ou interrompida. Uma mensagem explicativa é exibida. Os registros do instalador contêm detalhes. Para obter mais informações, consulte [Atualizar uma implantação](#).

## Introdução

As 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: sistema operacional multissessão ou sistema operacional de sessão única e máquinas Windows ou Linux.

O Web Studio orienta você a criar o primeiro catálogo de máquinas depois de criar o site. Depois de criar o primeiro catálogo, o Web Studio orienta você a criar o primeiro grupo de entrega. Posteriormente, você pode alterar o catálogo criado e criar mais catálogos.

**Dica:**

A atualização de uma implantação existente ativa o recurso de otimização de armazenamento (MCS I/O) do Machine Creation Services (MCS), sem necessidade de configuração adicional. O Virtual Delivery Agent (VDA) e a atualização do Delivery Controller lidam com a atualização de E/S do MCS.

## 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 do sistema a partir da imagem da máquina virtual. Ele ignora o restante dos discos de dados anexados à imagem.
- Se você usa o MCS para provisionar VMs, você fornece uma imagem mestre (ou instantâneo de uma imagem) para criar VMs idênticas no catálogo. Antes de criar o catálogo, primeiro você usa as ferramentas para criar e configurar a imagem mestre. Esse 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 instantâneo), especifica o número de VMs a serem criadas no catálogo e configura informações adicionais.
- Se suas máquinas já estiverem disponíveis, você ainda deverá criar um ou mais catálogos de máquinas para essas máquinas.
- Se você estiver criando um catálogo usando diretamente o SDK do PowerShell, 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. Posteriormente (depois de criar seu primeiro catálogo e grupo de entrega), você poderá alterar as informações sobre essa conexão ou criar mais conexões.

Depois de concluir o assistente de criação do catálogo, os testes são executados automaticamente para garantir que ele esteja configurado corretamente. Quando os testes forem concluídos, você poderá ver um relatório de teste. Execute os testes a qualquer momento no Web Studio.

### 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.

Para obter detalhes técnicos sobre as ferramentas de provisionamento da Citrix, consulte [Citrix Virtual Apps and Desktops Image Management](#).

## Verificação da licença RDS

Atualmente, o Web Studio não realiza a verificação de licenças válidas do Microsoft RDS ao criar um catálogo de máquinas que contém máquinas com sistema operacional Windows multissessão. Para

ver o status da licença Microsoft RDS para uma máquina com sistema operacional multissessão Windows \*\*, **acesse o Citrix Director. Veja o status da licença Microsoft RDS no painel \*\*Machine Details** . Esse painel está na página **Machine Details e User Details** . Para obter mais informações, consulte [Saúde da licença RDS da Microsoft](#).

## Registro de VDA

Um VDA deve ser registrado com um Delivery Controller ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos disponíveis de outra forma. Há vários motivos pelos quais um VDA pode não estar registrado, muitos dos quais um administrador pode solucionar. O Web Studio fornece informações sobre solução de problemas no assistente de criação de catálogos e depois de adicionar 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 talvez não tenha sido obtida informação sobre uma máquina, adicione a máquina mesmo assim.

Para obter mais informações, consulte:

- [CTX136668](#) para orientação de solução de problemas de registro de VDA
- Versões e níveis funcionais do VDA
- [Métodos de registro de VDA](#)

## Resumo da criação do catálogo MCS

Aqui está uma breve visão geral das ações padrão do MCS depois de fornecer 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 coloca a cópia 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 para leitura e compartilhada entre as VMs recém-criadas.
- Um disco de identidade exclusivo de 16 MB que dá a cada VM uma identidade exclusiva. Cada VM recebe um disco de identidade.
- Um disco diferenciado exclusivo para armazenar gravações feitas na VM. Esse disco é provisionado de forma fina (se suportado pelo armazenamento host) e aumenta até o tamanho máximo da imagem mestre, se necessário. Cada VM recebe um disco diferente. O disco de diferença contém as alterações feitas durante as sessões. É permanente para desktops dedicados. Para desktops agrupados, ele é excluído e um novo é criado após cada reinicialização por meio do controlador de entrega.

Como alternativa, ao criar VMs para fornecer desktops estáticos, você pode especificar (na página **Machines** do assistente de criação de catálogos) clones de VM espessos (cópia completa). Os clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem seu próprio arquivo.

### Considerações sobre armazenamento do MCS

Há muitos fatores ao decidir sobre soluções, configurações e capacidades de armazenamento para o MCS. As informações a seguir fornecem considerações apropriadas sobre a capacidade de armazenamento:

*Considerações sobre a capacidade:*

- Discos

Os discos Delta ou Differencing (Diff) consomem a maior quantidade de espaço na maioria das implantações de MCS para cada VM. Cada VM criada pelo MCS recebe no mínimo 2 discos após a criação.

- Disk0 = Diff Disk: contém o sistema operacional quando copiado da imagem base principal.
- Disk1 = Identity Disk: 16 MB - contém dados do Active Directory para cada VM.

À medida que o produto evolui, talvez seja necessário adicionar mais discos para satisfazer determinados casos de uso e consumo de recursos. Por exemplo:

- [O MCS Storage Optimization](#) cria um disco no estilo cache de gravação para cada VM.
- O MCS adicionou a capacidade de usar os clones completos em oposição ao cenário de disco Delta descrito na seção anterior.

Os recursos do hipervisor também podem entrar na equação. Por exemplo:

- O [XenServer IntelliCache](#) cria um disco de leitura no armazenamento local para cada XenServer. Essa opção economiza IOPS em relação à imagem mestre que pode ser mantida no local de armazenamento compartilhado.
- Sobrecarga do hipervisor

Hipervisores diferentes usam arquivos específicos que criam sobrecarga para as VMs. Os hipervisores também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir despesas gerais para:

- [Arquivos de log](#)
  - Arquivos específicos do hipervisor. Por exemplo:
    - \* A VMware adiciona mais arquivos à pasta **VM storage** . Consulte [Práticas recomendadas da VMware](#).
    - \* Calcule seus requisitos totais de tamanho de 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 que consomem 36,1 GB no total.
  - [Instantâneos para XenServer](#); [Instantâneos para VMware](#).
  - Sobrecarga do processo
- Criar um catálogo, adicionar uma máquina e atualizar um catálogo têm implicações de armazenamento exclusivas. Por exemplo:
- [A criação inicial do catálogo](#) exige que uma cópia do disco base seja copiada para cada local de armazenamento.
    - \* Também exige que você crie temporariamente uma VM [Preparation](#) .
  - [Adicionar uma máquina](#) a um catálogo não exige a cópia do disco base em cada local de armazenamento. A criação do catálogo varia de acordo com os recursos selecionados.
  - [Atualizando o catálogo](#) para criar um disco base extra em cada local de armazenamento. As atualizações do catálogo também experimentam um pico de armazenamento temporário em que cada VM no catálogo tem 2 discos Diff por um determinado período de tempo.

*Mais considerações:*

- **Dimensionamento da RAM:** Afeta o tamanho de determinados arquivos e discos do hipervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de instantâneo.
- **Provisionamento fino/espesso:** O armazenamento NFS é preferido devido aos recursos de provisionamento reduzido.

## Otimização do armazenamento do Machine Creation Services (MCS)

Com o recurso de otimização de armazenamento do Machine Creation Services (MCS), conhecido como MCS I/O:

- O contêiner do cache de gravação é *baseado em arquivos*, a mesma funcionalidade encontrada no Citrix Provisioning. Por exemplo, o nome do arquivo de cache de gravação do Citrix Provisioning é `D:\vdiskdif.vhdx` e o nome do arquivo de cache de gravação MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias no diagnóstico incluindo suporte para um arquivo de despejo de falhas do Windows gravado no disco de cache de gravação.
- O MCS I/O retém o cache da tecnologia *na RAM com transbordamento para o disco rígido* para fornecer a solução ideal de cache de gravação em várias camadas. 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** exige as seguintes alterações:

1. O MCS I/O não suporta mais cache somente de 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. Quando 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 esse 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 normalmente está associado ao tamanho da RAM da VM.

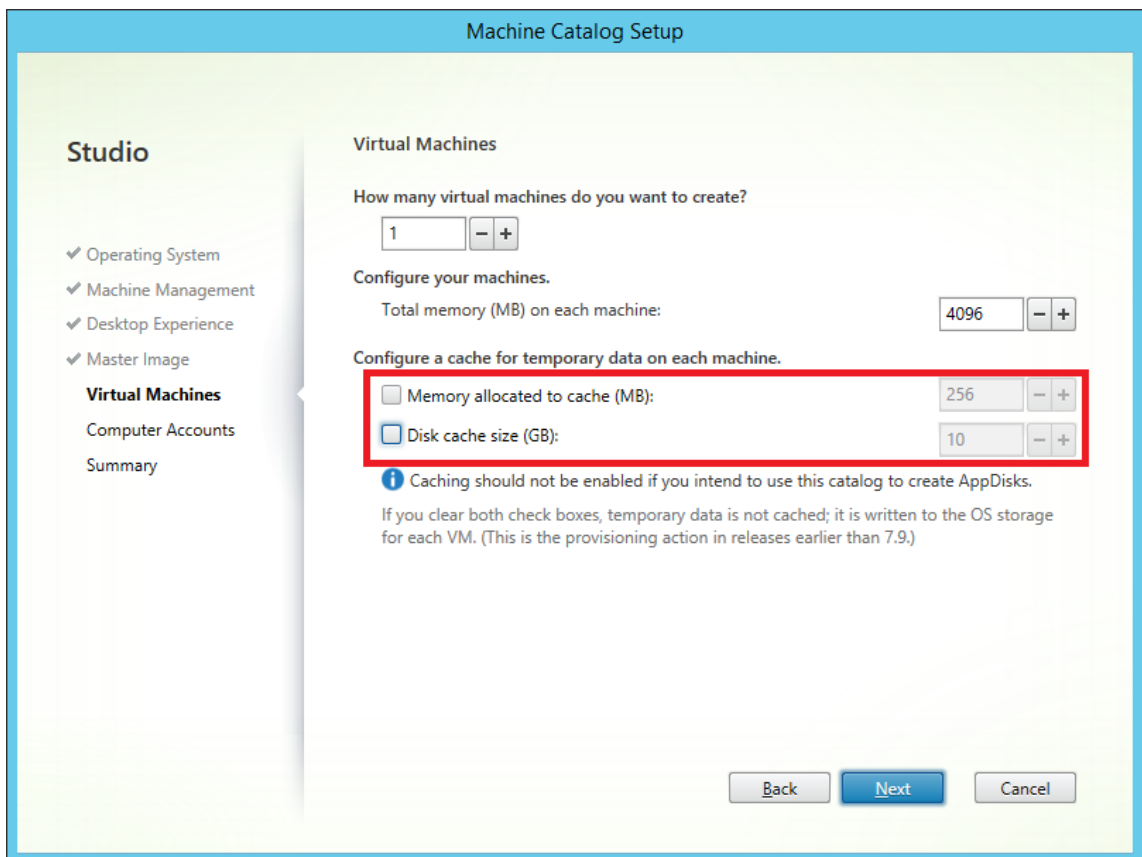
**Habilitando atualizações de otimização de armazenamento do MCS** Para habilitar a funcionalidade de otimização do armazenamento MCS I/O, atualize o Delivery Controller e o VDA para a versão mais recente do Citrix Virtual Apps and Desktops.

### Nota:

Se você atualizar uma implantação existente que tenha o MCS I/O ativado, nenhuma configuração adicional será necessária. A atualização do VDA e do Delivery Controller lida com a atualização de E/S do MCS.

Ao ativar a atualização de otimização de armazenamento do MCS, considere o seguinte:

- Ao criar um catálogo de máquinas, o administrador pode configurar a RAM e o tamanho do disco.



- Atualizar um catálogo de máquinas existente para um novo instantâneo de VM contendo um VDA configurado para a versão 1903 resulta no seguinte comportamento: o novo instantâneo continua usando a configuração de E/S MCS do catálogo existente para RAM e tamanho do disco. O disco bruto existente está formatado.

**Importante:**

A otimização do armazenamento MCS mudou com a versão 1903 do Citrix Virtual Apps and Desktops. Esta versão oferece suporte à tecnologia de cache de gravação baseada em arquivos, proporcionando melhor desempenho e estabilidade. A nova funcionalidade fornecida pelo MCS I/O pode exigir um requisito maior de armazenamento em cache de gravação 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 extra de pagina/arquivo. 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 drive específica ao disco de cache de write-back MCS I/O

Você pode atribuir uma letra de drive específica ao disco de cache de write-back de E/S do MCS. Essa implementação ajuda você a evitar conflitos entre a letra da unidade de qualquer aplicativo que você usa e a letra da unidade do disco de cache de write-back de E/S do MCS. Para atribuir a letra da unidade ao disco de cache de write-back MCS I/O, você pode usar os comandos do PowerShell. Os hipervisores compatíveis são Azure, GCP, VMware, SCVMM e XenServer.

### Nota:

Esse recurso requer o VDA versão 2305 ou posterior.

### Limitações

- Aplicável somente ao sistema operacional Windows
- Letra de unidade aplicável para disco de cache de gravação: E a Z
- Não aplicável quando o disco temporário do Azure é usado como um disco de cache de gravação
- Aplicável somente quando você cria um novo catálogo de máquinas

## Atribuir uma letra de unidade ao disco de cache de gravação

Para atribuir uma letra de drive a um disco de cache de gravação:

1. Abra a janela **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie um grupo 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:

```
1 New-ProvScheme -CleanOnBoot `
2 -HostingUnitName "<name>" `
3 -IdentityPoolName $schemeName `
4 -ProvisioningSchemeName $schemeName `
5 -InitialBatchSizeHint 1 `
6 -UseWriteBackCache -WriteBackCacheDiskSize 127 -
  WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
7 -MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
  resources.resourcegroup\
  MCSIOMasterVm_0sDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
  manageddisk" `
8 -NetworkMapping @{
9   "0"="XDHyp:\\HostingUnits\\name\\virtualprivatecloud.folder\\East
  US.region\\virtualprivatecloud.folder\\abcd-resources.
  resourcegroup\\abcd-resources-vnet.virtualprivatecloud\\
  default.network" }
```



```
10 `
11 -ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.
12 folder\\Standard_D2s_v5.serviceoffering" `
13 -CustomProperties '<CustomProperties xmlns="http://schemas.
14 citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
15 org/2001/XMLSchema-instance">
16 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
17 true" />
18 <Property xsi:type="StringProperty" Name="OsType" Value="Windows
19 " />
20 <Property xsi:type="StringProperty" Name="StorageType" Value="
21 Premium_LRS"/>
22 <Property xsi:type="StringProperty" Name="PersistWBC" Value="
23 false" />
24 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
25 false" />
26 <Property xsi:type="StringProperty" Name="PersistVm" Value="
27 false" />
28 <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
29 Value="Premium_LRS" />
30 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
31 Value="false" />
32 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
33 abcd-group1" />
34 <Property xsi:type="StringProperty" Name="LicenseType" Value="
35 Windows_Client" />
36 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="
37 2" />
38 </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/>.

## Prepare uma imagem mestre

Para obter informações sobre como criar hosts de conexões, 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 clonada, imagem dourada, VM base ou imagem base. Os fornecedores anfitriões 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 necessária para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo da máquina.
- Os catálogos de máquinas do Remote PC Access não usam imagens mestras.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou ferramentas VMware). Se você omitir essa 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 recentes. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros, conforme necessário, como software antivírus ou agentes eletrônicos de distribuição de software. Configure os serviços com configurações apropriadas para os usuários e o tipo de máquina (como atualizar recursos).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda a virtualização de aplicativos. A virtualização reduz os custos ao eliminar a necessidade de atualizar a imagem mestre depois de 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 os pacotes de idiomas e localidades. Durante o provisionamento, quando um snapshot é criado, as VMs provisionadas usam os locais e pacotes de idiomas instalados.

**Importante:**

Se você estiver usando o MCS, não execute o Sysprep em imagens mestras.

Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e instale o sistema operacional, além de todos os service packs e atualizações. Especifique o número de 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 0 do dispositivo. A maioria dos modelos de imagem mestre padrão configura esse local por padrão, mas alguns modelos personalizados talvez não.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, associe a imagem mestre ao domínio em que aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host em que as máquinas são criadas. Se você estiver usando o MCS, não é necessário associar a imagem mestre a um domínio. As máquinas provisionadas são unidas ao domínio especificado

no assistente de criação de catálogo.

5. A Citrix recomenda que você crie e nomeie um instantâneo da sua imagem mestre. Se você especificar uma imagem mestre em vez de um instantâneo ao criar um catálogo, o Web Studio criará um instantâneo. Você não pode nomeá-lo.

## Ativação do licenciamento por volume

O MCS oferece suporte à ativação do licenciamento por volume para automatizar e gerenciar a ativação dos sistemas operacionais Windows e do Microsoft Office. Os três modelos que o MCS suporta para ativação do 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 hospedado em um sistema que fornece outros serviços. Essa funcionalidade é compatível com todas as versões do Windows suportadas pela Citrix. Durante a preparação da imagem, o MCS rearma o Microsoft Windows e o Microsoft Office KMS. Você pode ignorar o rearme executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre o Microsoft Windows KMS Rearm e o Microsoft Office KMS Rearm durante a preparação da imagem, consulte [Machine Creation Services: Image Preparation Overview and Fault-Finding](#). Para obter mais informações sobre a ativação do KMS, consulte [Ativar usando o 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 que você ative máquinas por meio de suas conexões de domínio. As máquinas são ativadas imediatamente quando ingressam no domínio. Essas máquinas permanecem ativadas enquanto permanecerem unidas ao domínio e em contato com ele. Essa funcionalidade é compatível com todas as versões do Windows suportadas pela 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)

O 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. Toda vez que um sistema Windows é ativado, a contagem de ativações diminui. Há duas formas de ativar o sistema:

- Ativação on-line: se o sistema Windows que você deseja ativar tiver acesso à Internet, o sistema ativará automaticamente o Windows ao instalar a chave do produto. Esse processo reduz a contagem de ativações em 1 para a MAK correspondente.
- Ativação offline: Se o sistema Windows não conseguir se conectar à Internet para fazer a ativação on-line, o MCS receberá um ID de confirmação e um ID de instalação do servidor Microsoft para ativar o sistema Windows. Essa forma de ativação é útil para catálogos de máquinas não persistentes.

### Nota:

- O MCS não oferece suporte à ativação do Microsoft Office usando MAK.
- A versão mínima do VDA exigida 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 a ativação MAK](#) para obter as etapas para instalar a chave MAK em um sistema Windows.
- Se você não estiver usando a preparação de imagens:
  1. Adicione o valor DWORD do registro `Manual` em `Computer\ HKEY_LOCAL_MACHINE \ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ SoftwareProtectionP \ Activation`.
  2. Defina o valor como 1.

**Contagens de ativação** Para ver o número de ativações restantes para o MAK Key ou para verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação por Volume (VAMT). Veja [Instalar o VAMT](#).

**Ative o sistema Windows usando o MAK** Para ativar o sistema Windows usando o MAK:

1. Instale a chave do produto na imagem mestre. Essa etapa consome uma contagem de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagens:
  - a) Adicione o valor DWORD do registro `Manual` em `Computer\ HKEY_LOCAL_MACHINE \ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ SoftwareProtectionP \ Activation`.
  - b) Defina o valor como `1`.

Esse método desativa a opção de ativação on-line.

4. Adicione VMs ao catálogo de máquinas.
5. Ligue as VMs.
6. Dependendo da ativação online ou offline, o sistema Windows é ativado.
  - Se a ativação estiver on-line, o sistema Windows será ativado após a instalação da chave do produto.
  - Se a ativação estiver offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. O MCS então recupera um id de confirmação e um id instalado do servidor Microsoft. Esses IDs são usados para ativar o sistema Windows.

**Solução de problemas** Se a VM provisionada não estiver ativada com a chave MAK instalada, execute o comando `Get-ProvVM` ou `Get-ProvScheme` em uma janela do PowerShell.

- O comando `Get-ProvScheme` : veja o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS a partir da imagem mestre mais recente.
- O comando `Get-ProvVM` . Consulte os parâmetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorcode` e `WindowsActivation`.

Você pode verificar o erro e verificar as etapas para resolver o problema.

## Crie um catálogo de máquinas usando o Web Studio

Antes de criar um catálogo:

- Leia 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, o 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 catálogos:

1. Se esse for o primeiro catálogo 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) Entre no Web Studio, selecione **Machine Catalogs** no painel esquerdo e selecione **Create Machine Catalog** na barra de ação.
  - b) Para organizar catálogos usando pastas, crie pastas na pasta padrão **Machine Catalogs** . Para obter mais informações, consulte [Criar uma pasta de catálogo](#).
  - c) Selecione a pasta em que você deseja criar o catálogo e clique em **Create Machine Catalog**. O assistente de criação de catálogo é aberto.

O assistente orienta você nos seguintes itens. As páginas do assistente que você vê são diferentes, dependendo das seleções feitas.

## Sistema operacional

Cada catálogo contém máquinas de apenas um tipo. Selecione um.

- **Sistema operacional multissessão:** Um catálogo de sistemas operacionais com 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 ambas. (Consulte a documentação do Linux VDA para obter detalhes sobre esse sistema operacional.)
- **Sistema operacional de sessão única:** Um catálogo de sistema operacional de sessão única fornece desktops VDI que você pode atribuir a vários usuários diferentes.
- **Acesso remoto ao PC:** Um catálogo do Remote PC Access fornece aos usuários acesso remoto às suas máquinas desktop físicas do escritório. O acesso remoto ao PC não exige uma VPN para fornecer segurança.

## Gerenciamento de máquinas

Essa página não aparece quando você está criando catálogos do Remote PC Access.

A página **Machine Management** indica como as máquinas são gerenciadas e quais ferramentas você usa para implantá-las.

Escolha se as máquinas no catálogo são gerenciadas por meio do Web Studio.

- A energia das máquinas é gerenciada por meio do Web Studio, por exemplo, VMs ou PCs blade. Essa opção está disponível somente se você já configurou uma conexão com um host.
- As máquinas não são gerenciadas por meio do Web Studio, por exemplo, máquinas físicas.

Se você indicou que a energia das máquinas é gerenciada pelo Web Studio, escolha qual ferramenta usar para criar VMs.

- **Tecnologia de provisionamento Citrix**

- **Citrix Machine Creation Services (MCS)** Cria um catálogo de VMs provisionadas e com imagens 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 MCS e imagens usando PVS. Essas VMs funcionam como dispositivos de destino PVS e o servidor PVS pode transmitir uma única imagem de disco compartilhada para elas.

**Nota:**

Essa opção está disponível somente para sites PVS registrados no Citrix Cloud e atualmente está limitada aos recursos do Azure.

- **Outro serviço ou tecnologia** Uma ferramenta que gerencia máquinas que já estão 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)

Essa página aparece somente quando você está criando um catálogo contendo máquinas com sistema operacional de sessão única.

A página **Desktop Experience** determina o que ocorre toda vez que um usuário faz login. Selecione um dos seguintes:

- Os usuários se conectam a uma nova área de trabalho (aleatória) sempre que fazem login.
- Os usuários se conectam à mesma área de trabalho (estática) sempre que fazem login.

## Imagem e perfil da máquina

Essa página aparece somente 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 principal.** Uma imagem que ainda não passou pelo processo de preparação da imagem. O processo de preparação da imagem é iniciado automaticamente quando a criação do catálogo é iniciada.

**Nota:**

- Ao usar o MCS, não execute o Sysprep em imagens mestras.
- Se você especificar uma imagem mestre em vez de um instantâneo, o Web Studio cria um instantâneo, mas você não pode nomeá-lo.

- **Prepared image.** An image that has gone through the image preparation process and can be used for VM creation directly. Opting for prepared images rather than master images during catalog creation ensures faster and more reliable machine catalog creation, along with streamlined image lifecycle management.

```
1 > **Note:**
2 >
3 > - VMs created using prepared images don't support
  hibernation.
4 > - Currently, creating catalogs using prepared images are
  available only in Azure and VMware environments.
```

Para obter mais informações sobre como criar imagens preparadas, consulte [Gerenciamento de imagens \(pré-visualização\)](#).

Ao selecionar uma imagem, você pode adicionar uma nota para a imagem selecionada, se necessário.

Para permitir 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 de 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 instantâneo ou uma VM que não seja compatível com a tecnologia de gerenciamento de máquinas que você selecionou anteriormente no assistente.

2. Para usar uma VM existente como perfil de máquina, selecione **Usar um perfil de máquina**, em seguida, selecione a VM.

**Nota:**

Atualmente, o uso de perfis de máquina é restrito às VMs do Azure, AWS, GCP e VMware.

Para implantações da VMware, ao criar um catálogo de máquinas usando um perfil de máquina, você deve especificar a pasta em que deseja manter as máquinas virtuais.



Para fornecer a localização da pasta da máquina virtual, no assistente de criação do catálogo, vá para a página **Máquinas Virtuais** e vá para **Selecione uma pasta para colocar a seção** das máquinas e selecione a localização da pasta da máquina virtual. Se não for especificado, o sistema considerará a pasta do perfil de máquina selecionado como o local padrão.

3. Selecione o nível funcional mínimo para o catálogo. Para permitir o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada.

## Máquinas

Essa página não aparece quando você está criando catálogos do Remote PC Access.

O título desta página depende do que você selecionou na página **Machine Management : Machines, Virtual Machines** ou **VMs and users**.

### Ao usar o MCS:

- Especifique quantas máquinas virtuais devem ser criadas. Digite **0** (zero) se não quiser criar nenhum. Posteriormente, você pode criar VMs para um catálogo vazio executando **Adicionar máquinas**.
- Escolha a quantidade de memória (em MB) que cada VM tem.
- 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, você pode configurar um cache para ser usado para dados temporários em cada máquina. Consulte Configurar o 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 ou importá-la. Se você especificou máquinas estáticas na página **Desktop Experience**, você pode, opcionalmente, especificar o nome de usuário do Active Directory para cada VM adicionada.

Depois de adicionar ou importar nomes, você pode usar o botão **Remove** 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 talvez não estejam qualificadas para serem adicionadas ao catálogo ou que não possam se registrar em um controlador de entrega. Para obter detalhes, consulte Versões do VDA e níveis funcionais.

### Adicione SIDs ao criar máquinas virtuais

Agora você pode adicionar o parâmetro `AdAccountsID` para identificar de forma exclusiva 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:

```
1 New-ProvVM -ProvisioningSchemeName "name" -ADAccountSid @"SID  
") -RunAsynchronously
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta do AD que não está no pool de identidades do catálogo
- Uma conta do AD que não está no estado disponível

### Modo de cópia de máquina virtual

O modo de cópia que você especifica na página **Machines** determina se o MCS cria clones finos (cópia rápida) ou grossos (cópia completa) a partir da imagem mestre. (Padrão = clones finos)

- Use clones de cópia rápida para um uso mais eficiente do armazenamento e uma criação mais rápida da máquina.
- Use clones de cópia completa para melhorar a recuperação de dados e o suporte à migração, com IOPS potencialmente reduzido após a criação das máquinas.

### Versões e níveis funcionais do VDA

O nível funcional de um catálogo controla quais recursos do produto estão disponíveis para as máquinas no catálogo. O uso dos recursos introduzidos nas novas versões do produto exige um novo VDA. Definir um nível funcional torna todos os recursos introduzidos nessa versão (e posteriormente, se o nível funcional não mudar) disponíveis para as máquinas no catálogo. No entanto, as máquinas desse catálogo com uma versão anterior do VDA não podem se registrar.

Um menu na parte inferior da página **Machines** (ou **Devices**) permite que você selecione 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 os VDAs e os 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 [What's new](#) 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.

As 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. Essas máquinas provavelmente não conseguirão se registrar em um controlador posteriormente. Como alternativa, você pode:

- Remova as máquinas que contêm VDAs mais antigos da lista, atualize seus VDAs e adicione-os novamente ao catálogo.
- Escolha um nível funcional mais baixo que impeça o acesso aos recursos mais recentes do produto.

Uma mensagem também será publicada se uma máquina não tiver sido adicionada ao catálogo porque é do tipo errado de máquina. Os exemplos incluem a tentativa de adicionar um servidor a um catálogo de sistema operacional de sessão única ou a adição de uma máquina de sistema operacional de sessão única originalmente criada para alocação aleatória em 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)** continua sendo a padrão. Esse padrão é válido para todas as implantações agora.

Se você selecionar **1811 (ou mais recente)**, nenhuma versão anterior do VDA nesse catálogo poderá ser registrada em um controlador. No entanto, se o catálogo contiver somente VDAs com suporte na versão 1811 ou versões posteriores, todos eles poderão se registrar. Isso inclui catálogos contendo VDAs configurados para versões posteriores do Citrix Virtual Apps and Desktops, incluindo a versão 1903 e outras versões 19XX antes da versão atual.

### **Configurar o cache para dados temporários**

O armazenamento em cache de dados temporários localmente na VM é opcional. Você pode ativar o uso do cache de dados temporário na máquina ao usar o MCS para gerenciar máquinas agrupadas

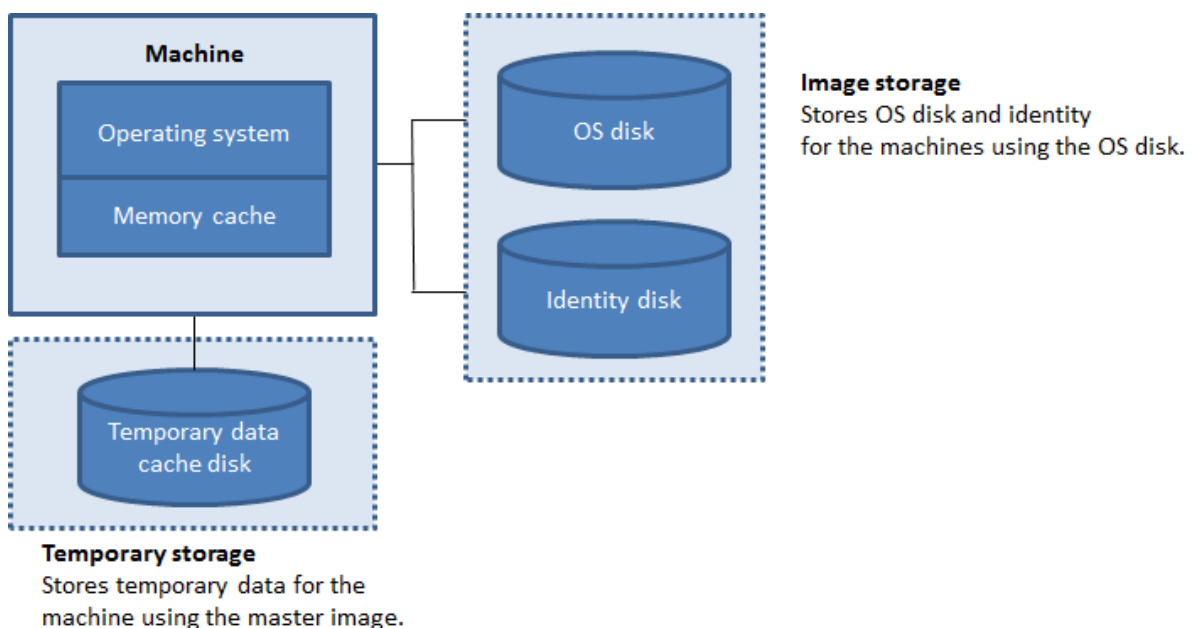
(não dedicadas) em um catálogo. Se o catálogo usar uma conexão que especifique o armazenamento de dados temporários, você poderá ativar e configurar as informações do cache de dados temporários ao criar o catálogo.

**Importante:**

Esse recurso requer um driver de E/S MCS atual. Instalar esse driver é uma opção quando você instala ou atualiza um VDA. Por padrão, esse driver não está instalado.

Você especifica se os dados temporários usam armazenamento compartilhado ou local ao criar a conexão que o catálogo usa. Para obter mais informações, consulte [Conexões e recursos](#). Para configurar um cache para dados temporários em cada máquina, você pode usar as duas opções a seguir: **Memória alocada para cache (MB)** e **Tamanho do cache de disco (GB)**. Por padrão, as duas opções estão desmarcadas. Para ativar a opção Memória alocada para cache (MB), marque a caixa de seleção Tamanho do cache de disco (GB). Se a caixa de seleção **Tamanho do cache de disco** não estiver marcada, a opção **Memória alocada para o cache** ficará acinzentada. Dependendo do tipo de conexão, os valores padrão dessas opções podem ser diferentes. Geralmente, os valores padrão são suficientes para a maioria dos casos. No entanto, leve em consideração o espaço necessário para:

- Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
- Dados do perfil do 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 por qualquer aplicativo que os usuários possam instalar dentro da sessão.



Para configurar um cache para dados temporários em cada máquina, esteja ciente dos três cenários a seguir:

- Se você não marcar a caixa de seleção Tamanho do cache de disco e a caixa de seleção Memória alocada ao cache, os dados temporários não serão armazenados em cache. Ele é gravado diretamente no disco diferente (localizado no armazenamento do sistema operacional) de cada VM. (Essa é a ação de provisionamento na versão 7.8 e anteriores.)
- Se você marcar a caixa de seleção Tamanho do cache de disco e a caixa de seleção Memória alocada ao cache, os dados temporários serão inicialmente gravados no cache de memória. Quando o cache de memória atinge seu limite configurado (o valor da memória alocada ao cache), os dados mais antigos são movidos para o disco de cache de dados temporário.

**Importante:**

- Se o cache do disco ficar sem espaço, a sessão do usuário ficará inutilizável.
- Esse recurso não está disponível ao usar uma conexão de host Nutanix.
- Você não pode alterar os valores do cache em um catálogo de máquinas após a criação da máquina.

**Nota:**

- A configuração do cache de gravação 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 ao cache (MB)** e especificar um tamanho maior que 0 para o cache de memória.
- O cache de memória faz parte da quantidade total de memória em cada máquina. Portanto, se você ativar a opção Memória alocada ao cache, considere aumentar a quantidade total de memória em cada máquina.
- Alterar o tamanho do cache de disco do valor padrão pode afetar o desempenho. O tamanho deve corresponder aos requisitos do usuário e à carga colocada na máquina.

## BOM

Essa página não aparece quando você está criando catálogos do Remote PC Access.

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 usada. Você também pode adicionar ou remover NICs dessa página.

## Contas de máquina

Essa página aparece somente ao criar catálogos do Remote PC Access.

Na página **Machine Accounts**, especifique as contas de máquina ou unidades organizacionais (OUs) do Active Directory a serem adicionadas que correspondam aos 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 exibido na lista:

- Pesquise usando uma correspondência exata.
- Navegue 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 poderá criar essa conexão posteriormente e editar o catálogo da máquina para atualizar as configurações de gerenciamento de energia.

## Identities da máquina

Essa 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 depois de criar o catálogo.

Um fluxo de trabalho geral para definir as configurações nesta página é o seguinte:

1. Selecione uma identidade na lista.
2. Indique se deseja criar contas ou usar contas existentes e o local (domínio) dessas contas.

Você pode selecionar uma das seguintes opções:

- **Active Directory local.** Máquinas pertencentes a uma organização e conectadas com uma conta do Active Directory que pertence a essa organização. Eles existem no local.
- **O Azure Active Directory híbrido ingressou em.** Máquinas pertencentes a uma organização e conectadas com uma conta dos Serviços de Domínio do Active Directory que pertence a essa organização. Eles existem na nuvem e no local. Para obter informações sobre os requisitos, limitações e considerações, consulte [Hybrid Azure Active Directory ingressou em](#).

### Nota:

- Antes de usar a associação híbrida do Azure Active Directory, certifique-se de que seu ambiente do Azure atenda aos pré-requisitos. Veja <https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains>.

- Essa opção exige que a imagem mestre atenda aos pré-requisitos do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid>.

#### Importante:

- Se você selecionar **Active Directory local** ou **Hybrid Azure Active Directory juntado** como o tipo de identidade, cada máquina no catálogo deverá ter uma conta de computador do Active Directory correspondente.

Se você criar contas, deverá ter permissão para criar contas de computador na OU em que as máquinas residem. Cada máquina no catálogo deve ter um nome exclusivo. Especifique o esquema de nomenclatura da conta para as máquinas que você deseja criar. Para obter mais informações, consulte Esquema de nomenclatura de contas de máquina.

#### Nota:

Certifique-se de que os nomes de OU não usem barras (/).

Se você usa contas existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo.csv contendo nomes de contas. O conteúdo do arquivo importado deve usar o formato:

- [Adicionar conta de computador] Adicionar nome da conta do computador.domínio

Certifique-se de que haja 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

Cada máquina em um catálogo deve ter um nome exclusivo. Você deve especificar um esquema de nomenclatura de conta de máquina ao criar um catálogo. Use curingas (marcas de hash) 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 juntar todos os curingas.
- O nome inteiro, incluindo curingas, deve conter pelo menos 2, mas não mais que 15 caracteres. Ele deve incluir pelo menos um caractere não numérico e um # (curinga).

- O nome não deve incluir espaços nem nenhum 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 nome da última conta criada (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 selecionados, os curingas especificados são resolvidos em números sequenciais.

**Nota:**

Se houver somente um curinga (#), os nomes das contas começarão 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 selecionados, os curingas especificados são resolvidos em letras sequenciais.

Por exemplo, um esquema de nomenclatura de PC-Sales-## (com **0-9** selecionado) resulta em contas denominadas 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 serão 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 serão 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 **Insira as 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 **Check name** para verificar se o nome de usuário é válido ou exclusivo. A opção é útil, por exemplo, quando:

- O mesmo nome de usuário existe em vários domínios. Você será solicitado a selecionar o usuário desejado.
- Você não consegue se lembrar do nome do domínio. Você pode inserir o nome de usuário sem especificar o nome do domínio. Se a verificação for aprovada, o nome de domínio será preenchido automaticamente.



**Nota:**

Se o tipo de identidade selecionado em **Machine Identities** for **Hybrid Azure Active Directory juntado a**, as credenciais inseridas devem ter recebido a permissão **Write UserCertificate**.

### Resumo, nome e descrição

Na página **Summary**, revise as configurações que você especificou. Insira um nome e uma descrição para o catálogo. Essas informações aparecem 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 **Machine Catalogs**, o novo catálogo aparece com uma barra de progresso embutida.

Para ver os detalhes do progresso da criação:

1. Passe o mouse sobre o catálogo da máquina.
2. Na dica de ferramenta exibida, clique em **Exibir detalhes**.

Um gráfico de progresso passo a passo aparece onde você pode ver o seguinte:

- História das etapas
- Progresso e tempo de execução da etapa atual
- Etapas restantes

### Sincronização de horário do MCS

A sincronização de tempo é determinada pela imagem mestre e pelo tipo de identidade da máquina associada ao catálogo. Você obtém o seguinte método de sincronização de horário de acordo com a imagem mestre e o catálogo:

---

<b>Imagem principal</b>	<b>Catálogo</b>	<b>Método de sincronização de tempo resultante</b>
NDJ	AD ou Azure AD híbrido	Por padrão, NT5DS. Você pode desativar o MCS de alterar a configuração de sincronização de horário usando as configurações do registro na imagem mestre.

<b>Imagem principal</b>	<b>Catálogo</b>	<b>Método de sincronização de tempo resultante</b>
NDJ	NDJ ou Azure AD	Igual à configuração original de sincronização de hora
AD ou Azure AD híbrido	AD ou Azure AD híbrido	Igual à configuração original de sincronização de hora
Azure AD	Azure AD	Igual à configuração original de sincronização de hora

**Nota:**

A sincronização de horário original é controlada pela seguinte configuração do registro e não pode ser alterada:

- Computador\ HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ W32Time\ Config

Valor: MaxAllowedPhaseOffset, MaxNegPhaseCorrection e MaxPosPhaseCorrection

- Computador\ HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ W32Time\ Parameters

Valor: Tipo

Para impedir que o MCS altere a configuração de sincronização de horário, defina o valor da seguinte configuração do 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 hora.
- 1: Mantém a configuração original de sincronização de hora e os valores dos parâmetros padrão.

**Consideração importante sobre a configuração de propriedades personalizadas**

As propriedades personalizadas devem ser definidas corretamente em `New-ProvScheme` e `Set-ProvScheme` nos ambientes GCP e Azure. Se você especificar uma propriedade ou propriedades personalizadas não existentes, receberá a seguinte mensagem de erro e os comandos falharão na execução.

- No Azure: Propriedade inválida encontrada: <invalid property>. Certifique-se de que o parâmetro CustomProperties ofereça suporte à propriedade.
- No GCP: Propriedade inválida encontrada: <invalid property>. Certifique-se de que o valor fornecido para a propriedade seja suportado no hipervisor.

## Solucionar problemas

### Importante:

Depois de criar o catálogo de máquinas usando o Web Studio, você não pode mais usar o comando `Get-ProvTask` do PowerShell para recuperar as tarefas associadas à criação do catálogo de máquinas. Essa restrição é resultado da exclusão dessas tarefas pelo Web Studio após a criação do catálogo de máquinas, independentemente de o catálogo ter sido criado com êxito.

A Citrix recomenda coletar registros para ajudar a equipe de suporte a fornecer soluções. Ao usar o Citrix Provisioning, use o procedimento a seguir 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 do PowerShell: `Set-ProvServiceConfiguration -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 e, nesse momento, ela relata a falha.
7. Execute o seguinte comando do PowerShell para reativar o desligamento automático das máquinas de preparação de imagens: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

## Problemas de preparação de imagens

Como o MCS cria muitas máquinas a partir de uma única imagem, algumas etapas são executadas para garantir que todas as máquinas sejam exclusivas e licenciadas corretamente. A preparação da imagem faz parte do processo de criação do catálogo. Essa preparação garante que todas as máquinas provisionadas tenham endereços IP exclusivos e se anunciem corretamente no servidor KMS como

instâncias exclusivas. No MCS, a preparação da imagem ocorre após a seleção do instantâneo da imagem mestre. Uma cópia é feita para permitir que o catálogo se isole da máquina selecionada. Uma VM de preparação é criada, com base na VM original, mas com a conexão de rede desconectada. Desconectar a conexão de rede evita conflitos com outras máquinas, ao mesmo tempo em que garante que a VM preparada seja conectada somente ao disco recém-copiado.

Um pequeno disco de instrução \*\*, contendo as etapas necessárias para executar a preparação da imagem, é anexado à VM preparada. Essa VM preparada é iniciada e o processo de preparação da imagem começa. A preparação da imagem inclui os seguintes processos:

- Ative o DHCP. A ativação do DHCP garante que as máquinas provisionadas não causem conflitos de endereço IP. O DHCP está ativado em todas as placas de rede.
- Microsoft Windows KMS Rearm. O rearmamento do KMS garante que o Microsoft Windows seja licenciado corretamente. O sistema operacional rearmado é invocado para que seja relatado corretamente como uma nova instância ao servidor de licenças KMS.
- Microsoft Office KMS Rearm (se o Microsoft Office estiver instalado). Rearmar o Microsoft Office garante que qualquer versão do Microsoft Office (2010+) seja registrada corretamente em seu servidor KMS. Depois que o Microsoft Office rearm é invocado, ele se reporta como uma nova instância ao servidor de licenças KMS.

**Dica:**

Quando o processo de preparação da imagem é concluído, o disco de instruções é obtido do hipervisor. O hipervisor contém as informações coletadas no processo de preparação da imagem.

Há vários motivos pelos quais o estágio de preparação da imagem pode falhar. É exibida uma mensagem de falha semelhante à seguinte: Falha na rearmação do escritório de preparação da imagem.

Essas falhas são discutidas nas seções a seguir.

**Habilitar DHCP** Esses casos de falha são causados por placas de rede que não suportam endereços IP estáticos. Por exemplo, versões anteriores das placas de rede Dell SonicWALL. A operação falhou porque uma placa SonicWALL é uma placa de rede de firewall, portanto, configurar a placa como DHCP não faz sentido, pois ela suporta apenas DHCP. Isso foi corrigido em versões posteriores do Citrix Virtual Apps and Desktops. No entanto, se for visto em outros tipos de placas de rede, ele deverá ser reportado à Citrix por meio dos fóruns ou de seu contato de suporte.

**Nota:**

Essa configuração do PowerShell nos exemplos a seguir é aplicada ao site Citrix Virtual Apps

and Desktops, portanto, afeta todos os novos catálogos e atualizações de imagem realizadas nos catálogos existentes.

Se você encontrar esse problema com outras placas de rede, poderá resolvê-lo executando um comando do PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcLuded_Steps  
-Value EnableDHCP
```

**Microsoft Office Rearm** Existem várias falhas de rearmamento do KMS que podem ocorrer durante o estágio de rearmamento do Microsoft Office. As principais falhas são:

- Alguns tempos de execução do Microsoft Office, por exemplo, **Access Runtime**, podem invocar o rearme do Office, fazendo com que ele falhe.
- Uma versão KMS do Microsoft Office não está instalada.
- A contagem de rebraços foi excedida.

Se o erro for um falso positivo, você poderá resolvê-lo executando o seguinte comando do PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcLuded_Steps  
-Value OfficeRearm
```

**Rearme do Microsoft Windows** Várias falhas de KMS podem ocorrer durante o estágio de rearme do Microsoft Windows. As principais falhas são:

- A versão do Windows instalada não é ativada usando o KMS. Por exemplo, ele usa uma chave de ativação múltipla (MAK).
- A contagem de rebraços foi excedida.

Se a versão do Microsoft Windows estiver licenciada corretamente, você poderá limpar o rearmamento do sistema operacional executando o seguinte comando do PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcLuded_Steps  
-Value OsRearm
```

**Instâncias de falha total** A máquina de preparação de imagens não está conectada à rede por design, isso significa que, às vezes, o estágio de preparação da imagem só pode relatar uma falha completa. Um exemplo desse tipo de falha é semelhante a: Falha na preparação da imagem mestre da VM. Verifique se a imagem selecionada tem um sistema operacional compatível (por exemplo, Windows 7) e a versão correta do VDA (7.0 ou posterior) instalada.

Os principais motivos para uma falha completa são:

**O Virtual Delivery Agent (VDA) não está instalado ou o VDA versão 5.x está instalado** Se o VDA 7.x não estiver instalado na imagem mestre, a preparação da imagem expirará após 20 minutos e relatará o erro acima. Isso ocorre porque não há software instalado na imagem mestre para executar o estágio de preparação da imagem e relatar sucesso ou falha. Para resolver isso, certifique-se de que o VDA (versão mínima 7) esteja instalado no instantâneo selecionado como imagem mestre.

**Política do DISKPART SAN** Todo o estágio de preparação da imagem pode falhar devido à política `DISKPART SAN` definida na imagem mestre. Se não estiver configurado para colocar o disco de instruções de preparação de imagem on-line, a máquina será desligada e a preparação da imagem relatará uma falha após 20 minutos. Para verificar isso na imagem mestre, execute os seguintes comandos:

```
1 C:\> Diskpart.exe
2 DISKPART> San
```

Esse comando retorna a política atual. Se não for *Online All*, altere-o executando o seguinte comando:

```
DISKPART> San policy=OnlineAll
```

Desligue a imagem mestre, crie um instantâneo dessa máquina e use-o como imagem básica do MCS.

**Se a preparação da imagem falhar por outro motivo** Se a preparação da imagem estiver falhando e não houver um motivo claro para a falha, você poderá ignorar o processo de preparação da imagem ao criar um catálogo MCS. No entanto, ignorar esse processo pode causar problemas com o licenciamento e a rede KMS (DHCP) em seu site. Use o seguinte comando do PowerShell:

```
1 Set-ProvServiceConfigurationData -Name
   ImageManagementPrep_DoImagePreparation -Value $false
```

Sempre que possível, colete registros para a equipe de suporte da Citrix. Relate o problema à Citrix por meio dos fóruns ou por meio do seu contato de suporte. Para coletar registros:

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. No Delivery Controller, inicie o PowerShell, com os snap-ins do Citrix PowerShell carregados, e execute `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Crie um catálogo com base nesse instantâneo.
4. Quando a VM de preparação for criada no hipervisor, faça login e extraia da raiz de C::

```
1 Image-prep.log
2 PvsVmAgentLog.txt
```

Desligue a máquina. Neste ponto, ele relata a falha.

Execute a partir do seguinte comando do PowerShell para reativar o desligamento automático das máquinas de preparação de imagens:

```
Remove-provServiceConfigurationData - Nome ImageManagementPrep_NoAutoShutdown
```

## Para onde ir a seguir

Para obter informações sobre a criação de catálogos específicos de serviços em nuvem, consulte:

- [Crie um catálogo da AWS](#)
- [Crie um catálogo do XenServer](#)
- [Crie um catálogo do Google Cloud Platform](#)
- [Crie um catálogo do Microsoft Azure](#)
- [Criar um catálogo do Microsoft System Center Virtual Machine Manager](#)
- [Crie um catálogo da Nutanix](#)
- [Crie um catálogo da VMware](#)

Se esse for o primeiro catálogo criado, o Web Studio orienta você 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. Essa implementação oferece as seguintes vantagens:

- Um único console unificado para gerenciar os catálogos MCS e Citrix Provisioning.
- Tenha novos recursos para os catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Atualmente, esse recurso está disponível somente para cargas de trabalho do Azure e do VMware. No entanto, em ambientes VMware, atualmente você pode criar os catálogos usando somente comandos do PowerShell. Para obter mais informações, consulte [Criar catálogos do Citrix Provisioning no Citrix Studio](#).

## Mais informações

- [Crie e gerencie conexões e recursos](#)
- [Crie catálogos de diferentes tipos de junção](#)
- [Gerenciar catálogos de máquinas](#)

## Crie um catálogo da AWS

November 8, 2024

[Criar catálogos de máquinas](#) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização da AWS.

### Observação:

Antes de criar um catálogo da AWS, você precisa concluir a criação de uma conexão com a AWS. Consulte [Conexão com a AWS](#).

### Limitação

Do Citrix Virtual Apps and Desktops 2203 LTSR e versões posteriores, o plug-in MCS AWS faz uma chamada de API da AWS `DescribeInstanceTypes` e, se isso for bem-sucedido, o MCS usará o nome do inventário criado a partir da resposta da API.

Portanto, ao atualizar do CVAD 1912 para 2203 ou posterior, desative a permissão `DefineInstanceType` na AWS e atualize o catálogo existente usando o comando `Set-ProvScheme` para corresponder ao esquema de nomenclatura da AWS. Em seguida, adicione as permissões `DescribeInstanceType` depois que a atualização do catálogo for concluída e a oferta de serviço 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. Essa VM de preparação está desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. Esse grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `citrix.xendesktop.IsolationGroup-GUID`, onde o GUID é gerado aleatoriamente.

### Configurar a localização da AWS

A AWS oferece as seguintes opções de localização:

- Localização compartilhada (o tipo padrão): várias instâncias do Amazon EC2 de clientes diferentes podem residir no mesmo equipamento de hardware físico.
- Localização dedicada: suas instâncias do EC2 são executadas somente no hardware com as outras instâncias que você implantou. Outros clientes não usam o mesmo equipamento de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando o PowerShell.



## Configurar a localização de host dedicada da AWS usando o PowerShell

Você pode criar um catálogo de máquinas com a localização de host definida por meio do PowerShell.

Um host dedicado [EC2] da Amazon é um servidor físico com capacidade de instância [EC2] totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM.

Os hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado dos tipos de instância C4 Large é limitado à execução de 16 instâncias. Consulte o [site da AWS](#) para obter mais informações.

Os requisitos de provisionamento para os hosts da AWS incluem:

- Uma imagem (AMI) importada da BYOL (traga sua própria licença). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para atender às solicitações de provisionamento.
- Ativar o **posicionamento automático**.

Para provisionar um host dedicado na AWS usando o PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro `TenancyType` definido como `Host`.

Consulte a [Documentação do Citrix Developer](#) para obter mais informações.

## Capture propriedades da máquina a partir 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/de ouro do catálogo. A partir dessa AMI, o MCS usa um instantâneo do disco. Em versões anteriores, se você quisesse funções ou marcações em suas máquinas, usaria o console da AWS para defini-las individualmente. Essa funcionalidade é ativada por padrão.

### Dica:

Para usar a captura de propriedade da instância da AWS, você deve ter uma VM associada à AMI.

Para melhorar esse processo, o **MCS lê** as propriedades da instância a partir da qual a AMI foi obtida e aplica a função de Identity Access Management (IAM) e as marcas da máquina às máquinas provisionadas de um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo localiza a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são armazenadas em um Launch Template da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturada.

As propriedades capturadas incluem:

- Funções de IAM –aplicadas a instâncias provisionadas.
- Marcações –aplicadas a instâncias provisionadas, seus discos e NICs. Essas marcações são aplicadas a recursos temporários da Citrix, incluindo: objetos e bucket S3, e AMIs, instantâneos e modelos de execução.

**Dica:**

A marcação de recursos temporários da Citrix é opcional e configurável usando a propriedade personalizada `AWSOperationalResourceTagging`.

### 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"  
...<parâmetros provscheme padrão
```

Consulte a [Documentação do Citrix Developer](#) para obter mais informações.

**Observação:**

O `AWSCaptureInstanceProperties` está obsoleto. Em vez disso, recomendamos usar perfis de máquina para especificar as propriedades da máquina para VMs.

### Capture as propriedades da máquina a partir dos perfis da máquina

Ao criar um catálogo para provisionar máquinas da AWS usando o MCS, você pode usar um perfil de máquina para predefinir determinadas configurações de propriedades da máquina.

Para isso, siga estes passos:

1. Armazene os perfis da máquina na mesma zona de disponibilidade dos recursos em que você está criando esse catálogo.
2. Na página **Machine Template** do assistente de criação de catálogo, selecione **Use a machine profile**. Perfis de máquina localizados na mesma zona disponível dos recursos que você selecionou são mostrados.
3. Selecione um perfil de máquina conforme necessário.

**Observação:**

Você pode usar um perfil de máquina ou uma AMI para capturar as propriedades da máquina. No Web Studio, quando você seleciona **Usar um perfil de máquina**, a opção **Aplicar propriedades do modelo de máquina às máquinas virtuais** fica automaticamente oculta.

## Marcar um recurso operacional AWS

Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode controlar se as propriedades de função e marcação com tag do IAM devem ser aplicadas a essas máquinas. Você também pode controlar se as marcas de máquina devem ser aplicadas aos recursos operacionais.

Uma Amazon Machine Image (AMI) representa um tipo de dispositivo virtual usado para criar uma máquina virtual dentro do ambiente de nuvem Amazon Cloud, comumente chamado de EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Quando cria um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem de ouro do catálogo.

### Importante:

A criação de catálogos por meio da captura de uma propriedade de instância e um modelo de execução é necessária para usar a marcação de recursos operacionais.

Para criar um catálogo da AWS, você deve primeiro criar uma AMI para a instância que você quer que seja a imagem de ouro. O MCS lê as marcas dessa instância e as incorpora ao modelo de execução. As marcas do modelo de execução são então aplicadas a todos os recursos da Citrix criados no seu ambiente da AWS, incluindo:

- Máquinas virtuais
- Discos VM
- Interfaces de rede VM
- Buckets do S3
- Objetos do S3
- Modelos de execução
- AMIs

## Marcar um recurso operacional

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell no host DDC.
2. Execute o comando `asnp citrix` para carregar módulos PowerShell específicos da Citrix.

Para marcar um recurso para uma VM provisionada, use a nova propriedade personalizada `AWSOperationalResourceTagging`. A sintaxe dessa propriedade é:

```
Novo-ProvScheme - CustomProperties "AwsCaptureInstanceProperties, verdadeiro; AwsOperationalResourcesTagging, verdadeiro"...<standard provscheme parameters>
```

## O que fazer a seguir

- Se este for o primeiro catálogo criado, o Web Studio orientará você 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 da AWS](#)

## Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do sistema operacional) especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer fonte de perfil de máquina (instância de VM da AWS ou versão do modelo de lançamento da AWS). Esse 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 **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando do 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 do modelo de lançamento) tiver duas interfaces de rede (eni-1 e eni-2) e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, a VM obterá as tags das duas interfaces de rede.

## Criar um catálogo usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, agora você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou iniciar a versão do modelo e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume do EBS, tipo de instância, otimização do EBS e outras configurações compatíveis da AWS. Ao editar o catálogo, o perfil de máquina das máquinas provisionadas pode ser alterado fornecendo uma VM ou um modelo de inicialização diferente.

### Observação:

As propriedades de volume do EBS são derivadas somente de um perfil de máquina.

## Considerações importantes

Considerações importantes ao criar um catálogo de máquinas MCS:

- Se você adicionar parâmetros de propriedade de hardware da máquina nos comandos `New-ProvScheme` e `Set-ProvScheme`, os valores fornecidos nos parâmetros substituirão os valores no perfil da máquina.
- Se você definir `AWSCaptureInstanceProperties` como `true` e não definir a propriedade `machineProfile`, somente as funções e tags do IAM serão capturadas.
- Você não pode definir `AWSCaptureInstanceProperties` e `MachineProfile` ao mesmo tempo.

Observação:

O `AWSCaptureInstanceProperties` está obsoleto.

- Você deve fornecer explicitamente os valores das seguintes propriedades:
  - `TenancyType`
  - Grupo de Segurança
  - NIC ou rede virtual
- Você pode ativar `AWSOperationalResourceTagging` somente se ativar `AWSCaptureInstancePro` ou especificar um perfil de máquina.

Considerações importantes após criar um catálogo de máquinas MCS:

- Somente as novas VMs adicionadas ao catálogo são afetadas pela alteração.
- Você não pode alterar de um catálogo baseado em perfil de máquina para um catálogo não baseado em perfil de máquina.

## Crie 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 do PowerShell específicos à Citrix.
3. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo,

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -  
Domain abcdf -NamingSchemeType Numérico
```

4. Execute o comando `New-ProvScheme`. Por exemplo:

```

1 Novo-ProvScheme -Nome do esquema de provisionamento demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -Perfil da máquina 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0
xxxxxxx).vm'

```

5. Conclua a criação do catálogo. Para obter mais informações, consulte [Citrix PowerShell SDK](#).

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina:

1. Execute o comando `Set-provScheme`. Por exemplo,

```

1 Definir-ProvScheme `
2 -ProvisioningSchemeUid "<ID" `
3 -MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
availabilityzone\citrix-cvad-machineprofile-instance (i-0
xxxxxxx).vm"

```

### Criar um catálogo com a versão do modelo de execução

Você pode criar um catálogo de máquinas MCS com uma versão do modelo de execução como entrada do perfil da máquina. Você também pode atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução e de uma versão de modelo de execução para uma VM.

No console da AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de execução juntamente com o número da versão. Quando você especifica a versão do modelo de execução como uma entrada de perfil de máquina ao criar ou atualizar um catálogo de máquinas, as propriedades dessa versão do modelo de execução são copiadas para as VMs VDA provisionadas.

As propriedades a seguir podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidos nos comandos `New-ProvScheme` ou `Set-ProvScheme`, eles terão precedência sobre os valores de perfil de máquina dessas propriedades.

- Oferta de serviço
- Redes
- Grupos de segurança
- Tipo de localização

**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 execução como uma entrada de perfil da máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos à Citrix.
3. Obtenha a lista de versões de modelo de execução de um modelo de execução. Por exemplo:

```
1 XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxx).launchtemplate>
ls | Seleccione Caminho Completo
```

4. Crie um pool de identidades se não tiver sido criado. Por exemplo:

```
1 Novo-AcctIdentityPool `
2 -IdentityPoolName "abc11" `
3 -NamingScheme "abc1-##" `
4 -NamingSchemeType Numérico `
5 -Domínio "citrix-xxxxxx.local" `
6 -ZoneUid "xxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão do modelo de execução como entrada do perfil da máquina. Por exemplo:

```
1 Novo-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxxxx" `
4 -IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxx-d-ue1a\apollo-non-
persistent-vda-win2022 (ami-0axxxxxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxx-d-ue1a\machineprofiletest
(lt-01xxxx).launchtemplate\lt-01xxxx
launchtemplateversion"
```

Você também pode substituir parâmetros como oferta de serviço, grupos de segurança, localização e redes. Por exemplo:

```
1 Novo-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxxxx" `
4 -IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxx-d-ue1a\apollo-non-
persistent-vda-win2022 (ami-0axxxxxxxxxxxxx).template" `
6 -CleanOnBoot `
```

```

7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
8 -ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Instância
  grande.serviceoffering"

```

6. Registre o esquema de provisionamento como um catálogo de agente. Por exemplo:

```

1 New-BrokerCatalog -Nome "MPLT1" `
2 -AllocationType Random `
3 -Description "Catálogo de perfil de máquina" `
4 -ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxx `
5 -ProvisioningType Mcs `
6 -SessionSupport MultiSession `
7 -PersistUserChanges Descartar

```

7. Conclua a criação do catálogo. Para obter mais informações, consulte [Citrix PowerShell SDK](#)

Você também pode atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução e de uma versão de modelo de execução para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfis de máquina de uma VM para uma versão de modelo de execução:

```

1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx (1).
  launchtemplateversion"

```

- Para atualizar a entrada de um catálogo de perfis de máquina de uma versão do modelo de execução para uma VM:

```

1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
  availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
  xxxxxxxx).vm"

```

## Filtrar instâncias de VM

Uma instância do AWS EC2 que você usa como uma VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criada e funcione corretamente. Para listar as instâncias do AWS EC2 que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode navegar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

### Paginação:



**Get-HypInventoryItem** suporta dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens devem ser ignorados do início absoluto (ou final absoluto) da lista no hipervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:
  - `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.
  - `-ContinuationToken`: devolve os itens imediatamente após (ou antes, se `forwardDirection` for **false**), mas sem incluir o item fornecido no `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem `TotalItemsCount` e `TotalFilteredItemsCount`:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -Modelo ResourceType
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType modelo -MaxRecords 10 | seleccione Nome
```

- Para retornar uma matriz de registros que terminam com o nome mais alto:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType template -ForwardDirection $False -MaxRecords 10
  | seleccione Nome
```

- Para retornar uma matriz de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -Modelo ResourceType -ContinuationToken "ami-07xxxxxxxxxx" -
  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 `Obter`. Por exemplo:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType modelo -MaxRecords 100 -ContainName 'apollo' |
   seleccione Nome
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Obter`. Por exemplo:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -MaxRecords 100 -Tags '{
2 "opex owner": "Não marcado" }
3 ' | seleccione Nome
```

#### Observação:

Dois valores de tag são suportados. O valor da tag **Not Tagged** corresponde a itens que não têm a tag especificada em sua lista de tags. **Todos os valores** tag value correspondem aos itens que têm a tag, independentemente do valor da tag. Caso contrário, a correspondência só acontece se o item tiver a tag e o valor for igual ao fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Obter`. Por exemplo:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType modelo -Id ami-xxxxxxxxxxxxxxxx
```

#### Filtragem pelo parâmetro `AdditionalData`:

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em `AdditionalData`. Por exemplo:

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).Dados
   Adicionais
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs estão incluídas em um campo `additionalData` chamado **Warning**. Por exemplo:

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-
   -015xxxxxxxxxx" -Warn $true).Dados Adicionais
```

#### Mais informações

- [Crie e gerencie conexões e recursos](#)

- [Conexão com a AWS](#)
- [Criar catálogos de máquinas](#)

## Criar um catálogo do Microsoft Azure

November 7, 2024

### Observação:

Desde julho de 2023, a Microsoft renomeou o Azure Active Directory (Azure AD) para Microsoft Entra ID. Neste documento, qualquer referência ao Azure Active Directory, Azure AD ou AAD agora se refere ao Microsoft Entra ID.

[Criar catálogos de máquinas](#) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

### Observação:

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 por meio de uma imagem do Azure Resource Manager no Web Studio](#)
- [Criar um catálogo de máquinas usando o PowerShell](#)

### Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

Uma imagem pode ser um disco, um instantâneo ou a versão imagem de uma definição de imagem na Galeria de Computação do Azure que é usada para criar as VMs em um catálogo de máquinas. Antes de criar o catálogo de máquinas, crie uma imagem no Azure Resource Manager. Para obter informações gerais sobre imagens, consulte [Criar catálogos de máquinas](#).

### Observação:

O suporte ao uso de uma imagem mestre de uma região diferente daquela configurada na

conexão do host está obsoleto. Use a Galeria de Computação do Azure para replicar a imagem mestre na 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 licenças. Essa VM temporária é chamada de VM de preparação. O nome desta VM de preparação segue o formato **Preparati-84x9n**, onde os últimos cinco caracteres são gerados aleatoriamente para evitar duplicação. A convenção de nomenclatura para esta 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 o 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 **Create machine catalogs** e **Machine Management** não contêm informações específicas do Azure. Siga as instruções no artigo [Criar catálogos de máquinas](#).
- Na página **Imagem**, escolha uma imagem que você deseja usar como modelo para criar máquinas nesse 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:

1. (Aplicável somente às conexões configuradas com imagens compartilhadas com ou entre locatários) Selecione a assinatura em que a imagem reside.
2. Selecione um grupo de recursos.
3. Navegue até o Azure VHD, a Galeria de Computação do Azure ou a versão de imagem do Azure. 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 conectado a uma VM, deverá desligá-la 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 Galeria de Computação do Azure compartilhada com essa assinatura. Nessas assinaturas, somente galerias compartilhadas são exibidas. Para obter informações sobre como con-

figurar assinaturas compartilhadas, consulte [Compartilhar imagens com um locatário \(entre assinaturas\)](#) e [Compartilhar imagens entre locatários](#).

- O uso de um perfil de máquina com início confiável como **Security Type** é obrigatório quando você seleciona uma imagem ou instantâneo com início confiável habilitado. Em seguida, você pode ativar ou desativar o SecureBoot e o vTPM especificando seus valores no perfil de máquina. O Trusted Launch não é compatível com a Galeria de Imagens Compartilhadas. Para obter informações sobre o lançamento confiável do Azure, consulte <https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch>.
- Você pode criar um esquema de provisionamento usando o disco de SO efêmero no Windows com início confiável. Ao selecionar uma imagem com início confiável, você deve selecionar um perfil de máquina com início confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando o disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
- Quando a replicação de imagem está em andamento, você pode prosseguir e selecionar a imagem como a imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode demorar mais para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída dentro de uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo não se completará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.
- Quando você seleciona uma imagem mestre para catálogos de máquinas no Azure, o MCS identifica o tipo de SO com base na imagem mestre e no perfil de máquina selecionados. Se o MCS não conseguir identificá-lo, selecione o tipo de SO que corresponde à imagem mestre.
- Você pode provisionar um catálogo de VM Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem antiga que não tenha informações de geração é uma imagem Gen1.

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 o Azure Active Directory)** é marcada automaticamente. Clique em **Select a machine profile** para navegar até a especificação de uma VM ou modelo ARM a partir de uma lista de grupos

de recursos. As VMs no catálogo podem herdar configurações do perfil de máquina selecionado.

Valide a especificação do modelo ARM para garantir que possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Há duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Next**. Mensagens de erro são exibidas se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  - \* `Teste-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - \* `Teste-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Exemplos de configurações que as máquinas virtuais podem herdar de um perfil de máquina incluem:

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

Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Machine Catalogs**, selecione o catálogo para exibir seus detalhes no painel inferior. Em seguida, clique na guia **Template Properties** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **View all**.

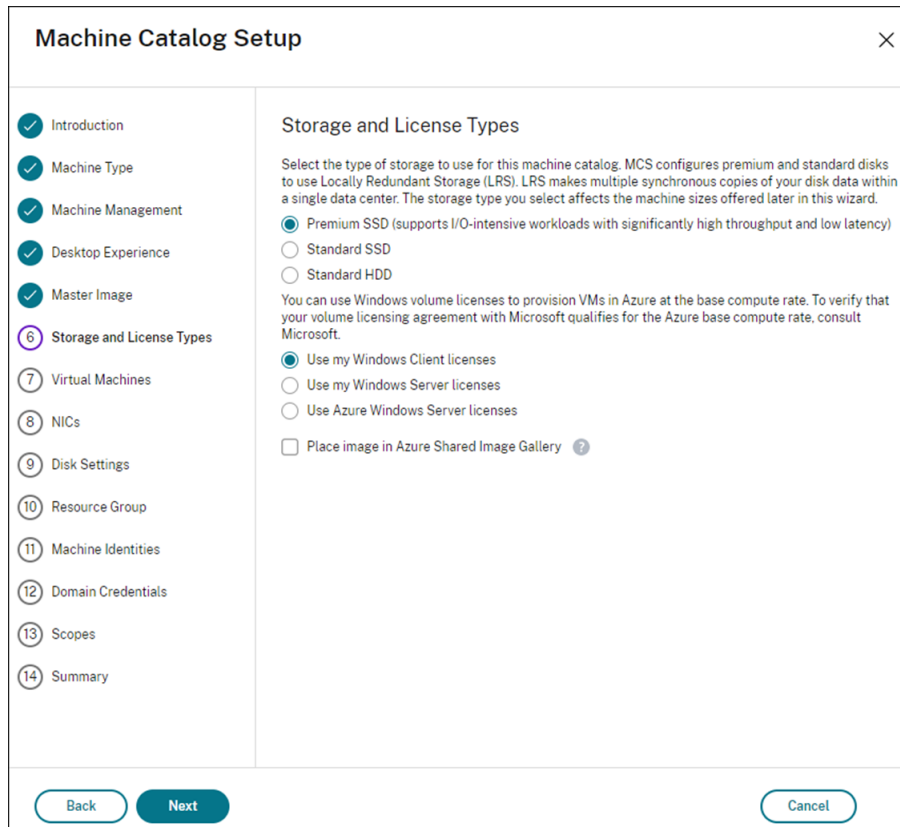
Se desejar que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts dedicados** e selecione um grupo de hosts na lista. Um grupo de hosts é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço que fornece servidores físicos que hospedam uma ou mais máquinas virtuais. Seu servidor é dedicado à sua assinatura do Azure, não compartilhado com outros assinantes. Quando você usa um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em execução nesse host. Esse recurso é adequado para cenários em que você precisa atender aos requisitos regulamentares ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

**Importante:**

- Somente são exibidos os grupos de hosts que têm o posicionamento automático do Azure habilitado.

- O uso de um grupo de hosts altera a página **Virtual Machines** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são mostrados nessa página. Além disso, as zonas de disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Storage and License Types** só aparece quando você usa uma imagem do Azure Resource Manager.



Os seguintes tipos de armazenamento podem ser usados no catálogo de máquinas:

- **Premium SSD.** Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência adequada para VMs com cargas de trabalho intensivas de E/S.
- **Standard SSD.** Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
- **Standard HDD.** Oferece uma opção de armazenamento em disco confiável e de baixo custo adequada para VMs que executam cargas de trabalho insensíveis à latência.
- **Azure ephemeral OS disk.** Oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Como alternativa, você pode usar o PowerShell para criar máquinas que usam discos de SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Leve em consideração os seguintes aspectos ao usar um disco de SO efêmero:

- \* O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.
- \* Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
- \* Não é possível usar a opção **Retain VM and system disk during power cycles** 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 padrão para usar o Armazenamento com Redundância Local (LRS). O LRS faz várias cópias síncronas dos dados do disco em um único data center. Os discos de SO efêmeros do Azure usam o disco local das VMs para armazenar o sistema operacional. Para obter detalhes sobre os tipos de armazenamento do Azure e a replicação de armazenamento, consulte o seguinte:

- <https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/>
- <https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/>
- <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/>

Selecione se deseja usar as licenças existentes do Windows ou do Linux.

- Licenças do Windows: o uso de licenças do Windows junto com imagens do Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs do Windows no Azure a um custo reduzido. Existem dois tipos de licenças:
  - \* **Windows Server license.** Possibilita que você use suas licenças do Windows Server ou do Azure Windows Server, permitindo que você use os Benefícios Híbridos do Azure. Para obter detalhes, consulte <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>. O Azure Hybrid Benefit reduz o custo de execução de VMs no Azure para a taxa de computação básica, dispensando o custo de licenças extras do Windows Server da galeria do Azure.
  - \* **Windows Client license.** Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e do Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de [acesso para cliente e licenças de gerenciamento](#).



Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando do PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows\_Server**. Mais instruções estão disponíveis em <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>.
- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows\_Client**. Mais instruções estão disponíveis em <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>.

Como alternativa, você pode usar o SDK do PowerShell `Get-ProvScheme` para fazer a verificação. Por exemplo: `Get-ProvScheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre esse cmdlet, consulte <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>.

- Licenças do Linux: com as licenças BYOS (traga sua própria assinatura) do Linux, você não precisa pagar pelo software. A cobrança da BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:
  - \* **RHEL\_BYOS**: para usar o tipo RHEL\_BYOS com sucesso, habilite o Red Hat Cloud Access na sua assinatura do Azure.
  - \* **SLES\_BYOS**: as versões BYOS do SLES incluem suporte da SUSE.

Você pode definir o valor do `LicenseType` para as opções do Linux em `New-ProvScheme` e `Set-ProvScheme`.

Exemplo de configuração de `LicenseType` como `RHEL_BYOS` em `New-provScheme`:

```
1 Novo-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` como `SLES_BYOS` em `Set-ProvScheme`:

```
1 Definir-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 Azure Windows Server License ou Azure Linux License, dependendo do valor `OsType`.

Exemplo de configuração de `LicenseType` como vazio:

```
1 Definir-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/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>
- <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>

A Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas do Azure) é um repositório para gerenciar e compartilhar imagens. Ele permite que você disponibilize suas imagens em toda a organização. Recomendamos que você armazene uma imagem na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos de SO VDA. Depois que você selecionar **Place prepared image in Azure Compute Gallery**, aparece a seção **Azure Compute Gallery settings**, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

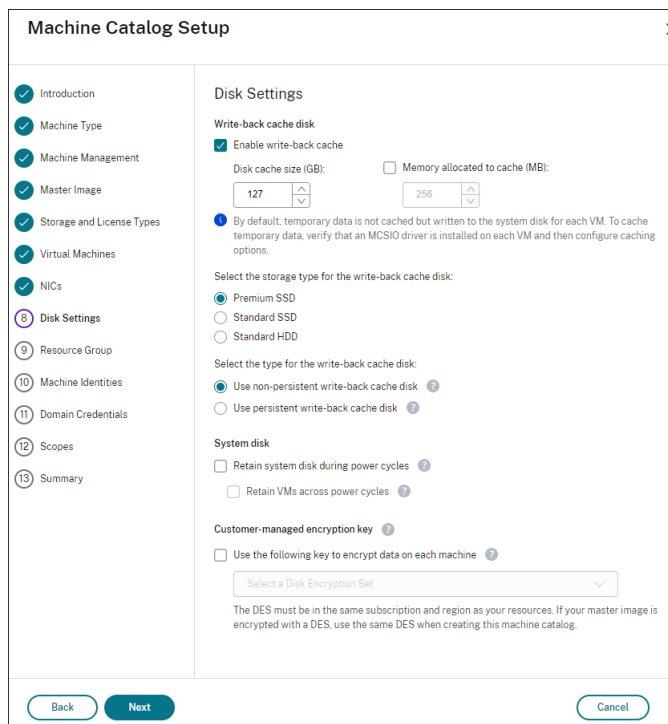
- **Ratio of virtual machines to image replicas.** Permite especificar a proporção de máquinas virtuais para réplicas de imagem que você deseja que o Azure mantenha. Por padrão, o Azure mantém uma única réplica de imagem para cada 40 máquinas não persistentes. Em máquinas persistentes, o número assume o valor padrão 1.000.

- **Maximum replica count.** Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 10.

**Observação:**

Uma galeria é criada no ACG para armazenar a imagem. Essa galeria é acessível somente ao MCS para criação de VMs e não aparece na página **Selecionar uma imagem**.

- Na página **Virtual Machines**, indique quantas VMs você deseja criar. Você deve especificar pelo menos um e selecionar um tamanho de máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.
- A página **NICs** não contém informações específicas do Azure. Siga as instruções no artigo [Criar catálogos de máquinas](#).
- Na página **Disk Settings**, escolha se deseja ativar o cache write-back. Com o recurso de otimização de armazenamento do MCS ativado, você pode definir as seguintes configurações ao criar um catálogo: Essas configurações se aplicam aos ambientes Azure e GCP.



Depois de ativar o cache de write-back, você pode fazer o seguinte:

- Configurar o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte [Configurar cache para dados temporários](#).
- Selecionar o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:

- \* Premium SSD
  - \* Standard SSD
  - \* Standard HDD
- Escolha se deseja que o disco de cache write-back persista para as VMs provisionadas. Selecione **Enable write-back cache** para disponibilizar as opções. Por padrão, a opção **Use non-persistent write-back cache disk** está selecionada.
- Selecione o tipo para o disco de cache de write-back.
- \* **Use non-persistent write-back cache disk.** Se selecionado, o disco de cache write-back é excluído durante os ciclos de alimentação de energia. Todos os dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Template Properties**. Se o disco temporário for usado, você verá **Non-persistent Write-back Cache Disk** e seu valor será **Yes (using VM's temporary disk)**. Caso contrário, você verá **Non-persistent Write-back Cache Disk** e seu valor será **No (not using VM's temporary disk)**.
  - \* **Use persistent write-back cache disk.** Se selecionado, o disco de cache de write-back persistirá para as VMs provisionadas. Habilitar a opção aumenta os custos de armazenamento.
- Escolha se deseja reter VMs e discos do sistema para VDAs durante os ciclos de alimentação de energia.

**Reten VM e disco do sistema durante ciclos de energia.** Disponível quando você seleciona **Ativar cache de write-back**. Por padrão, VMs e discos de sistema são excluídos no desligamento e recriados na inicialização. Se você quiser reduzir o tempo de reinicialização da VM, selecione essa opção. Lembre-se de que ativar essa opção também aumenta os custos de armazenamento.

- Escolha se deseja ativar a **Economia de custos de armazenamento**. Se ativada, economize nos custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Standard quando a VM for desligada. A VM muda para suas configurações originais na reinicialização. A opção se aplica aos discos de armazenamento e cache de write-back. Como alternativa, você também pode usar o PowerShell. Consulte [Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada](#).

**Observação:**

A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie as mudanças

no tipo de armazenamento no futuro. Para obter mais informações, consulte este [artigo da Microsoft](#).

- Escolha se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia no lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas no catálogo. Para obter mais informações, consulte Criptografia do servidor do Azure.
- Na página **Resource Group**, escolha se deseja criar grupos de recursos ou usar grupos existentes.
  - Se você optar por criar grupos de recursos, selecione **Next**.
  - Se você optar por usar grupos de recursos existentes, selecione grupos na lista **Available Provisioning Resource Groups**. **Lembre-se:** selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Será exibida uma mensagem se você escolher muito poucos. Talvez você queira selecionar mais do que o mínimo necessário se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que o catálogo é criado.

Para obter mais informações, consulte Azure resource groups.

- Na página **Machine Identities**, escolha um tipo de identidade e configure identidades para máquinas nesse catálogo. Se você selecionar as VMs como **Azure Active Directory joined**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:
  1. No campo **Identity type**, selecione **Azure Active Directory joined**. A opção **Azure AD security group (optional)** é exibida.
  2. Clique em **Azure AD security group: Create new**.
  3. Insira o nome do grupo e clique em **Create**.
  4. Siga as instruções na tela para fazer logon no Azure. Se o nome do grupo não existir no Azure, um ícone verde é exibido. Caso contrário, uma mensagem de erro é exibida solicitando que você insira um novo nome.
  5. Insira o esquema de nomenclatura da conta da 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 no catálogo são adicionadas automaticamente ao grupo de segurança.

Adicionar VMs com um esquema de nomenclatura diferente a esse catálogo exige que você entre no Azure. O Citrix 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 esse catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.

- As páginas **Domain Credentials** e **Summary** não contêm informações específicas do Azure. Siga as instruções no artigo [Criar catálogos de máquinas](#).

Conclua o assistente.

### Condições para que o disco temporário do Azure seja elegível para disco de cache write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem atendidas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.
- O tamanho escolhido da VM do Azure deve incluir um disco temporário.
- Não é necessário ativar o disco de SO efêmero
- Aceite colocar o arquivo de cache de write-back no disco temporário do Azure.
- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco do cache de write-back + espaço reservado para o arquivo de paginação + 1 GB de espaço no buffer).

### Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back durante a criação do catálogo de máquinas.

---

Cenário	Resultado
Todas as condições para usar o disco temporário para cache write-back estão satisfeitas.	O arquivo WBC <code>mcsdif.vhdx</code> é colocado no disco temporário.
O disco temporário não tem espaço suficiente para o uso do cache write-back.	Um disco VHD <code>MCSWCdisk</code> é criado e o arquivo WBC <code>mcsdif.vhdx</code> é colocado nesse disco.
O disco temporário tem espaço suficiente para o uso do cache de gravação, mas <code>useTempDiskForWBC</code> está definido como <b>false</b> .	Um disco VHD <code>MCSWCdisk</code> é criado e o arquivo WBC <code>mcsdif.vhdx</code> é colocado nesse 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 nos comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Acesse o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a interface de rede e a VM. No menu ..., na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para o provisionamento de catálogos.
3. Clique em **Adicionar à biblioteca** para modificar a especificação do modelo posteriormente.
4. Na página **Importando modelos**, insira as informações necessárias, como **Nome**, **Assinatura**, **Grupo de recursos**, **Local** e **Versão**. Clique em **Próximo: Editar modelo**.
5. Você também precisa de uma interface de rede como um recurso independente se quiser provisionar catálogos. Portanto, você deve remover qualquer **DependsOn** especificado na especificação do modelo. Por exemplo:

```
“
“depende de”: [
“[resourceId(‘Microsoft.Network/networkInterfaces’, ‘tnic937’)]]”
],
“
```

1. Crie **Revisar+Criar** e crie a especificação do modelo.
2. Na página **Especificações do modelo**, verifique a especificação do modelo que você acabou de criar. Clique na especificação do modelo. No painel esquerdo, clique em **Versões**.
3. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação do modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação do modelo.

Você pode obter informações sobre a especificação e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação do modelo, execute:

```
1 obter-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
resourcegroup\bggTemplateSpec.templatespec
```

- Para obter informações sobre a versão da especificação do modelo, execute:

```
1 obter-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
templatespecversion
```

## Usar a especificação do modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou os comandos do PowerShell.

- Para o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio
- Para o PowerShell, consulte Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell

## Criptografia 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 de seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte [Server-side encryption of Azure Disk Storage](#).

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco está criptografado, você altera a chave atual no `DiskEncryptionSet`. Todos os recursos associados a esse `DiskEncryptionSet` mudam para serem criptografados com a nova chave.
- Quando você desabilita ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja habilitada novamente ou você atribua uma nova chave. Qualquer catálogo usando a chave não pode ser ligado e você não pode adicionar VMs a ele.

## Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente

Considere o seguinte ao usar esse recurso:

- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Depois de habilitar a chave de criptografia gerenciada pelo cliente, você não poderá desativá-la posteriormente. Se quiser desativar ou remover a chave de criptografia gerenciada pelo cliente, copie todos os dados para um disco gerenciado diferente que não esteja usando a chave de criptografia gerenciada pelo cliente.



- Os discos criados a partir de imagens personalizadas criptografadas usando criptografia no lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados usando as mesmas chaves gerenciadas pelo cliente. Esses discos devem estar na mesma assinatura.
- Os instantâneos criados a partir de discos criptografados com criptografia do lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados com as mesmas chaves gerenciadas pelo cliente.
- Discos, instantâneos e imagens criptografados com chaves gerenciadas pelo cliente não podem ser movidos para outro grupo de recursos e assinatura.
- Os discos gerenciados criptografados atualmente ou anteriormente usando a Criptografia de Disco do Azure não podem ser criptografados usando chaves gerenciadas pelo cliente.
- Consulte o [site da Microsoft](#) para ver as limitações dos conjuntos de criptografia de disco por região.

#### **Observação:**

Consulte [Início rápido: criar um cofre de chaves usando o portal do Azure](#) para obter informações sobre como configurar a criptografia do servidor do Azure.

## **Chave de criptografia gerenciada pelo cliente do Azure**

Ao criar um catálogo de máquinas, você pode escolher se deseja criptografar dados nas máquinas provisionadas no catálogo. A criptografia no lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas no catálogo. Um Conjunto de Criptografia de Disco (DES) representa uma chave gerenciada pelo cliente. Para usar esse recurso, você deve primeiro criar seu DES no Azure. Um DES está no seguinte formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos. Se a imagem estiver criptografada com um DES, use o mesmo DES ao criar o catálogo da máquina. Você não pode alterar o DES depois de criar o catálogo.

Se você criar um catálogo com uma chave de criptografia e depois desabilitar o DES correspondente no Azure, não poderá mais ligar as máquinas no catálogo ou adicionar máquinas a ele.

Consulte [Criar um catálogo de máquinas usando a 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 suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma especificação de modelo ou uma VM como entrada para um perfil de máquina.

Esse método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta.

### Restrições:

A criptografia de disco do Azure no host é:

- Incompatível com todos os tamanhos de máquinas do Azure
- Incompatível com a criptografia de disco do Azure

Para criar um catálogo de máquinas com capacidade de criptografia no host:

1. Verifique se a assinatura tem o recurso de criptografia no host ativado ou não. Para fazer isso, consulte <https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/>. Se não estiver ativado, você deve ativar o recurso para a assinatura. Para obter informações sobre como ativar o recurso para sua assinatura, consulte <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>.
2. Verifique se um determinado tamanho de VM do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute uma destas opções:

```
1 PS XDHyp:\Conexões\\east us.region\  
serviceoffering.folder>
```

```
1 PS XDHyp:\HostingUnits\\serviceoffering.folder>
```

3. Crie uma especificação de modelo ou uma VM como entrada para o perfil da máquina no portal do Azure com a criptografia no host ativada.
  - Se você quiser criar uma VM, selecione um tamanho de VM que suporte criptografia no host. Depois de criar a VM, a propriedade da VM **Encryption at host** é ativada.
  - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `SecurityProfile`.
4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina selecionando uma especificação de modelo ou VM.

- Disco de SO/Disco de dados: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma
- Disco de SO efêmero: é criptografado somente pela chave gerenciada pela plataforma
- Disco de cache: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma

Você pode criar o catálogo de máquinas usando o Web Studio ou executando comandos do 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 da máquina.

Por exemplo: quando a entrada do perfil da máquina for uma VM, execute o seguinte comando:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.vm).Dados Adicionais
```

Por exemplo: quando a entrada do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_templatespec.templatespec\EncryptionAtHost.templatespecversion).Dados Adicionais
```

### Criptografia dupla no disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Todos os catálogos criados com esse recurso têm todos os discos do lado do servidor criptografados com chaves gerenciadas pela plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a chave de criptografia e os conjuntos de criptografia de disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

#### Observação:

- Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web

Studio e os comandos do PowerShell. Consulte Criar um catálogo de máquinas com criptografia dupla para comandos do PowerShell.

- Você pode usar um fluxo de trabalho não baseado em perfil de máquina ou um fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
- Se você usar um fluxo de trabalho não baseado em perfil de máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetID` armazenado.
- Se você usa um perfil de máquina, pode usar uma especificação de VM ou modelo como uma entrada de perfil de máquina.

### Limitações:

- A criptografia dupla não é suportada em Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desabilitar uma chave `DiskEncryptionSet` associada a um catálogo, as VMs do catálogo serão desativadas.
- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você só pode criar até 50 conjuntos de criptografia de disco por região por assinatura.
- Você não pode atualizar um catálogo de máquinas que já tenha um `DiskEncryptionSetID` com um `DiskEncryptionSetID` diferente.

### Grupos de recursos do Azure

Os grupos de recursos de provisionamento do Azure fornecem uma maneira de provisionar as VMs que fornecem aplicativos e áreas de trabalho aos usuários. Você pode adicionar grupos de recursos do Azure vazios existentes ao criar um catálogo de máquinas do MCS ou criar novos grupos de recursos para você. Para obter informações sobre grupos de recursos do Azure, consulte a [documentação da Microsoft](#).

### Uso do grupo de recursos do Azure

Não há limite para o número de máquinas virtuais, discos gerenciados, instantâneos e imagens por Grupo de Recursos do Azure. (O limite de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure foi removido.)

- Ao usar uma entidade de serviço de escopo completo para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar uma entidade de serviço de escopo restrito para criar um catálogo de máquinas, você deve fornecer um Grupo de Recursos do Azure vazio e pré-criado para o catálogo.

## Discos efêmeros do Azure

Um [disco efêmero do Azure](#) permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte [Criar um catálogo com discos efêmeros do Azure](#).

### Observação:

Os catálogos persistentes não oferecem suporte a discos de SO efêmeros.

Os discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Imagens Compartilhadas.

## Armazenando um disco temporário do sistema operacional efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM ou em um disco de recursos. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não tenha um cache ou que tenha cache insuficiente. Essas VMs têm um disco temporário ou de recursos para armazenar um disco operacional efêmero, como [Ddv4](#).

Considere o seguinte:

- Um disco efêmero é armazenado no disco de cache da VM ou no disco temporário (recurso) da VM. O disco de cache tem preferência em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco de SO.
- Para atualizações, uma nova imagem maior que o disco de cache, mas menor que o disco temporário, resulta na substituição do disco de SO efêmero pelo disco temporário da VM.

## Otimização de armazenamento de disco efêmero do Azure e do MCS (Machine Creation Services) (MCS I/O)

O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Não é possível criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- Os parâmetros do PowerShell ([useWritebackCache](#) e [useEphemeralDisk](#)) falham com mensagens de erro adequadas se você defini-los como **true** em [New-ProvScheme](#) ou [Set-ProvScheme](#).

- Para catálogos de máquinas existentes criados com os dois recursos ativados, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

## Galeria de Computação do Azure

Use a Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas do Azure) como um repositório de imagens publicadas para máquinas provisionadas do MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação dos discos de SO, melhorando os tempos de início e de inicialização do aplicativo para VMs não persistentes. A galeria de imagens compartilhadas contém os seguintes três elementos:

- *Galeria*: as imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de imagem na 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.
- *Versões da Imagem da Galeria*: Cada imagem em uma Galeria de Imagens Compartilhada pode ter várias versões, e cada versão pode ter várias réplicas em diferentes regiões. Cada réplica é uma cópia completa da imagem publicada.

### Observação:

A funcionalidade da Galeria de Imagens Compartilhadas só é compatível com discos gerenciados. Não está disponível para catálogos de máquinas legadas.

Para obter mais informações, consulte a [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 usando o PowerShell, consulte [Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure](#).

## VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida durante o uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho do perfil da máquina para criar esse catálogo. Você pode usar as especificações do modelo VM e ARM como uma entrada de perfil de máquina.

## Considerações importantes sobre VMs confidenciais

As considerações importantes sobre os tamanhos de VM compatíveis e a criação de um catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM compatíveis: as VMs confidenciais aceitam os seguintes tamanhos de VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Crie catálogos de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com VMs confidenciais do Azure usando os comandos do Web Studio e do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquina com VMs Confidenciais do Azure. Você pode usar uma especificação de modelo ou VM como a entrada do perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar ativadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:
    - \* **VMGuestStateOnly**: VM confidencial com apenas o estado de convidado da VM criptografado
    - \* **DiskWithVMGuestState**: VM confidencial com disco do sistema operacional e estado de convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco operacional normal quanto o efêmero podem ser criptografados.
  - Você pode obter informações da VM confidencial de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM usando o parâmetro `AdditionalData`. Por exemplo:

```
1 PS C:\Usuários\nome de usuário> (get-item XDHyp:\HostingUnits
  \minharede\imagem.pasta\nome de usuário-dev-testing-rg.
  resourcegroup\nome de usuário-dev-tsvda.vm).
  DadosAdicionais
```

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 "xDHY p:\Connections\my -connection-name\ East Us.region\ serviceoffering.folder\ abc.serviceoffering").additionalData`

O campo de dados adicional é `ConfidentialComputingType`.

- Você não pode alterar a imagem mestre ou o perfil da máquina do tipo de segurança confidencial para não confidencial ou do tipo de segurança não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

### Preparar imagens mestras 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 sistema operacional confidencial:** ativada.
  - **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 e o VDA necessários na VM criada.

#### Observação:

Não há suporte para a criação de VMs confidenciais usando VHD. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil de máquina usando uma das seguintes formas:
  - Use a VM existente criada na etapa 1 se ela tiver as propriedades de máquina necessárias.
  - Se você optar por uma especificação de modelo do ARM como perfil de máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos confidenciais de VM, como `SecurityEncryptionType` e `DiskEncryptionSet` (para chave gerenciada pelo cliente). Para obter mais informações, consulte [Criar uma especificação de modelo do Azure](#).

#### Observação:

- Certifique-se de que a imagem mestre e o perfil de máquina tenham o mesmo tipo de chave de segurança.



- Para criar VMs confidenciais que exijam criptografia confidencial de disco do sistema operacional com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil de máquina sejam idênticos.

### **Criar VMs confidenciais usando comandos do Web Studio ou PowerShell**

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Web Studio, siga as etapas descritas em [Criar catálogos de máquinas](#). Lembre-se das seguintes considerações:

- 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 de máquina é obrigatória e somente os perfis que correspondam ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.
- Na página **Máquinas virtuais**, somente os tamanhos de máquina que permitem VMs confidenciais aparecem para seleção.
- Na página **Configurações do disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

### **Azure Marketplace**

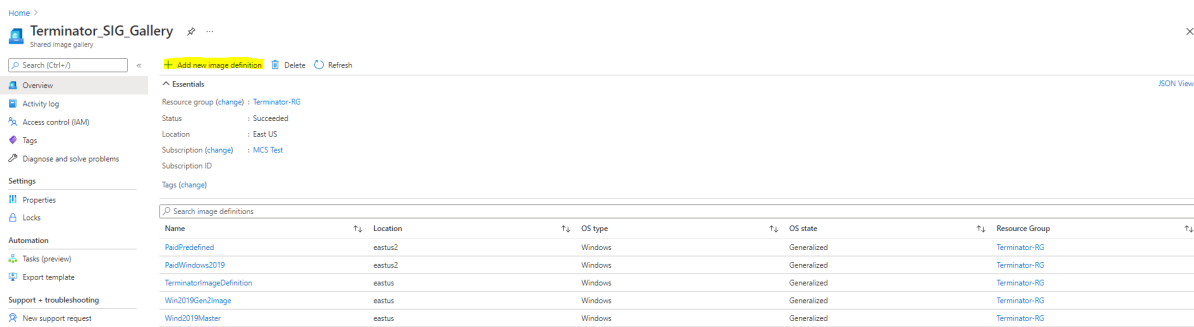
O Citrix Virtual Apps and Desktops oferece suporte ao uso de uma imagem mestre no Azure que contém informações do plano para criar um catálogo de máquina. Para obter mais informações, consulte [Microsoft Azure Marketplace](#).

#### **Dica:**

Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não acrescentam informações do plano. O recurso Citrix Virtual Apps and Desktops é para imagens pagas.

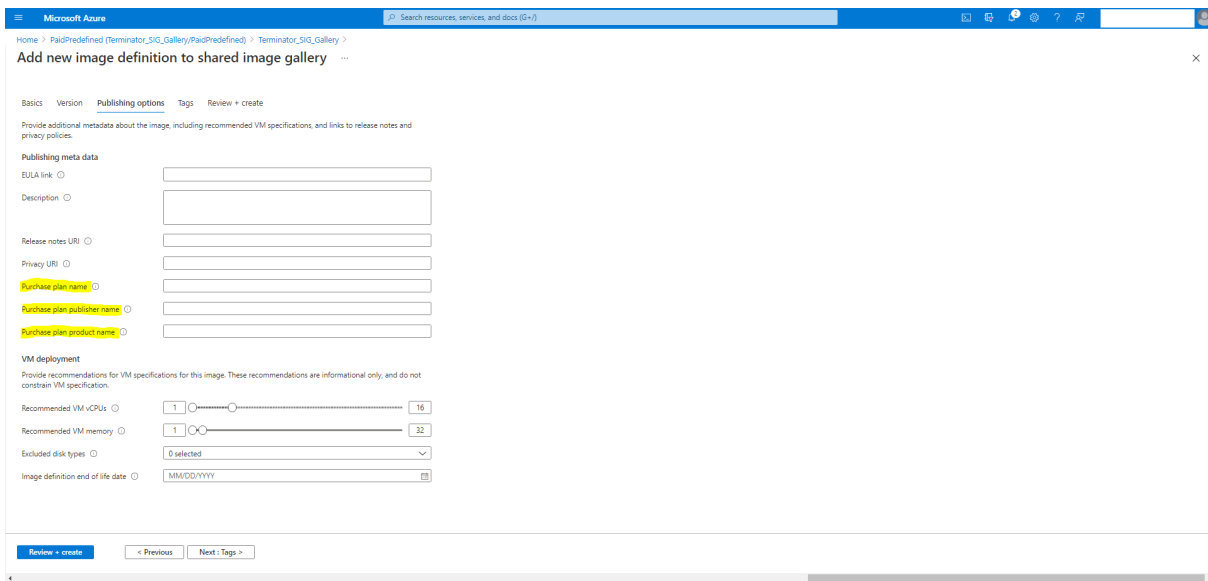
### **Verifique se a imagem criada na Galeria de Imagens Compartilhadas contém informações do plano do Azure**

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Opcionalmente, essas imagens podem ser usadas para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.



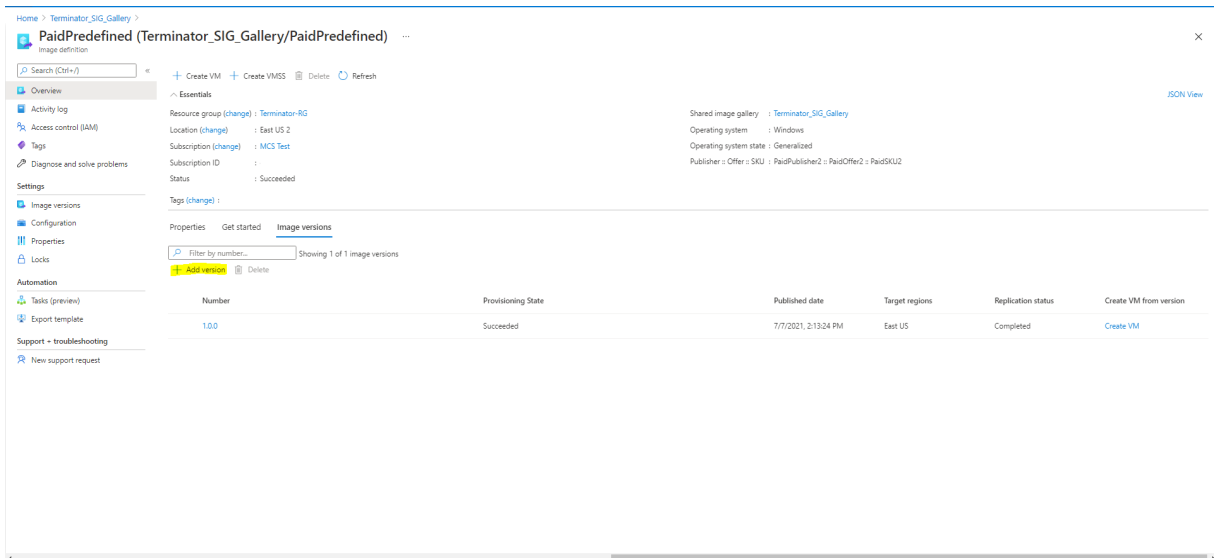
Na página **Publishing options**, verifique as informações do plano de compra.

Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. Se você deixar de preencher as informações do plano de compra, isso pode causar falha no processo do catálogo de máquinas.



Depois de verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Isso é usado como a imagem mestre. Clique em **Add version**:

## Aplicativos e desktops virtuais Citrix 7 2402 LTSR



Home > Terminator\_SIG\_Gallery > PaidPredefined (Terminator\_SIG\_Gallery/PaidPredefined)

Image definition

Search (Ctrl+F)

Essentials

Resource group (change) : Terminator-RG  
Location (change) : East US 2  
Subscription (change) : MCS Test  
Subscription ID :  
Status : Succeeded

Tags (change) :

Shared image gallery : Terminator\_SIG\_Gallery  
Operating system : Windows  
Operating system state : Generalized  
Publisher : Offer : SKU : PaidPublisher2 : PaidOffer2 : PaidSKU2

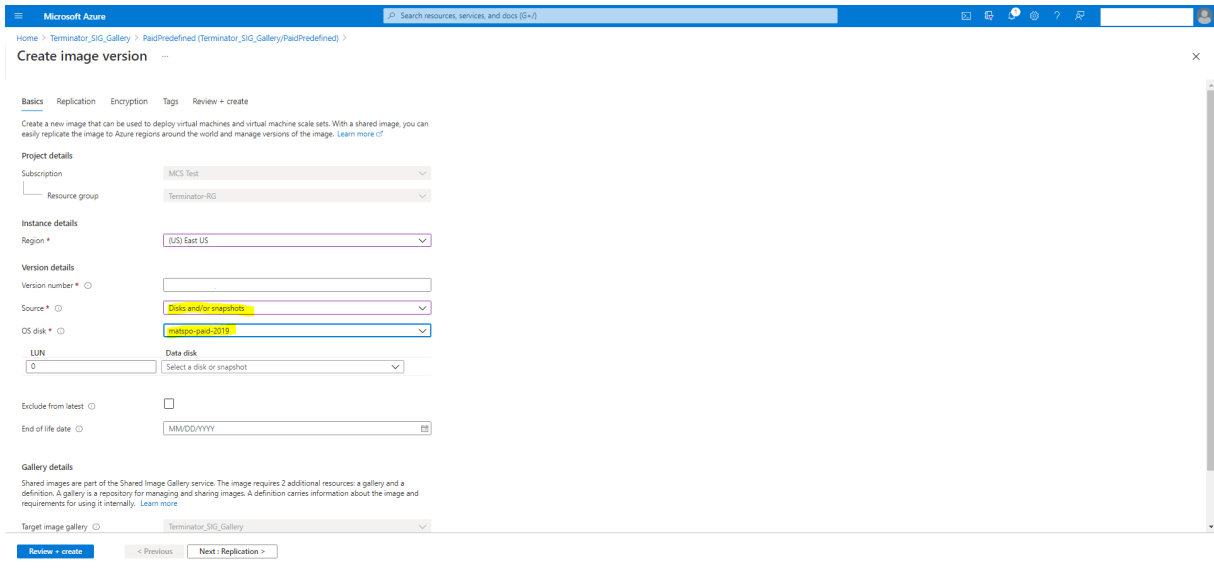
Properties Get started Image versions

Filter by number... Showing 1 of 1 image versions

Add version Delete

Number	Provisioning State	Published date	Target regions	Replication status	Create VM from version
1.0.0	Succeeded	7/7/2021, 2:13:24 PM	East US	Completed	Create VM

Na seção **Version details**, selecione o instantâneo da imagem ou o disco gerenciado como origem:



Microsoft Azure Search resources, services, and docs (Ctrl+)

Home > Terminator\_SIG\_Gallery > PaidPredefined (Terminator\_SIG\_Gallery/PaidPredefined)

Create image version

Basics Replication Encryption Tags Review + create

Create a new image that can be used to deploy virtual machines and virtual machine scale sets. With a shared image, you can easily replicate the image to Azure regions around the world and manage versions of the image. [Learn more](#)

Project details

Subscription : MCS Test  
Resource group : Terminator-RG

Instance details

Region : (US) East US

Version details

Version number :  
Source : Disk and/or snapshots  
OS disk : managed-2019  
LUN : Data disk  
Data disk : Select a disk or snapshot

Exclude from latest :  
End of life date : MM/DD/YYYY

Gallery details

Shared images are part of the Shared Image Gallery service. The image requires 2 additional resources: a gallery and a definition. A gallery is a repository for managing and sharing images. A definition carries information about the image and requirements for using it internally. [Learn more](#)

Target image gallery : Terminator\_SIG\_Gallery

Review + create < Previous Next: Replication >

## Criar um catálogo de máquinas usando o PowerShell

Esta seção detalha como você pode criar catálogos usando o PowerShell:

- Criar um catálogo com disco de cache de write-back não persistente
- Criar um catálogo com disco de cache de write-back não persistente
- Melhorar o desempenho de inicialização com o MCSIO
- Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell
- Catálogos de máquinas com início confiável
- Usar valores de propriedades do perfil da máquina
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

- 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 a imagem da Galeria de Computação do Azure
- Configurar a Galeria de Imagens Compartilhadas
- Provisionar máquinas em zonas de disponibilidade especificadas
- Tipos de armazenamento
- Localização do arquivo de paginação
- Atualizar configuração do arquivo de página
- Criar um catálogo usando VMs do Azure Spot
- Configurar tamanhos de VM de backup
- Copiar marcas em todos os recursos
- Provisionar VMs do catálogo com o Azure Monitor Agent 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 do PowerShell `New-ProvScheme CustomProperties`. A propriedade personalizada `UseTempDiskForWBC` indica se você está aceitando usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como verdadeiro ao executar `New-ProvScheme` se você quiser usar o disco temporário como disco de cache de gravação. Se essa propriedade não for especificada, o parâmetro será definido como **False** por padrão.

Por exemplo, usando o parâmetro `CustomProperties` para definir `UseTempDiskForWBC` como **true**:

```
1 -Propriedades Personalizadas '<CustomProperties xmlns=" http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org
   /2001/XMLSchema-instance"> `
2 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
3 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
4 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
5 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
6 <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
   Premium_LRS"/> `
7 <Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
8 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
   true"/> `
9 </CustomProperties>'
```

**Observação:**

Depois de confirmar o catálogo da máquina para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar o VHD posteriormente.

## Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. Esse parâmetro oferece suporte a uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de gravação persiste em máquinas provisionadas pelo MCS. A propriedade `PersistWBC` só é usada quando o parâmetro `UseWritebackCache` é especificado e quando o parâmetro `WritebackCacheDiskSize` é definido para indicar que um disco foi criado.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes do suporte ao `PersistWBC` incluem:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
   />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvalde5RG3" />
5 </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 gravação 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 gravação 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 assumirá como padrão **false** e o cache de gravação será excluído quando a máquina for desligada usando o Web Studio.

Por exemplo, usando o parâmetro `CustomProperties` para definir `persistWBC` como `true`:

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benva1dev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>

```

**Importante:**

A propriedade `PersistWBC` só pode ser definida usando o cmdlet `New-ProvScheme` PowerShell. A tentativa de alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo da máquina e na persistência do disco de cache de gravação quando uma máquina é desligada.

Por exemplo, defina `New-provScheme` para usar o cache de write-back enquanto define a propriedade `persistWBC` como `true`:

```

1 Novo-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
  /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
  XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
  UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benva1dev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSI0-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256

```

## Melhorar o desempenho de inicialização com o MCSIO

Você pode melhorar o desempenho de inicialização dos discos gerenciados do Azure e do GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada PowerShell `PersistOsDisk` no comando `New-provScheme` para configurar esse recurso. As opções associadas ao `New-ProvScheme` incluem:

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource ` ` ` ` ` ` <!--NeedCopy
  -->
5 ` ` ` ` ` ` ` ` ` ` Grupos" Valor="benvaldev5RG3" />
6 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
  />
7 </CustomProperties>

```

Para ativar esse recurso, defina a propriedade personalizada `PersistOsDisk` como **true**. Por exemplo:

```

1 Novo-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
  /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
  XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
  UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSIO-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256

```

## Usar a especificação do modelo na criação ou atualização de um catálogo usando o 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 os comandos do PowerShell.

Para o Web Studio, consulte Criar um catálogo de máquinas por meio de 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:

```
1 Novo-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/  
  image.folder/fgthj.resourcegroup/nab-ws-  
  vda_0sDisk_1_xxxxxxxxxxa.manageddisk"  
2 MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.  
  folder/fgthj.resourcegroup/test.templatespec/V1.  
  templatespecversion"  
3 -ProvisioningSchemeName <String>  
4 -HostingUnitName <String>  
5 -IdentityPoolName <String>  
6 [-ServiceOffering <String>][-CustomProperties <String>  
7 [-LoggingId <Guid>]  
8 [-BearerToken <String>][-AdminAddress <String>]  
9 [<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:

```
1 Set-ProvScheme -MasterImageVm 'XDHyp://Conexões/Azure/East Us  
  .region/vm.folder/MasterDisk.vm'  
2 MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.  
  folder/fgthj.resourcegroup/testing.templatespec/V1.  
  templatespecversion'  
3 [-ProvisioningSchemeName] <String>  
4 [-CustomProperties <String>][-ServiceOffering <String>] [-  
  PassThru]  
5 [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <  
  String>] [<CommonParameters>]
```



## Catálogos de máquinas com início confiável

Para criar com êxito um catálogo de máquinas com início confiável, use:

- Um perfil de máquina com início confiável
- Um tamanho de VM que ofereça suporte ao início confiável
- Uma versão de VM do Windows que ofereça suporte ao início confiável. Atualmente, o Windows 10, o Windows 11 e o Windows Server 2016, 2019 e 2022 oferecem suporte ao início confiável.

### Importante:

O MCS oferece suporte à criação de um novo catálogo com VMs habilitadas para o início confiável. No entanto, para atualizar um catálogo persistente existente e as VMs existentes, você precisa usar o portal do Azure. Você não pode atualizar o início confiável de um catálogo não persistente. Para obter mais informações, consulte o documento da Microsoft [Habilitar o Início confiável em VMs existentes do Azure](#).

Para exibir os itens de inventário da oferta do Citrix Virtual Apps and Desktops e determinar se o tamanho da VM oferece suporte ao início confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnpcitrix\*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
1 $s = (ls XDHyp:\HostingUnits\\
    serviceoffering.folder\
```

4. Execute `$s | select -ExpandProperty Dados adicionais`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
  - Se `SupportTrustedLaunch` for **True**, o tamanho da VM suporta o lançamento confiável.
  - Se `SupportTrustedLaunch` for **False**, o tamanho da VM não suporta o lançamento confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que oferecem suporte ao início confiável:

```
1 (Get-AzComputeResourceSku | onde {
2   $_.Locations.Contains($region) -e ($_.Name -eq "<VM size>") }
3 ) [0].Capacidades
```

Veja a seguir exemplos que descrevem se o tamanho da VM oferece ou não suporte ao início confiável após a execução do comando do Azure PowerShell.

- *Exemplo 1:* se a VM do Azure oferecer suporte somente à Geração 1, a VM não é compatível com o início confiável. Portanto, o recurso `TrustedLaunchDisabled` não é exibido após a execução do comando Azure PowerShell.
- *Exemplo 2:* Se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` for **True**, o tamanho da VM da Geração 2 não terá suporte para inicialização confiável.
- *Exemplo 3:* Se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` não for exibido após a execução do comando PowerShell, o tamanho da VM da Geração 2 terá suporte para inicialização confiável.

Para obter mais informações sobre o início confiável de máquinas virtuais do Azure, consulte o documento da Microsoft [Início confiável para máquinas virtuais do Azure](#).

### Criar um catálogo de máquinas com início confiável

1. Crie uma imagem mestre habilitada com o início confiável. Consulte a documentação da Microsoft [Imagens da VM de início confiável](#).
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de início confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft [Implantar uma VM de início confiável](#).
3. Crie um catálogo de máquinas usando os comandos do Web Studio ou do PowerShell.
  - Se você quiser usar o Web Studio, consulte [Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio](#).
  - Se você quiser usar comandos do PowerShell, use o comando `New-ProvScheme` com a VM ou a especificação do modelo como uma entrada de perfil de máquina. Para obter a lista completa de comandos para criar um catálogo, consulte [Criação de um catálogo](#).

Exemplo de `New-ProvScheme` com VM como entrada de perfil de máquina:

```
1 Novo-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
  IdentityPoolName "nome" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
  resourcegroup/nab-ws-vda_0sDisk_1_XXXXXXXXXX.manageddisk"
3 -MachineProfile "XDHyp:\HostingUnits\\machineprofile.
  folder\
```

Exemplo de `New-ProvScheme` com especificação de modelo como entrada de perfil de máquina:

```

1 Novo-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
  IdentityPoolName "nome" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
  resourcegroup/nab-ws-vda_0sDisk_1_xxxxxxxxxxa.manageddisk"
3 MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
  folder/fgthj.resourcegroup/test.templatespec/V1.
  templatespecversion"
4 -ProvisioningSchemeName <String>
5 -HostingUnitName <String>
6 -IdentityPoolName <String>
7 [-Oferta de serviço <String>][-Propriedades personalizadas <
  String>]
8 [<CommonParameters>]
  
```

### Erros ao criar catálogos de máquinas com o início confiável

Você verá os erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com início confiável:

Cenário	Erro
Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado	MachineProfileNotSupportedForUnmanagedCatalog
Se você selecionar um perfil de máquina compatível com início confiável ao criar um catálogo com disco não gerenciado como imagem mestre	Tipo de segurança não suportado para disco não gerenciado
Se você não selecionar um perfil de máquina ao criar um catálogo gerenciado com a origem de uma imagem mestre com início confiável como o tipo de segurança	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 ofereça suporte ao início confiável, mas usar uma imagem mestre compatível com início confiável ao criar um catálogo	MachineSizeNotSupportTrustedLaunch

## Usar valores de propriedades do perfil da máquina

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

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

Se essas propriedades personalizadas não forem definidas explicitamente, os valores da propriedade serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como o perfil da máquina. Além disso, se `ServiceOffering` não for especificado, ele será definido a partir do perfil da máquina.

### Observação:

Se algumas das propriedades estiverem ausentes no perfil da máquina e não estiverem definidas nas propriedades personalizadas, os valores padrão das propriedades serão usados sempre que aplicável.

A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` tem todas as propriedades definidas ou os valores são derivados do `MachineProfile`.

- Cenário New-ProvScheme
  - `MachineProfile` tem todas as propriedades e `CustomProperties` não estão definidas. Exemplo:

```
Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit  
\machineprofile.folder\azure.resourcegroup\mpA.vm"
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1 Obter-ProvScheme | selecione Propriedades Personalizadas  
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/  
   machinecreation" xmlns:xsi="http://www.w3.org/2001/  
   XMLSchema-instance">  
3 <Property xsi:type="StringProperty" Name="StorageAccountType"  
   Value="<mpA-value>"/>  
4 <Property xsi:type="StringProperty" Name="OSType" Value="<mpA  
   -value>"/>  
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=  
   "<mpA-value>"/>
```

```

6 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
  " Value="<mpA-value>"/>
7 <Property xsi:type="StringProperty" Name="
  DedicatedHostGroupId" Value="<mpA-value>"/>
8 <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
  value>"/>
9 </CustomProperties>

```

- MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem somente LicenseType e OsType.

```

Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"

```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```

1 Obter-ProvScheme | selecione Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
  -value>"/>
4 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<mpA-value>"/>
5 </CustomProperties>

```

- Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

```

Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
$CustomPropertiesA

```

As propriedades personalizadas têm prioridade. Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```

1 Obter-ProvScheme | selecione Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<CustomPropertiesA-value>"/>
4 <Property xsi:type="StringProperty" Name="OSType" Value="<
  CustomPropertiesA-value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<CustomPropertiesA-value>"/>
6 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
  " Value="<CustomPropertiesA-value>"/>
7 <Property xsi:type="StringProperty" Name="
  DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
8 <Property xsi:type="StringProperty" Name="Zones" Value="<
  CustomPropertiesA-value>"/>
9 </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

```
Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
$CustomPropertiesA
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1 Obter-ProvScheme | selecione Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>
4 <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
-value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
"<CustomPropertiesA-value>"/>
6 <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>
7 </CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não está definida. Exemplo:

- \* CustomProperties definem StorageType
- \* MachineProfile define LicenseType

```
1 Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\
azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"
2 -ServiceOffering "XDHyp:\HostingUnits\azureunit\
serviceoffering.folder\<explicit-machine-size>.
serviceoffering"
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1 Obter-ProvScheme | selecionar ServiceOffering
2 serviceoffering.folder\<explicit-machine-size>.
serviceoffering
3
4 Obter-ProvScheme | selecionar CustomProperties
5 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
6 <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>
7 <Property xsi:type="StringProperty" Name="LicenseType" Value=
"value-from-machineprofile"/>
```

```
8 </CustomProperties>
```

- Se OsType não estiver em CustomProperties nem em MachineProfile, então:
  - \* O valor é lido a partir da imagem mestre.
  - \* Se a imagem mestre for um disco não gerenciado, OsType será definido como Windows. Exemplo:

```
Novo-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
"XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

O valor da imagem mestre é gravado nas propriedades personalizadas, nesse caso, Linux.

```
1 Obter-ProvScheme | selecionar Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="OsType" Value="
Linux"/>
4 </CustomProperties>
```

- Cenários Set-ProvScheme

- Um catálogo existente com:
  - \* Propriedades personalizadas para StorageAccount Type e OsType
  - \* MachineProfile Mpa .vm que define zonas
- Atualizações:
  - \* MachineProfile mpB.vm que define StorageAccountType
  - \* Um novo conjunto de propriedades personalizadas \$CustomPropertiesB que define LicenseType e OsType

```
Definir-ProvScheme -MachineProfile "XDHyp:\HostingUnits\
azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm
"-CustomProperties $CustomPropertiesB
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1 Obter-ProvScheme | selecione Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>
4 <Property xsi:type="StringProperty" Name="OsType" Value="<
CustomPropertiesB-value>"/>
```

```

5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<CustomPropertiesB-value>"/>
6 </CustomProperties>

```

- Um catálogo existente com:

- \* Propriedades personalizadas para `Spara RageAccountType` e `OStype`
- \* `MachineProfile MPA . vm` que define `StorageAccountType` e `LicenseType`

- Atualizações:

- \* Um novo conjunto de propriedades personalizadas `$CustomPropertiesB` que define `StorageAccountType` e `OsType`.

`Definir-ProvScheme -Propriedades Personalizadas $CustomPropertiesB`

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```

1 Obter-ProvScheme | selecione Propriedades Personalizadas
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<CustomPropertiesB-value>"/>
4 <Property xsi:type="StringProperty" Name="OSType" Value="<
  CustomPropertiesB-value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<mp-A-value>"/>
6 </CustomProperties>

```

- Um catálogo existente com:

- \* Propriedades personalizadas para `StorageAccount Type` e `OStype`
- \* `MachineProfile Mpa . vm` que define zonas

- Atualizações:

- \* Um `MachineProfile mpB.vm` que define `StorageAccountType` e `LicenseType`
- \* `ServiceOffering` não está especificada

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit  
\machineprofile.folder\azure.resourcegroup\mpB.vm"`

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```

1 Obter-ProvScheme | selecionar ServiceOffering
2 serviceoffering.folder\<value-from-machineprofile>.
  serviceoffering
3
4 Obter-ProvScheme | selecionar CustomProperties

```



```
5 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
6 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<mpB-value>"/>
7 <Property xsi:type="StringProperty" Name="OSType" Value="<
  prior-CustomProperties-value>"/>
8 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<mpB-value>"/>
9 </CustomProperties>
```

## Provisionar VMs do catálogo com o Azure Monitor Agent instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e atuar nos dados de telemetria de seus ambientes do Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos computacionais, como máquinas virtuais, e entrega os dados para o Azure Monitor. Atualmente, ele oferece suporte à coleção de métricas de Logs de eventos, Syslog e Desempenho e a envia para fontes de dados do Azure Monitor Metrics e do Azure Monitor Logs.

Para habilitar o monitoramento identificando de forma exclusiva as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

### Requisitos

- Permissões: verifique se você tem as permissões mínimas do Azure, conforme especificado em [Permissões necessárias do Azure](#), e as seguintes permissões para usar o Azure Monitor:
  - Microsoft.Compute/virtualMachines/extensões/leitura
  - Microsoft.Compute/virtualMachines/extensões/escrever
  - Microsoft.Insights/DataCollectionRuleAssociations/Leitura
  - Microsoft.Insights/dataCollectionRuleAssociations/escrever
  - Microsoft.Insights/Regras de coleta de dados/Leitura
- Regra de coleta de dados: configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar um DCR, consulte [Criar uma regra de coleta de dados](#). Um DCR é específico da plataforma (Windows ou Linux). Certifique-se de criar um DCR de acordo com a plataforma necessária. A AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e fontes de dados, como Azure Monitor Metrics e Azure Monitor Logs.

- Espaço de trabalho padrão: crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um espaço de trabalho, consulte [Criar um espaço de trabalho do Log Analytics](#). Quando você coleta logs e dados, as informações são armazenadas em um espaço de trabalho. Um espaço de trabalho tem um ID de espaço de trabalho e um ID de recurso exclusivos. O nome do espaço de trabalho deve ser exclusivo para um determinado grupo de recursos. Depois de criar um espaço de trabalho, configure fontes de dados e soluções para armazenar seus dados no espaço de trabalho.
- Incluiu a extensão do monitor na lista branca: As extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões definidas pela Citrix na lista branca. Para ver a lista de extensões na lista branca, use o comando PoSH, `Get-ProvMetadataConfiguration`.
- Imagem mestre: a Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso poderá levar a arquivos remanescentes e comportamento inesperado. Para obter mais informações, consulte [Se a VM for recriada a partir de uma VM existente](#).

Para provisionar VMs de catálogo com o AMA ativado:

1. Configure um modelo de perfil de máquina.

- Se você quiser usar uma máquina virtual como modelo de perfil de máquina:
  - a) Crie uma VM no portal do Azure.
  - b) Ligue a VM.
  - c) Adicione a VM à regra de coleta de dados em **Resources**. Isso invoca a instalação do agente na VM modelo.

**Observação:**

Se você precisar criar um catálogo Linux, configure uma máquina Linux.

- Se você quiser usar a especificação do modelo como modelo de um perfil de máquina:
  - a) Configure uma especificação de modelo.
  - b) Adicione a seguinte associação de extensão e regra de coleta de dados à especificação do modelo gerado:

```
1 {
2
3 "tipo": "Microsoft.Compute/virtualMachines/extensões",
4 "apiVersion": "2022-03-01",
5 "nome": "<vm-name>/AzureMonitorWindowsAgent",
6 "dependsOn": [
7     "Microsoft.Compute/virtualMachines/<vm-name>"
8 ],
```

```
9  "localização": "<azure-region>",
10 "propriedades": {
11
12     "publicador": "Microsoft.Azure.Monitor",
13     "tipo": "AzureMonitorWindowsAgent",
14     "typeHandlerVersion": "1.0",
15     "autoUpgradeMinorVersion": verdadeiro,
16     "enableAutomaticUpgrade": verdadeiro
17 }
18
19 }
20 ,
21 {
22
23     "tipo": "Microsoft.Insights/
24         dataCollectionRuleAssociations",
25     "apiVersion": "2021-11-01",
26     "nome": "<associatio-name>",
27     "escopo": "Microsoft.Compute/virtualMachines/<vm-name>"
28     ,
29     "dependsOn": [
30         "Microsoft.Compute/virtualMachines/<vm-name>",
31         "Microsoft.Compute/virtualMachines/<vm-name>/extensions
32             /AzureMonitorWindowsAgent"
33     ],
34     "properties": {
35         "description": "Associação de regra de coleta de
36             dados. A exclusão desta associação interromperá a
37             coleta de dados para este servidor Arc.",
38         "dataCollectionRuleId": "/subscriptions/<azure-
39             subscription>/resourcegroups/<azure-resource-group>/
40             providers/microsoft.insights/datacollectionrules
41             /<azure-data-collection-rule>"
42     }
43 }
```

## 2. Crie ou atualize um catálogo de máquinas MCS existente.

- Para criar um novo catálogo MCS:
  - a) Selecione essa de VM ou especificação modelo como um perfil de máquina no Web Studio.
  - b) Continue com as próximas etapas para criar o catálogo.
- Para atualizar um catálogo MCS existente, use os seguintes comandos PoSH:
  - Para que as novas VMs obtenham o modelo de perfil de máquina atualizado, execute o seguinte comando:

```
1 Set-ProvScheme -ProvisioningSchemeName "nome"
```

```
2 -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.  
folder\abc.resourcegroup\ab-machine-profile.vm"
```

- Para atualizar as VMs existentes com o modelo de perfil de máquina atualizado:

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName meu-cat  
álogo -StartsNow -DurationInMinutes -1
```

3. Ligue as máquinas virtuais do catálogo.
4. Acesse o portal do Azure e verifique se a extensão do monitor está instalada na VM e se a VM aparece nos recursos do DCR. Depois de alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

### Solução de problemas

Para obter informações para orientar a solução de problemas do agente do Azure Monitor, consulte o seguinte:

- <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/>
- <https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/>

### Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

As etapas detalhadas sobre como criar um catálogo de máquinas com a chave de criptografia gerenciada pelo cliente são:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos à Citrix.
3. Digite `cd xdhyp:/`.
4. Digite `cd. \ HostingUnits\` (sua unidade de hospedagem).
5. Digite `cd diskencryptionset.folder`.
6. Digite `dir` para obter a lista de Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma cadeia de caracteres de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

```

1 $customProperties = "<CustomProperties xmlns='http://schemas.
  citrix.com/2014/xd/machinecreation' xmlns:xsi='http://www.w3.
  org/2001/XMLSchema-instance'">
2 <Property xsi:type='StringProperty' Name='StorageAccountType'
  Value='Standard_LRS' />
3 <Property xsi:type='StringProperty' Name='persistWBC' Value='
  False' />
4 <Property xsi:type='StringProperty' Name='PersistOsDisk' Value
  ='false' />
5 <Property xsi:type='StringProperty' Name='UseManagedDisks'
  Value='true' />
6 <Property xsi:type='StringProperty' Name='DiskEncryptionSetId'
  Value='/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxx/
  resourceGroups/abc/providers/Microsoft.Compute/
  diskEncryptionSets/abc-des' />
7 </CustomProperties>

```

9. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```

1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
  Domain def.local -NamingSchemeType Numérico

```

10. Execute o comando New-ProvScheme. Por exemplo:

```

1 Novo-ProvScheme -CleanOnBoot -HostingUnitName "nome" -
  IdentityPoolName "nome" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
  resourcegroup\def.snapshot"
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
  def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
  " }
5
6 -ProvisioningSchemeName "nome"
7 -ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
  folder\Standard_DS2_v2.serviceoffering"
8 -MachineProfile "XDHyp:\HostingUnits\<adnet>\machineprofile.folder
  \<def.resourcegroup>\<machine profile vm>"
9 -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 os comandos do PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e um DES com chaves gerenciadas pela plataforma e pelo cliente. Para

obter informações sobre como criar um Azure Key Vault e um DES, consulte [Usar o portal do Azure para habilitar a criptografia dupla inativa para discos gerenciados](#).

2. Para procurar os DiskEncryptionSets disponíveis em sua conexão de hospedagem:

- a) Abra uma janela do **PowerShell**.
- b) Execute os seguintes comandos do PowerShell:
  - i. `asnp citrix*`
  - ii. `cd xdhyp:`
  - iii. `cd HostingUnits`
  - iv. `cd NomeDaUnidadeDeHospedagem` (ex. azure-east)
  - v. `cd diskencryptionset.folder`
  - vi. `dir`

Você pode usar um ID do `DiskEncryptionSet` para criar ou atualizar um catálogo usando propriedades personalizadas.

3. Se você quiser usar o fluxo de trabalho do perfil da máquina, crie uma especificação de VM ou modelo como entrada do perfil da máquina.

- Se você quiser usar uma VM como entrada de perfil de máquina:
  - a) Crie uma VM no Portal do Azure.
  - b) Navegue até **Disks>Key management** para criptografar a VM diretamente com 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, siga um dos procedimentos a seguir, além das etapas em [Criar catálogos de máquinas](#).
  - Se você não usar o fluxo de trabalho baseado em perfil de máquina, na página **Configurações do disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue a criar o catálogo.
  - Se estiver usando o fluxo de trabalho do perfil da máquina, na página **Imagem**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID do conjunto de criptografia de disco em suas propriedades.

Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

- Se estiver usando comandos do PowerShell, faça o seguinte:
  - Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada `diskEncryptionSetID` no comando `New-provScheme`. Por exemplo:

```
1 Novo-ProvScheme -CleanOnBoot -CustomProperties '<
   CustomProperties xmlns="http://schemas.citrix.com/2014/
   xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />
3 <Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
5 </CustomProperties>'
6 -HostingUnitName "Redigido"
7 -IdentityPoolName "Redigido"
8 -InitialBatchSizeHint 1
9 -MasterImageVM "Redigido"
10 -NetworkMapping @{
11 "0"="Redigido" }
12
13 -ProvisioningSchemeName "Redigido"
14 -ServiceOffering "Redigido"
```

- Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `New-provScheme`. Por exemplo:

```
1 Novo-ProvScheme -CleanOnBoot
2 -HostingUnitName azure-east
3 -IdentityPoolName aio-ip
4 -InitialBatchSizeHint 1
5 -MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
6 -NetworkMapping @{
7 "0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
   }
8
9 -ProvisioningSchemeName aio-test
10 -MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
```

5. Conclua a criação do 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/](https://docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/). Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

### Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina) somente se o catálogo não tiver sido criptografado anteriormente.

- Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada `diskEncryptionSetID` no comando `Set-provScheme`. Por exemplo:

```
1 Definir-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
4 </CustomProperties>'
```

- Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `Set-provScheme`. Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
   XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
```

Depois de bem-sucedidas, todas as novas VMs que você adiciona ao seu catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

### Verificar se o catálogo está criptografado duas vezes

- No Web Studio:
  1. Navegue até **Machine Catalogs**.
  2. Selecione o catálogo que você deseja verificar. Clique na guia **Template Properties** localizada na parte inferior da tela.
  3. Em **Azure Details**, verifique o ID do conjunto de criptografia de disco em **Disk Encryption Set**. Se o ID do DES do catálogo estiver em branco, o catálogo não está criptografado.
  4. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.
- Usando o comando do PowerShell:



1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos à Citrix.
3. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

```
1 Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

4. Recupere a propriedade personalizada DES Id do catálogo da máquina. Por exemplo:

```
1 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
  Value="/subscriptions
  /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
  -RG/providers/Microsoft.Compute/diskEncryptionSets/
  SampleEncryptionSet" />
```

5. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.

## 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` estiver definida como **false** ou se um valor não for especificado, todos os VDAs provisionados continuarão usando um disco do sistema operacional provisionado.

Veja a seguir um exemplo de conjunto de propriedades personalizadas que devem ser usadas no esquema de provisionamento:

```
1 "CustomProperties": [  
2     {  
3  
4         "Nome": "UseManagedDisks",  
5         "Valor": "true"  
6     }  
7 ,  
8     {  
9  
10        "Nome": "StorageType",  
11        "Valor": "Standard_LRS"  
12    }  
13 ,  
14    {  
15
```

```
16         "Nome": "UseSharedImageGallery",
17         "Valor": "true"
18     }
19     ,
20     {
21         "Nome": "SharedImageGalleryReplicaRatio",
22         "Valor": "40"
23     }
24     ,
25     {
26         "Nome": "SharedImageGalleryReplicaMaximum",
27         "Valor": "10"
28     }
29     ,
30     {
31         "Nome": "LicenseType",
32         "Valor": "Windows_Server"
33     }
34     ,
35     {
36         "Nome": "UseEphemeralOsDisk",
37         "Valor": "true"
38     }
39     ],
```

### Configurar um disco efêmero para um catálogo

Para configurar um disco de sistema operacional temporário do Azure para um catálogo, use o parâmetro `useEphemeralOsDisk` em `Set-provScheme`. Defina o valor do parâmetro `useEphemeralOsDisk` como **true**.

#### Observação:

Para usar esse recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-do-catálogo -
   CustomProperties <CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
   />
```

```
3 <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value="
  "true" />
4 <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
  "true" />
5 </CustomProperties>'
```

### Considerações importantes para discos efêmeros

Para provisionar discos de sistema operacional efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve oferecer suporte a discos de SO efêmeros.
- O tamanho do cache ou disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco de SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também esses problemas nas seguintes situações:

- Criação do esquema de provisionamento.
- Modificação do esquema de provisionamento.
- Atualização da imagem.

### Hosts dedicados do Azure

Você pode usar o MCS para provisionar VMs em hosts dedicados do Azure. Antes de provisionar VMs em hosts dedicados do Azure:

- Crie um grupo de hosts.
- Crie hosts nesse grupo de hosts.
- Verifique se há capacidade de host suficiente reservada para a criação de catálogos e máquinas virtuais.

Você pode criar um catálogo de máquinas com locação de host definida por meio do seguinte script do PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
  xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
  ="http://www.w3.org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="HostGroupId" Value="
  myResourceGroup/myHostGroup" />
3 ...outras propriedades personalizadas...
4 </CustomProperties>
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade de catálogo e não pode ser alterado depois que o catálogo é criado. Atualmente, a locação dedicada não é suportada no Azure.
- É necessário um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, ao usar o parâmetro `HostGroupID`.
- É necessário o posicionamento automático do Azure. Essa funcionalidade faz uma solicitação para integrar a assinatura associada ao grupo de hosts. Para obter mais informações, consulte [Conjunto de escala de VM em hosts dedicados do Azure - Pré-visualização pública](#). Se o posicionamento automático não estiver habilitado, o MCS emitirá um erro durante a criação do catálogo.

## Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure

Ao selecionar uma imagem a ser usada para criar um catálogo de máquina, você pode selecionar imagens criadas na Galeria de Computação do Azure.

Para que essas imagens apareçam, você deve:

1. Configurar um site do Citrix Virtual Apps and Desktops.
2. Conectar-se ao Azure Resource Manager.
3. No portal do Azure, criar um grupo de recursos. Para obter detalhes, consulte [Criar uma Galeria de 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 da imagem, crie uma versão da 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 do PowerShell específicos à Citrix.
3. Selecione um grupo de recursos e liste todas as galerias do grupo de recursos.

```
1 Get-ChildItem -LiteralPath @"(XDHyp:\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resourcegroup)"
```

4. Selecione uma galeria e liste todas as definições de imagem da galeria.

```
1 Get-ChildItem -LiteralPath @"(XDHyp:\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resourcegroup\sharedImageGallery.sharedimagegallery)"
```

5. Selecione uma definição de imagem e liste todas as versões da definição de imagem.

```
1 Get-ChildItem -LiteralPath @"(\"XDHyp:\HostingUnits\testresource\  
image.folder\sharedImageGalleryTest.resourcegroup\  
sharedImageGallery.sharedimagegallery\sigtestimage.  
imagedefinition")
```

6. Crie e atualize um catálogo MCS usando os seguintes elementos:

- Resource group
- Gallery
- Gallery image definition
- Gallery image version

Para obter informações sobre como criar um catálogo usando o SDK remoto do PowerShell, 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 Compartilhada. Use o comando `Set-ProvScheme` para ativar ou desativar esse recurso em um esquema de provisionamento e alterar a proporção da réplica e os valores máximos da réplica.

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para dar 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 estiver definida, o valor padrão será **False**.

### `SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas de versão de imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não estiver definida, os valores padrão serão usados. O valor padrão para discos de SO permanentes é 1000 e o valor padrão para discos de SO não persistentes é 40.

### `SharedImageGalleryReplicaMaximum`

- Define o número máximo de réplicas para cada versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.

- Se a propriedade não estiver definida, o valor padrão será 10.
- Atualmente, o Azure oferece suporte a até 10 réplicas para uma versão única de imagem de galeria. Se a propriedade for definida com um valor maior do que o suportado pelo Azure, o MCS tentará usar o valor especificado. O Azure gera um erro, que registra o MCS deixa a contagem de réplicas atual inalterada.

**Dica:**

Ao usar a Galeria de Imagens Compartilhadas para armazenar uma imagem publicada para catálogos provisionados do MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na proporção de réplicas e no máximo de réplicas. A contagem de réplicas é calculada dividindo-se o número de máquinas no catálogo pela taxa de réplica (arredondando para o valor inteiro mais próximo) e, em seguida, limitando o valor à contagem máxima de réplicas. Por exemplo, com uma taxa de réplica de 20 e um máximo de 5, 0 a 20 máquinas têm uma réplica criada, 21 a 40 têm 2 réplicas, 41 a 60 têm 3 réplicas, 61 a 80 têm 4 réplicas, mais de 81 têm 5 réplicas.

**Caso de uso: Atualizando a taxa de réplica da Galeria de Imagens Compartilhadas e o máximo de**

O catálogo de máquinas existente usa a Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para atualizar as propriedades personalizadas de todas as máquinas existentes no catálogo e de quaisquer máquinas futuras:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-do-catálogo -
  CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
  /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance"> <Property xsi:type="StringProperty" Name="
  StorageType" Value="Standard_LRS"/> <Property xsi:type="
  StringProperty" Name="UseManagedDisks" Value="True"/> <Property xsi:
  type="StringProperty" Name="UseSharedImageGallery" Value="True"/> <
  Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio
  " Value="30"/> <Property xsi:type="IntProperty" Name="
  SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

**Caso de uso: convertendo um catálogo de instantâneos em um catálogo da Galeria de Imagens Compartilhadas**

Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.

2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-do-catálogo -  
   CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com  
/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/  
XMLSchema-instance"> <Property xsi:type="StringProperty" Name="  
StorageType" Value="Standard_LRS"/> <Property xsi:type="  
StringProperty" Name="UseManagedDisks" Value="True"/> <Property xsi:  
type="StringProperty" Name="UseSharedImageGallery" Value="True"/> <  
Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio  
" Value="30"/> <Property xsi:type="IntProperty" Name="  
SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

**Dica:**

Os parâmetros `sharedImageGalleryReplicaRatio` e `sharedImageGalleryReplicaMaximum` não são necessários. Depois que o comando `Set-ProvScheme` for concluído, a imagem da Galeria de Imagens Compartilhadas ainda não foi criada. Depois que o catálogo estiver configurado para usar a galeria, a próxima operação de atualização do catálogo armazenará a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. O ciclo de energia das máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Imagens Compartilhadas e todas as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente dentro de algumas horas.

**Caso de uso: conversão de um catálogo da galeria de imagens compartilhadas em um catálogo de instantâneos**

Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-do-catálogo -  
   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 de cada máquina ainda não foram atualizados para refletir as novas propriedades personalizadas. Execute o comando a seguir para ver as propriedades personalizadas originais da Galeria de Imagens Compartilhada: `Get-ProvVM -ProvisioningSchemeName catalog-name`. Depois que o comando `Set-ProvScheme` for concluído, o instantâneo da imagem ainda não foi criado. Depois que o catálogo estiver configurado para não usar a galeria, a próxima operação de atualização do catálogo armazenará a imagem publicada como um instantâneo. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o instantâneo e todas as máquinas recém-provisionadas são criadas a partir do instantâneo. O ciclo de inicialização das máquinas as atualiza. Nesse momento, 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 do Azure. Você pode conseguir isso usando o PowerShell.

**Observação:**

Se nenhuma zona for especificada, o MCS permitirá que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribuirá aleatoriamente as máquinas entre elas.

## Configurar zonas de disponibilidade por meio do PowerShell

Usando o PowerShell, você pode visualizar os itens de inventário da oferta usando `Get-Item`. Por exemplo, para ver a oferta de serviço *da região leste dos EUA standard\_B1LS*:

```
1 $serviceOffering = Get-Item -path "XDHyp:\Conexões\nome-da-minha-
conexão\Leste dos EUA.região\oferta_de_serviços.pasta\B1ls_Padrão.
oferta_de_serviços"
```

Para visualizar as zonas, use o parâmetro `additionalData` para o item:

```
$serviceOffering.Dados Adicionais
```



Se as zonas de disponibilidade não forem especificadas, não haverá alteração na forma como as máquinas são provisionadas.

Para configurar as zonas de disponibilidade por meio do PowerShell, use a propriedade personalizada **Zones** disponível com a operação `New-ProvScheme`. A propriedade **Zones** define uma lista de zonas de disponibilidade para provisionar máquinas. Essas zonas podem incluir uma ou mais zonas de disponibilidade. Por exemplo, `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` para as zonas 1 e 3.

Use o comando `Set-provScheme` para atualizar as zonas de um esquema de provisionamento.

Se for fornecida uma zona inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro será exibida fornecendo instruções sobre como corrigir o comando inválido.

**Dica:**

Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e será exibida uma mensagem de erro relevante.

## Tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes do Azure que usam o MCS. Para VMs de destino, o MCS oferece suporte a:

- Disco de SO: SSD, SSD ou HDD premium
- Disco de cache de gravação: SSD, SSD ou HDD premium

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM oferece suporte ao tipo de armazenamento selecionado.
- Se sua configuração usar um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

**Dica:**

`StorageType` está configurado para um tipo de sistema operacional e uma conta de armazenamento. O `wbcDiskStorageType` está configurado para o tipo de armazenamento em cache de write-back. Para um catálogo normal, é necessário `StorageType`. Se o `wbcDiskStorageType` não estiver configurado, o `StorageType` será usado como padrão para `wbcDiskStorageType`.

Se `WBCDiskStorageType` não estiver configurado, `StorageType` será usado como padrão para `WBCDiskStorageType`.

## Configurar tipos de armazenamento

Para configurar os tipos de armazenamento para a VM, use o parâmetro `StorageType` em `New-provScheme`. Defina o valor do parâmetro `StorageType` como um dos tipos de armazenamento suportados.

Veja a seguir um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
1 Set-ProvScheme -ProvisioningSchemeName nome-do-catálogo -  
   CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com  
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/  
   XMLSchema-instance">  
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"  
   />  
3 <Property xsi:type="StringProperty" Name="StorageType" Value="  
   Premium_LRS" />  
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="  
   Windows_Client" />  
5 </CustomProperties>'
```

## Habilitar o armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica de forma síncrona seu disco gerenciado do Azure em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium\_ZRS** e **StandardSSD\_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser definido usando propriedades personalizadas existentes ou por meio do modelo **MachineProfile**. O armazenamento ZRS também é suportado com o comando `Set-ProvVmUpdateTimeWindow` com os parâmetros `-StartSnow` e `-DurationInMinutes -1`, e você pode alterar a máquina existente de armazenamento LRS para ZRS.

### Limitações:

- Compatível somente com discos gerenciados
- Compatível apenas com unidades de estado sólido (SSD) premium e standard
- Não compatível com `StorageTypeAtShutdown`
- Disponível somente em determinadas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em grande escala. Portanto, para a primeira ativação, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

## Defina o armazenamento com redundância de zona como o tipo de armazenamento em disco

Você pode selecionar armazenamento com redundância de zona durante a criação do catálogo inicial

ou atualizar seu tipo de armazenamento em um catálogo existente.

**Selecionar armazenamento com redundância de zona usando comandos do PowerShell** Ao criar um novo catálogo no Azure usando o comando `New-ProvScheme` do PowerShell, use `Standard_ZRS` como o valor no `StorageAccountType`. Por exemplo:

```
1 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="StandardSSD_ZRS" />
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se ele pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso do ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks:** a propriedade personalizada `StorageTypeAtShutdown` não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion:** essa exceção ocorre se você tentar usar o Armazenamento ZRS em uma região do Azure que não oferece suporte a ZRS
- **ZrsRequiresManagedDisks:** você pode usar armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento em disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

#### Observação:

Durante a criação do catálogo, o disco do sistema operacional `StorageType` do perfil da máquina é usado se as propriedades personalizadas não estiverem definidas.

## Capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina enquanto cria um catálogo de máquinas, atualiza um catálogo de máquinas existente e atualiza as VMs existentes.

Você pode criar uma VM ou especificação de modelo como fonte de perfil de máquina.

### Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação de modelo.

- Storage account
  - Espaço de trabalho de análise de logs
  - Namespace do hub de eventos com preços de nível padrão
2. Crie uma fonte de perfil de máquina.
  3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize as VMs existentes.

### Configurar os IDs necessários no Azure

Configure uma das seguintes opções no Azure:

- Storage account
- Espaço de trabalho de análise de logs
- Namespace do hub de eventos com preços de nível padrão

**Configurar uma conta de armazenamento** Crie uma conta de armazenamento padrão no Azure. Na especificação do modelo, forneça o resourceID completo da conta de armazenamento como `storageAccountID`.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, eles podem ser encontrados no contêiner `insights-metrics-pt1m`.

**Configurar um espaço de trabalho de análise de logs** Crie um espaço de trabalho de análise de logs. Na especificação de modelo, forneça o resourceId completo para o espaço de trabalho de análise de logs como `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 | resumir Count=count()por ResourceId
```

**Configurar um hub de eventos** Faça o seguinte para configurar um hub de eventos no portal do Azure:

1. Crie um namespace de hub de eventos com o preço de nível padrão.
2. Crie um hub de eventos abaixo do namespace.
3. Navegue até **Capturar** no hub de eventos. ATIVE o seletor 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 fonte de perfil de máquina**

Você pode criar uma VM ou especificação de modelo como fonte 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, primeiro defina as configurações de diagnóstico na própria VM de 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 à NIC:

```
1 lista de configurações de diagnóstico do monitor az --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
1 lista de configurações de diagnóstico do monitor az --resource-group matspo --resource matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

**Criar um modelo de perfil de máquina baseado em especificações 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 do ARM, essas configurações não serão incluídas automaticamente no modelo. Você deve adicionar ou modificar manualmente as configurações de diagnóstico no modelo do ARM.

No entanto, se você quiser uma VM como perfil de sua máquina, o MCS garante que as configurações críticas de diagnóstico sejam capturadas e aplicadas com precisão aos recursos em seu catálogo do 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 obter o escopo, faça referência a

uma VM ou NIC que esteja no modelo pelo nome com uma ID parcial. Por exemplo, para criar configurações de diagnóstico anexadas a uma VM chamada test-VM na especificação de modelo, especifique o escopo como:

```
1 "escopo": "microsoft.compute/virtualMachines/test-VM",
```

3. Use a especificação de modelo como uma fonte de perfil de máquina.

### Criar ou atualizar um catálogo com configurações de diagnóstico

Depois de criar uma fonte 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 as VMs existentes usando o comando `request-ProvVmUpdate`.

### Localização do arquivo de paginação

Em ambientes do Azure, o arquivo de paginação é configurado no local apropriado quando a VM é criada. A configuração do arquivo de paginação é definida no formato `<page file location> [tamanho mínimo] [tamanho máximo]` (o tamanho está em MB). Para obter mais informações, consulte o documento da Microsoft [Como determinar o arquivo de paginação apropriado](#).

Quando você cria `ProvScheme` durante a preparação da imagem, o MCS determina a localização do arquivo de página com base em certas regras. Depois de criar `ProvScheme`:

- A alteração do tamanho da VM será bloqueada se o tamanho da VM de entrada fizer com que a configuração do arquivo de paginação seja diferente.
- A atualização do perfil da máquina será bloqueada se a oferta de serviço for alterada devido à atualização do perfil da máquina que faz com que a configuração do arquivo de paginação seja diferente.
- As propriedades do disco do SO efêmero (EOS) e MCSIO não podem ser alteradas.

### Determinação da localização do arquivo de paginação

Os recursos como EOS e MCSIO têm seu próprio local de arquivo de paginação esperado e são exclusivos entre si. A tabela mostra a localização esperada do arquivo de paginação para cada recurso:

Recurso	Local esperado do arquivo de paginação
EOS	Disco do sistema operacional

Recurso	Local esperado do arquivo de paginação
MCSIO	Disco temporário do Azure primeiro, caso contrário, disco de cache de write-back

**Observação:**

Mesmo que a preparação da imagem seja dissociada da criação do esquema de provisionamento, o MCS determina corretamente o local do arquivo de paginação. O local padrão do arquivo de paginação é o disco do SO.

**Cenários de configuração do arquivo de paginação**

A tabela descreve alguns cenários possíveis de configuração do arquivo de paginação durante a preparação da imagem e a atualização do esquema de provisionamento:

Durante	Cenário	Resultado
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco temporário, enquanto o tamanho da VM especificado no esquema de provisionamento não tem disco temporário	O arquivo de paginação é colocado no disco do SO
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco do SO, enquanto o tamanho da VM especificado no esquema de provisionamento tem disco temporário.	O arquivo de paginação é colocado no disco temporário.
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco temporário, enquanto o disco de SO efêmero é ativado no esquema de provisionamento.	O arquivo de paginação é colocado no disco do SO

Durante	Cenário	Resultado
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento, o tamanho original da VM tem disco temporário e a VM de destino não tem disco temporário.	Rejeita a alteração com uma mensagem de erro
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento, o tamanho original da VM não tem disco temporário e a VM de destino tem disco temporário	Rejeita a alteração com uma mensagem de erro

### Atualizar configuração do arquivo de página

Você também pode especificar a configuração do arquivo de paginação, incluindo o local e o tamanho, usando explicitamente o comando do the PowerShell. Isso substitui o valor determinado pelo MCS. Você pode fazer isso executando o comando `New-ProvScheme` incluindo as seguintes propriedades personalizadas:

- `PageFileDiskDriveLetterOverride`: Letra da unidade de disco de localização do arquivo de página
- `initialPageFileSizeInMB`: Tamanho inicial do arquivo da página em MB
- `MaxPageFileSizeInMB`: Tamanho máximo do arquivo de página em MB

Exemplo de uso das propriedades personalizadas:

```

1 -Propriedades Personalizadas '<CustomProperties xmlns=" http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org
   /2001/XMLSchema-instance"> `
2 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
3 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
4 <Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
5 <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
6 <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196"/> `
7 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
8 <Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
9 </CustomProperties>'

```



#### Restrições:

- Você pode atualizar a configuração do arquivo de paginação somente ao criar o esquema de provisionamento executando o comando `New-provScheme` e a configuração do arquivo de página não pode ser alterada posteriormente.
- Forneça todas as propriedades relativas da configuração do arquivo de página (`PageFileDiskDriveLetter`, `initialPageFileSizeInMB` e `MaxPageFileSizeInMB`) nas propriedades personalizadas ou não forneça nenhuma delas.
- 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.
- Esse recurso não é compatível com o Web Studio.

### Criar um catálogo usando VMs do Azure Spot

As VMs do Azure Spot permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa. No entanto, a capacidade de alocar uma VM do Azure Spot depende da capacidade e do preço atuais. Portanto, o Azure pode expulsar sua VM em execução, falhar ao criar a VM ou não ligar a VM de acordo com a [política de despejo](#). Portanto, as VMs do Azure Spot são boas para alguns aplicativos e áreas de trabalho não críticos. Para obter mais informações, consulte [Usar máquinas virtuais do Azure Spot](#).

#### Limitações

- Nem todos os tamanhos de VM são compatíveis com as VMs do Azure Spot. Para obter mais informações, consulte [Limitações](#).

Você pode executar o seguinte comando do PowerShell para verificar se um tamanho de VM oferece suporte a VMs do Spot ou não. Se um tamanho de VM suportar Spot VM, então `SupportsSpotVM` é **True**.

```
1 (Obter-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering"). Dados Adicionais
```

- Atualmente, as VMs do Azure Spot não oferecem suporte à hibernação.

#### Requisito

Ao criar a fonte do perfil de máquina (especificação de VM ou modelo) para o catálogo de VMs do Azure Spot, você deve selecionar Azure Spot Instance (se estiver usando VM) ou definir `priority`

como **Spot** (se estiver usando a especificação do modelo).

## Etapas para criar um catálogo usando VMs do Azure Spot

1. Criar uma fonte de perfil de máquina (VM ou modelo de inicialização).

- Para criar uma VM usando o portal do Azure, consulte [Implantar máquinas virtuais do Azure Spot usando o portal do Azure](#).
- Para criar uma especificação de modelo, adicione as seguintes propriedades em **resources > type: Microsoft.compute/VirtualMachines > properties** na especificação do modelo. Por exemplo:

```
“
“prioridade”: “Local”,
“evictionPolicy”: “Desalocar”,
“billingProfile”: {
“maxPrice”: 0,01
```

```
}
““
```

```
1 > **Observação:**
2 >
3 > - A política de despejo pode ser **Desalocar** ou **Excluir**.
4 >   - Para VMs não persistentes, o MCS sempre define a política de
despejo como **Excluir**. Se a VM for despejada, ela será excluída
junto com todos os discos não persistentes (por exemplo, disco do
sistema operacional). Nenhum disco permanente (por exemplo, disco de
identidade) não é excluído. No entanto, um disco do sistema
operacional é persistente se o tipo de catálogo for persistente ou
se a propriedade personalizada `PersistosDisk` estiver definida como
True. Da mesma forma, um disco WBC é persistente se a propriedade
personalizada `PersistWBC` estiver definida como **True**.
5 >   - Para VMs persistentes, o MCS sempre define a política de
despejo como Desalocar. Se a VM for despejada, ela será desalocada.
Nenhuma alteração é feita nos discos.
6 > - O preço máximo é o preço que você está disposto a pagar por hora.
Se você estiver usando Somente capacidade, isso será -1. O
preço máximo só pode ser nulo, -1 ou um decimal maior que zero. Para
obter mais informações, consulte [Preços](https://learn.microsoft.
com/pt-br/azure/virtual-machines/spot-vm#pricing).
```

1. Você pode executar o seguinte comando do PowerShell para verificar se um perfil de máquina está habilitado para a VM do Azure Spot ou não. Se o parâmetro **SpotEnabled** for **True** e **SpotEvictionPolicy** estiver definido como **Deallocate** ou **Delete**, o perfil da máquina estará habilitado para Azure Spot VM. Por exemplo,

- Se a fonte do perfil de máquina for uma VM, execute o seguinte comando:

```
1 (Obter-Item "XDHyp:\HostingUnits\azure-res-conn2\
machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
delete.vm").Dados Adicionais
```

- Se a fonte do perfil de máquina for uma especificação de modelo, execute o seguinte comando:

```
1 (Obter-Item "XDHyp:\HostingUnits\azure-res-conn2\
machineprofile.folder\fifthcolumn.resourcegroup\fc-neh-
templatespec.templatespec\14.0.0-spot-delete.
templatespecversion").Dados Adicionais
```

2. Crie um catálogo de máquinas usando um perfil de máquina com o comando `New-ProvScheme PowerShell`.

Você pode atualizar um catálogo usando o comando `Set-provScheme`. Você também pode atualizar as VMs existentes usando o comando do PowerShell `Set-ProvVmUpdateTimeWindow`. O perfil de máquina é atualizado na próxima inicialização.

### Despejos em uma VM do Azure Spot em execução

Se a capacidade de computação não estiver disponível ou o preço por hora for maior do que o preço máximo conforme configurado, o Azure despejará uma VM do Spot em execução. Por padrão, você não é notificado sobre um despejo. A VM simplesmente congela e é despejada. A Microsoft recomenda o uso de eventos agendados para monitorar despejos. Consulte [Monitorar continuamente o despejo](#). Você também pode executar scripts em uma VM para receber uma notificação antes do despejo. Por exemplo, a Microsoft tem um script de pesquisa em [ScheduledEvents.cs](#) do Python.

### Solução de problemas

- Você pode ver as propriedades da VM Spot nos CustomMachineData da VM provisionada usando o comando `Get-ProvVM`. Se o campo de prioridade estiver definido como **Spot**, o Spot estará em uso.
- Você pode verificar se uma VM está usando o Spot no Portal do Azure:
  1. Encontre a VM no Portal do Azure.
  2. Acesse a página **Visão geral**.
  3. Role até a parte inferior e localize a seção **Azure Spot**.
    - Se o Spot não estiver em uso, esse campo estará vazio.

- Se o Spot estiver em uso, os campos **Azure Spot** e **Política de despejo do Azure Spot** serão definidos.

1. Você pode verificar o perfil de cobrança ou o preço máximo por hora da VM na página Configuração.

## Configurar tamanhos de VM de backup

Às vezes, as nuvens públicas podem ficar sem capacidade para um tamanho específico de VM. Além disso, se você usar VMs do Azure Spot, as VMs serão removidas a qualquer momento com base nas necessidades de capacidade do Azure. Nesse caso de capacidade insuficiente no Azure ou de falha na alimentação de uma VM do 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 usar os tamanhos das VMs de backup na ordem fornecida por você na lista.

Quando o MCS usa uma configuração de backup específica para a VM, ele continua usando 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 inicializar novamente uma configuração de tamanho de VM de backup conforme a lista.

Esse recurso tem suporte para:

- um catálogo que usa um perfil de máquina
- catálogos de máquinas do MCS persistentes e não persistentes
- ambientes do Azure atualmente

## Considerações importantes

- Você pode fornecer mais de um tamanho de VM de backup na lista.
- A lista deve ser exclusiva.
- Você pode adicionar a propriedade do tipo de instância para cada uma das VMs na lista. O tipo é **Spot** ou **Regular**. Se o tipo não for especificado, o MCS considerará a VM como **Regular**.
- Você pode alterar a lista de tamanhos de VM de backup de um catálogo existente usando os comandos `Set-ProvScheme` do PowerShell.
- 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 tamanhos de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVmUpdateTimeWindow` e inicie as VMs dentro da janela. Se o comando `Set-ProvVM`

for usado em uma VM, a VM continuará usando a lista de tamanhos 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

### Observação:

Para resolver o problema do congelamento da interface do usuário do Studio, substitua todas as aspas simples por `&quot;`; ao executar os comandos do PowerShell.

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos à Citrix.
3. Crie um catálogo de agentes. Esse catálogo é preenchido com máquinas que estão prestes a ser criadas.
4. Crie um pool de identidades. Isso se torna um contêiner para contas do AD criadas para as máquinas que serão criadas.
5. Crie um esquema de provisionamento com o perfil de 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 as VMs existentes

Você pode atualizar as VMs existentes em um catálogo usando o comando `Set-ProvVmUpdateTimeWindow` do PowerShell. O comando atualiza as VMs criadas a partir do esquema de provisionamento associado ao catálogo na próxima inicialização dentro da janela de tempo especificada. Por exemplo:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "12/03/2022 03:00"-DurationInMinutes 60`
- `Definir-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

**Observação:**

`StartSnow` indica a hora de início programada. `DurationInMinutes` é a janela de tempo da programação.

Você pode configurar a lista de tamanhos de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVmUpdateTimeWindow` e inicie as VMs dentro da janela. Por exemplo:

1. Execute o comando `Set-provVM` para configurar a lista de tamanhos de VM de backup para uma VM MCS existente selecionada. Por exemplo:

```

1 Set-ProvVM -ProvisioningSchemeName "nome" -VMName "Vm-001"
2 -CustomProperties
3 "<CustomProperties xmlns='http://schemas.citrix.com/2014/xd/
   machinecreation' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
   instance'">
4 <Property xsi:type='\"StringProperty\"' Name='\"UseManagedDisks\"'
   Value='\"true\"' />
5 <Property xsi:type='\"StringProperty\"' Name='\"StorageAccountType\"'
   Value='\"Premium_LRS\"' />
6 <Property xsi:type='\"StringProperty\"' Name='\"LicenseType\"' Value='\"
   Windows_Server\"'/>
7 <Property xsi:type='\"StringProperty\"' Name='\"PersistWBC\"' Value='\"
   true\"'/>
8 <Property xsi:type='\"StringProperty\"' Name='\"BackupVmConfiguration
   \"' Value='\"[{
9   &quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;; &quot;
   Type&quot;: &quot;Spot&quot;; }
10  , {
11  &quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;;, &quot;
   Type&quot;: &quot;Regular&quot;; }
12  , {
13  &quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;;, &quot;
   Type&quot;: &quot;Spot&quot;; }
14  ]\"'/>
15 </CustomProperties>"

```

2. Execute o comando `Set-ProvVmUpdateTimeWindow` para aplicar as atualizações. Por exemplo:

```

1 Definir-ProvVmUpdateTimeWindow -ProvisioningSchemeName azure-
   catalog -StartsNow -DurationInMinutes 60

```

**Copiar marcas em todos os recursos**

Você pode copiar marcações especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do sistema operacional, disco de identidade e disco de cache de write-

back) de uma nova VM ou de uma VM existente em um catálogo de máquinas. A origem do perfil da máquina pode ser uma especificação de modelo de ARM ou VM.

**Observação:**

Você deve adicionar a política nas marcações (consulte [Atribuir definições de política para conformidade de marca](#)) ou adicionar as marcações em uma origem de perfil de máquina para reter as marcações nos recursos.

**Pré-requisitos**

Crie a origem do perfil da máquina (especificação do modelo de ARM ou VM) para ter marcações na VM, nos discos e nas NICs dessa VM.

- Se você quiser ter uma VM como entrada de perfil de máquina, aplique as marcações na VM e em todos os recursos no portal do Azure. Consulte [Aplicar marcas com o portal do Azure](#).
- Se você quiser ter a especificação do modelo ARM como uma entrada de perfil de máquina, adicione o seguinte bloco de marcações sob cada recurso.

```
““  
  “tags”: {  
    “TagC”: “Valor3”  
  },  
““
```

**Observação:**

Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

**Copiar marcações para os recursos de uma VM em um novo catálogo de máquinas**

1. Crie um catálogo não persistente ou persistente com uma especificação de modelo de ARM ou VM como a entrada do perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

**Observação:**

Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidas no perfil da máquina e o número de NICs que você deseja que as VMs usem.

## Modificar marcações nos recursos de uma VM existente

1. Crie um perfil de máquina com as marcações em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
1 Definir-ProvScheme -NomeDoEsquemaDeProvisionamento <
   YourCatalogName> -PerfilDaMáquina <PathToYourMachineProfile>
```

3. Desative a VM na qual você deseja aplicar as atualizações.
4. Solicite uma atualização agendada para a VM. Por exemplo:

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
   YourCatalogName> -VMName machine1 -StartsNow -
   DurationInMinutes -1
```

5. Ligue a VM.
6. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes.

### Observação:

Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidos no perfil da máquina e o número de NICs fornecidos no `Set-ProvScheme`.

## O que fazer a seguir

- Se este for o primeiro catálogo criado, o Web Studio orientará você 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

- [Crie e gerencie conexões e recursos](#)
- [Conexão com o Microsoft Azure Resource Manager](#)
- [Criar catálogos de máquinas](#)



## Gerenciar catálogos de máquinas

January 24, 2025

### Nota:

Você pode gerenciar a 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 abrange somente 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, upgrades do sistema operacional ou alterações de configuração.

- Catálogos contendo 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 com eficiência um grande número de máquinas de usuários.
- Para catálogos contendo máquinas estáticas, atribuídas permanentemente, e para catálogos de máquinas de acesso remoto ao PC, você gerencia as atualizações nas máquinas dos usuários fora do Web Studio. Execute essa tarefa individual ou coletivamente usando ferramentas de distribuição de software de terceiros.

Para obter informações sobre como criar e gerenciar conexões para hospedar hipervisores, 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 preexistentes continuam

usando 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 os catálogos de discos permanentes, as máquinas preexistentes não são atualizadas para a nova imagem, mas todas as novas máquinas adicionadas ao catálogo usam a nova imagem.
- Para catálogos de discos não permanentes, a imagem da máquina é atualizada na próxima vez em que a máquina for reiniciada.
- Com catálogos de máquinas persistentes, a atualização da imagem também atualiza as instâncias do catálogo que a usam.
- 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

### Use o Web Studio

Esta seção detalha como você pode gerenciar catálogos usando 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](#)
- [Excluir um catálogo](#)
- [Gerenciar contas de computador do Active Directory em um catálogo](#)
- [Atualizar um catálogo](#)
- [Alterar o nível funcional ou desfazer a alteração](#)
- [Clonar um catálogo](#)
- [Organize catálogos usando pastas](#)

### 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 esse 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 para um usuário aleatoriamente.
Tipo de máquina	Definido neste campo, as máquinas no catálogo são alocadas. Os valores possíveis incluem: Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: Descartar. Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: No disco local
Contagem de máquinas	Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: Descartar. Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: No disco local
Contagem alocada	Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: Descartar. Tipo de sistema operacional: sistema operacional multissessão (virtual); Dados do usuário: No disco local
Pasta	Operacional de sessão única (virtual) Machine Catalogs. No disco local, 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 de atualização do VDA. Os valores possíveis incluem: Não configurado, agendado, disponível e atualizado.
Status da imagem	O status de atualização da imagem do catálogo. Aplicável somente a catálogos de máquinas não persistentes. Os valores possíveis incluem: Totalmente atualizado, Parcialmente atualizado, Atualizações pendentes, Preparação

## 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.
- Verifique se você tem 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 usa o Web Studio para criar contas de computador do Active Directory para as máquinas adicionais, você deve ter a permissão apropriada de administrador de domínio.

Para adicionar máquinas a um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar máquinas** na barra de ação.
4. Selecione o número de máquinas virtuais a serem adicionadas.
5. Se não houver contas existentes do Active Directory suficientes para o número de VMs que você está adicionando, selecione o domínio e o local em que as contas serão criadas. Especifique um esquema de nomenclatura de contas usando marcas de hash para indicar onde os números ou letras sequenciais aparecem. Não use uma barra (/) em um nome de OU. 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 denominadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.
6. Se você usa contas existentes do Active Directory, navegue até as contas ou clique em **Importar** e especifique um arquivo.csv contendo nomes de contas. Verifique se 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 na criação de muitas máquinas. A criação da máquina 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 são 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 **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Exibir máquinas** na barra de ação.
4. Selecione uma ou mais máquinas e, em seguida, selecione **Excluir** na barra de ação.

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 foram mantidas, desativadas ou excluídas.

## Editar um catálogo

1. Na página **Descrição**, altere a descrição do catálogo.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Editar catálogo de máquinas** na barra de ação.
4. Na página **Scopes**, altere os escopos.
5. Você pode ver outras páginas dependendo do tipo de catálogo.

Para catálogos criados usando uma imagem do Azure Resource Manager, as páginas a seguir estão visíveis. Lembre-se de que as alterações feitas se aplicam somente às máquinas adicionadas posteriormente ao catálogo. As máquinas existentes permanecem inalteradas.

- Na página **Virtual Machines**, altere o tamanho da máquina e as zonas de disponibilidade em que você deseja criar máquinas.

### Nota:

- Somente os tamanhos de máquina que o catálogo suporta são mostrados.
- Se necessário, selecione **Mostrar somente tamanhos de máquinas usados em outros catálogos de máquinas** para filtrar a lista de tamanhos de máquinas.

- On the **Machine Profile** page, choose whether to use or change a machine profile.
- (Visible only when the catalog is configured with a dedicated group host) On the **Dedicated host group** page, choose whether to change a host group.
- On the **Storage and License Types** page, choose whether to change the storage type, license type, and Azure Computer Gallery settings (available only when **Place prepared image in Azure Gallery** is in use).

**Nota:**

Se a configuração recém-selecionada não suportar o tamanho atual da máquina, uma caixa de diálogo de aviso será exibida, informando que a alteração da configuração redefina a configuração do tamanho da máquina. Se você optar por continuar, um ponto vermelho aparecerá ao lado do menu **Virtual Machines**, solicitando que você selecione um novo tamanho de máquina.

- On the **License Type** page, choose whether to change the Windows license or Linux license setting.

Para catálogos do Remote PC Access, as seguintes páginas estão visíveis:

- On the **Power Management** page, change the power management settings and select a power management connection.
- Na página **Organizational Units**, adicione ou remova OUs do Active Directory.

6. 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 **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Renomear catálogo de máquinas** na barra de ação.
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, diferente do hipervisor que contém as VMs nesse catálogo, afeta o desempenho.

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Move** na barra de ação.
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 estão desconectados e você não executa nenhuma sessão desconectada.
- O modo de manutenção é ativado para todas as máquinas no catálogo para que novas conexões não possam ser feitas.
- Todas as máquinas do catálogo estão desligadas.
- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Excluir catálogo de máquinas** na barra de ação.
4. Indique se as máquinas no catálogo foram excluídas. Se você optar por excluir as máquinas, indique se as contas de computador do Active Directory para essas máquinas foram mantidas, desativadas 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 dos catálogos de sistemas operacionais de sessão única e sistemas operacionais de várias sessões. Essas contas podem então ser usadas para outras máquinas.
- Adicione contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam em vigor. Não use uma barra (/) em um nome de OU.

Para gerenciar contas do Active Directory:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Gerenciar contas do AD** na barra de ação.
4. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas da conta: redefina-as todas ou insira uma senha que se aplique a todas as contas.

Você pode redefinir as 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 elas são importadas. Ao excluir uma conta, escolha se a conta no Active Directory será mantida, desativada ou excluída.

Indique se as contas do Active Directory são retidas, desativadas ou excluídas quando você remove máquinas de um catálogo ou exclui um catálogo.

## Atualizar um catálogo

Recomendamos que você salve cópias ou instantâneos das imagens mestras antes de atualizar as máquinas no catálogo. O banco de dados mantém um registro histórico das imagens mestras usadas em cada catálogo de máquinas. Reverta ou reverta máquinas em um catálogo para usar a versão anterior da imagem mestre. Execute essa 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 mestras. Você não pode reverter um catálogo para usá-los.

Depois que uma máquina é atualizada, ela é reiniciada automaticamente.

## Atualizar ou criar uma imagem mestre

Antes de atualizar o catálogo da máquina, 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. Esse instantâneo pode ser usado para reverter (reverter) 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 mestras de GPU, você pode alterar a imagem mestre somente por meio do console XenServer.

## Alterar a imagem mestre

Para preparar e implementar a atualização em todas as máquinas em um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Alterar imagem mestre** na barra de ação.
4. Na página **Image**, selecione o host e a imagem que você deseja lançar. > **Dica:** >> Para um catálogo criado pelo MCS, você pode anotar sua imagem adicionando uma nota à imagem. Uma



nota pode conter até 500 caracteres. Sempre que você altera a imagem mestre, uma entrada relacionada à nota é criada se 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 **Rollout Strategy**, escolha quando as máquinas no catálogo de máquinas serão atualizadas com a nova imagem mestre: no próximo desligamento ou imediatamente. > **Nota:** >> A página **Rollout Strategy** não está disponível para VMs persistentes porque a implantação só é aplicável a VMs não persistentes.
6. Verifique as informações na página **Summary** e clique em **Finish**. Cada máquina é reiniciada automaticamente após a atualização.

Para acompanhar o progresso da atualização, localize o catálogo em **Machine Catalogs** para ver a barra de progresso embutida 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 isso como uma alternativa para uma imagem ou um instantâneo de uma imagem.

#### **Estratégia de lançamento:**

A atualização de imagens no próximo desligamento afetará imediatamente qualquer máquina que não esteja em uso no momento, ou seja, máquinas que não tenham uma sessão de usuário ativa. Um sistema que está 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 com sistema operacional de sessão única, as máquinas são atualizadas imediatamente quando a máquina não está em uso ou quando os usuários não estão logados.
- Para um sistema operacional multissessão com máquinas secundárias, as reinicializações não ocorrem automaticamente. Para aplicar a imagem mestre atualizada, reinicie as máquinas usando o Studio, o PowerShell ou o Workspace. Reiniciar a partir das máquinas ou do hipervisor não aplica a atualização.

#### **Dica:**

Limite o número de máquinas que estão sendo reinicializadas usando as configurações avançadas para uma conexão de host. Use essas configurações para modificar as ações tomadas em um determinado catálogo; as configurações avançadas variam de acordo com o hipervisor.

## Reverter a imagem mestre

Depois de lançar uma imagem mestre atualizada ou nova, você pode revertê-la. Esse processo pode ser necessário se ocorrerem problemas com as máquinas recém-atualizadas. Quando você reverte, as máquinas no catálogo são revertidas para a última imagem em funcionamento. Quaisquer novos recursos que exijam a imagem mais recente não estão mais disponíveis. Assim como na implantação, a reversão de uma máquina inclui uma reinicialização.

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione o catálogo e, em seguida, selecione **Roll Back Master Image** na barra de ação.
4. Especifique quando aplicar a imagem mestre anterior às máquinas, conforme descrito na seção anterior para a operação de implantação.

A reversão é aplicada somente às máquinas que precisam ser revertidas. As máquinas que não estão atualizadas com a imagem mestre nova ou atualizada não recebem mensagens de notificação e não são forçadas a se desconectar.

Para acompanhar o progresso da reversão, localize o catálogo em **Machine Catalogs** para ver 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 de um catálogo de máquinas:

- Inicie as máquinas atualizadas para que elas se registrem no Controller. Esse processo permite que o Web Studio determine se as máquinas no catálogo precisam ser atualizadas.

Para alterar o nível funcional de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione o catálogo. A guia **Details** no painel inferior exibe informações sobre a 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 explica o porquê. Para garantir que todas as máquinas funcionem corretamente, a Citrix recomenda que você resolva os problemas da máquina antes de clicar em **Alterar** para continuar.

Depois que a alteração do catálogo for concluída, você poderá reverter as máquinas para suas versões anteriores do VDA selecionando o catálogo e selecionando **Undo Functional Level Change** na barra de ação.

## Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Você não pode alterar as configurações associadas ao sistema operacional e [machine management](#). 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. Entre no Web Studio e selecione **Machine Catalogs** no painel esquerdo.
  2. Selecione um catálogo e, em seguida, selecione **Clone** na barra de ação.
  3. Na janela **Clone Selected Machine Catalog**, visualize as configurações do catálogo clonado e defina-as conforme aplicável. Selecione **Próximo** para prosseguir para a próxima página.
  4. Na página **Summary**, veja um resumo das configurações e selecione **Finish** para iniciar a clonagem.
  5. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.

## Organize catálogos usando pastas

Você pode criar pastas para organizar catálogos e 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, primeiro planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas com até cinco níveis de profundidade (excluindo a pasta raiz padrão).
- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós no Web Studio (como os nós **Machine Catalogs** e **Applications**) 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 às pastas de primeiro nível em nós diferentes.

Para criar uma pasta de catálogo, siga estas etapas:

1. Selecione **Machine Catalogs** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar pasta** na barra **Action**.
3. Insira um nome para a nova pasta e clique em **Concluído**.

**Dica:**

Se você criar uma pasta em um local não desejado, poderá arrastá-la para o local correto.

### Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Machine Catalogs** no painel esquerdo.
2. Visualize os catálogos por pasta. Você também pode ativar **Exibir todos os** acima da hierarquia de pastas para visualizar todos os catálogos ao mesmo tempo.
3. Clique com o botão direito do mouse em um catálogo e selecione **Move Machine Catalog**.
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 catálogos

Você pode excluir, renomear e mover pastas do 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 **Machine Catalogs** 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 **Move Folder**.
3. Siga as instruções na tela para concluir as etapas restantes.

## Use o PowerShell

Esta seção detalha como você pode gerenciar catálogos usando o PowerShell:

- [Recupere avisos e erros associados a um catálogo](#)
- [Adicionar descrições a uma imagem](#)
- [Redefinir disco do sistema operacional](#)
- [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 em catálogo de máquinas baseado em perfil de máquina](#)
- [Reparar as informações de identidade das contas de computador ativas](#)
- [Alterar a configuração do cache em um catálogo de máquinas existente](#)
- [Suporte de atualização de VDA por meio de acesso ao compartilhamento de arquivos local](#)

## Recupere 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 os comandos do PowerShell, você pode:

- Obtenha uma lista de erros ou avisos
- Altere o estado de aviso de **Novo** para **Reconhecido**
- Exclua os erros ou avisos

Para executar os comandos do 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-ProOperationEvent`.

- Sem parâmetros: obtém todos os erros e avisos
- Com o parâmetro `LinkedObjectType` e `LinkedObjectId`: 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 esse ID de evento
- Com o parâmetro `Filter`: Obtém erros ou avisos por filtro personalizado

Para alterar o estado dos erros ou avisos de **Novo** para **Reconhecido**:

Execute o comando `Confirm-ProOperationEvent`.

- Com o parâmetro `EventID` : define o estado de um erro ou aviso específico que corresponde a esse ID de evento. Você pode obter o `EventID` de um erro ou aviso específico como saída do comando `Get-ProOperationEvent`
- Com os parâmetros `LinkedObjectType` e `LinkedObjectId` : 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-ProOperationEvent` .

- Com o parâmetro `EventID` : remove um erro ou aviso específico que corresponde a esse ID de evento. Você pode obter o `EventID` de um erro ou aviso específico como saída do comando `Get-ProOperationEvent`
- Com os parâmetros `LinkedObjectType` e `LinkedObjectId` : 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](#).

## Adicionar descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas às atualizações de imagens para catálogos de máquinas. Use esse recurso para adicionar uma descrição ao criar um catálogo ou ao atualizar uma imagem mestre existente para um catálogo. Você também pode exibir informações para cada imagem mestre no catálogo. Use os comandos a seguir para adicionar ou visualizar descrições de imagens:

- Para adicionar uma nota ao criar um catálogo de máquinas com uma imagem mestre, use o parâmetro `MasterImageNote` no comando `NewProvScheme` . Por exemplo:

```
1 C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
   HostingUnitName <name> -IdentityPoolName <name> -
   MasterImageVM
2 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:

```
1 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:

```
1 C:\PS>Get-ProvSchemeMasterVMImageHistory -
   ProvisioningSchemeName MyScheme -Showall
```

Para acompanhar o progresso da reversão, localize o catálogo em **Machine Catalogs** para ver a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em determinados cenários, incluindo os seguintes. (A opção **Roll Back Master Image** não 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 sistema operacional.
- O instantâneo usado para criar o catálogo foi corrompido.
- As alterações do usuário nas máquinas no catálogo não persistem.
- As máquinas do catálogo estão funcionando.

## Redefinir disco do sistema operacional

Use o comando do PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS. Atualmente, esse recurso é aplicável ao AWS, Azure, XenServer e Google Cloud. Ambientes de virtualização SCVMM e VMware.

Para executar com êxito o comando do PowerShell, 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 que o esquema de provisionamento tem entradas corretas.
- O hipervisor não está no modo de manutenção.
- As VMs de destino estão desligadas e em modo de manutenção.

Execute as seguintes etapas para redefinir o disco do sistema operacional:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix\*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando do PowerShell `Reset-ProvVMDisk` de qualquer uma das seguintes maneiras:
  - Especifique a lista de VMs como uma lista separada por vírgulas e execute a redefinição em cada VM:

```
1 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:

```
1 (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-
   ProvVMDisk "abc" -OS
```

- Especifique uma única VM pelo nome:

```
1 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 e verificação de conexão para cada VM.

```
1 Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
   -ProvisioningSchemeName "xxx" -OS
```

4. É exibido um prompt de confirmação que lista as VMs a serem redefinidas junto com uma mensagem de aviso de que é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma ação adicional será realizada.

**Nota:**

Não tire as VMs do modo de manutenção nem as ligue até a conclusão do processo de reinicialização.

Você pode executar o comando do PowerShell `-WhatIf` para imprimir a ação que ela executaria e sair sem executar a ação.

Você também pode ignorar o aviso de confirmação usando um dos seguintes métodos:

- Forneça o parâmetro `-Force`:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
   " -OS -Force
```

- Forneça o parâmetro `-Confirm:$false`:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
   " -OS -Confirm:$false
```

- Antes de executar o `Reset-ProvVMDisk`, altere `$ConfirmPreference` para **None**:

```
1 PS C:\Windows\system32> $ConfirmPreference='None'
2 PS C:\Windows\system32> $ConfirmPreference
3 None
4 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 de um esquema de provisionamento existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede.

### Nota:

Esse recurso é suportado no Citrix Virtual Apps and Desktops 2203 LTSR CU3 e versões posteriores.

Para alterar a configuração de rede de um esquema de provisionamento existente, faça o seguinte:

1. Na janela do PowerShell, execute o comando `asnp citrix*` para carregar os módulos do PowerShell.
2. Execute `(Get-ProvScheme -ProvisioningSchemeName "name").networkMaps` para acessar o caminho de rede que você deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

```
1 $NewNetworkMap = @{  
2 "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. Em seguida, você pode gerenciar as várias versões do catálogo de máquinas usando os comandos do PowerShell. Você pode:

- Veja 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:

- Contagem de CPUs do VMC
- Memória VM MB
- Propriedades personalizadas
- Oferta de serviços
- Perfil da máquina
- Mapeamento de rede
- Grupo de segurança

Execute os comandos a seguir (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:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Para ver os detalhes de configuração de uma versão específica de um catálogo de máquinas:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -  
Version 2
```

- Para ver o número total de versões associadas a um catálogo de máquinas:

```
1 (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).  
Count
```

- Para usar qualquer versão anterior para atualizar o catálogo de máquinas:

```
1 Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para excluir manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas:

```
1 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 em todos os catálogos. Por exemplo, nesse caso, no máximo 15 versões serão mantidas para todos os catálogos provisionados pelo MCS.

```
1 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 as versões mais antigas estiverem sendo usadas por qualquer uma das VMs no catálogo de máquinas. Nesse caso, faça o seguinte:

- 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 VMs e possam ser excluídas.

## Converter um catálogo de máquinas não baseado em perfil de máquina em catálogo de máquinas baseado em perfil de máquina

Você pode usar uma VM, uma especificação de modelo (no caso do Azure) ou um modelo de lançamento (no caso da AWS) como uma entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina em um catálogo de máquinas baseado em perfil de máquina. As novas VMs adicionadas ao catálogo obtêm valores de propriedade do perfil da máquina, a menos que sejam substituídas por uma propriedade personalizada explícita.

### Nota:

Um catálogo de máquinas existente baseado em perfil de máquina não pode ser alterado para um catálogo de máquinas que não seja 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 **PowerShell**.
3. Execute o comando `Set-PropScheme` para aplicar os valores das propriedades do perfil da máquina às novas VMs adicionadas ao catálogo da máquina. Por exemplo:

- No caso do Azure:

```
1 Set-PropScheme = Set-PropScheme -ProvisioningSchemeName  
xxxx -MachineProfile XDHyp:\HostingUnits\  
HostingUnitName>\machineprofile.folder\  
ResourceGroupName>\<TemplateName>\<VersionName>
```

- No caso da AWS:

```
1 Set-PropScheme = Set-PropScheme -ProvisioningSchemeName  
xxxx -MachineProfile "XDHyp:\HostingUnits\  
<hosting-unit>\<launch-template>.launchtemplate\  
<launch-template-version>.launchtemplateversion"
```

## Reparar as informações de identidade das contas de computador ativas

Você pode redefinir as informações de identidade das contas de computador ativas que tenham problemas relacionados à identidade. Você pode optar por redefinir somente a senha da máquina e as

chaves de confiança ou redefinir todas as configurações do disco de identidade. Essa implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

**Nota:**

Atualmente, o recurso é suportado somente para ambientes de virtualização Azure e VMware.

## Condições

Certifique-se do seguinte para redefinir com êxito o disco de identidade:

- Desligue e defina a VM para o modo de manutenção
- Não inclua o parâmetro `-OS` no comando do PowerShell

## Redefinir disco de identidade

Para redefinir o disco de identidade:

1. Abra a janela **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Redefina as informações de identidade.
  - Para redefinir somente a senha da máquina e as chaves de confiança, execute o seguinte comando:

```
1 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`.
  - Alvo: Alvo para a ação de reparo. Pode ser o `IdentityInfo` para reparar a senha/chave de confiança da conta e o `UserCertificate` para reparar os atributos do certificado do usuário das identidades de máquinas unidas do Hybrid AzureAD.
- Para redefinir todas as configurações do disco de identidade, execute os seguintes comandos na seguinte ordem:

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -  
PrivilegedUserName TEST\admin1 -PrivilegedUserPassword  
$password -Target IdentityInfo
```

```
1 Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <
name> -Identity
```

- Para recriar completamente o disco de identidade:

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <
name> -Identity -Recreate
```

4. Digite **y** para confirmar a ação. Você também pode ignorar a solicitação de confirmação usando o parâmetro `-Force`. Por exemplo:

```
1 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 do cache em um catálogo de máquinas existente

Depois de criar um catálogo não persistente com o MCSIO ativado, você pode usar o comando `Set-provScheme` para modificar os seguintes parâmetros:

- Tamanho da memória cache de Writeback
- Tamanho do disco de cache de gravação

Atualmente, esse recurso é aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO habilitado

## Requisitos

Os requisitos para modificar a configuração do cache são:

- Atualize para a versão mais recente do VDA (2308 ou posterior).
- Ative o parâmetro `UseWritebackCache` para o catálogo de máquinas existente. Use `New-ProvScheme` para criar um catálogo de máquinas com `useWritebackCache` ativado. Por exemplo:

```
1 New-ProvScheme -ProvisioningSchemeName $CatalogName -
HostingUnitUid $HostingUnitUid `
2 -IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
```

```
3 -MasterImageVM $MasterImage `
4 -ServiceOffering $ServiceOffering `
5 -NetworkMap $NetworkMap `
6 -SecurityGroup $SecurityGroup `
7 -UseWriteBackCache -WriteBackCacheDiskSize 8
```

## Alterar a configuração do cache

Execute o comando Set-provScheme. Por exemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDiskSize -
   WriteBackCacheMemorySize 128
```

### Nota:

- O valor de `writebackCacheDiskSize` deve ser maior que zero porque é necessário pelo menos 1 GB de armazenamento em disco cache.
- O valor de `WritebackCacheMemorySize` deve ser menor que o tamanho da memória do catálogo da máquina.
- Essas alterações afetam somente as novas VMs adicionadas ao catálogo após a alteração ser feita. As VMs existentes não são afetadas por essas mudanças.

## Suporte de atualização de VDA por meio de acesso ao compartilhamento de arquivos local

Especifique a localização do instalador do VDA por meio dos cmdlets do PowerShell, o que reduz seu esforço de fornecer regras de rede para permitir que cada VDA busque o novo instalador de VDA no 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 sistema operacional da estação de trabalho
- **vdaServerPackageURI** - para especificar o caminho UNC para o instalador VDA do sistema operacional do servidor

## Pré-requisitos

- VUS Agent Installer que vem com o VDA 2311
- Agente de upgrade do VDA para a versão 7.40.0.35 ou posterior (usando o instalador do VDA versão 2311 ou posterior)
- Aplicativos e desktops virtuais Remote PowerShell SDK versão 7.40 ou mais recente (lançado em 10 de janeiro de 2024 ou posterior)

## Como definir permissões de compartilhamento de arquivos

Os compartilhamentos de rede contendo pacotes do instalador de VDA devem ter acesso de leitura para o serviço VDA Upgrade Agent, que é executado como Sistema Local (NT AUTHORITY\ SYSTEM principal).

### • Permissão de compartilhamento de arquivos associados a um domínio

Quando a máquina VDA é unida ao domínio, a conta **Local System** (o VUA é executado como Sistema Local) usa as credenciais do computador ao acessar compartilhamentos de rede.

A permissão de privilégio mínimo pode ser definida concedendo ao **Read** o acesso aos computadores do domínio.

1. Escolha as pessoas da sua rede com quem você deseja compartilhar o arquivo.
2. Clique em **Configurações avançadas de compartilhamento** e ative **Compartilhamento de arquivos e impressoras**.

### • Permissão de compartilhamento de arquivos não vinculados ao domínio

Quando a máquina VDA não está associada ao domínio, a conta **Local System** (o VUA é executado como Sistema Local) usa **ANONYMOUS LOGON** ao acessar compartilhamentos de rede.

1. Selecione uma pasta compartilhada.
2. Desative a proteção por senha.
  - a) Vá para a pasta **Propriedades**.
  - b) Selecione **Central de Rede e Compartilhamento**.
  - c) Desative **Compartilhamento protegido por senha**.
3. Clique em **Compartilhamento Avançado** para conceder uma permissão de compartilhamento.
  - a) Selecione **Permissões**.
  - b) Conceda uma permissão de compartilhamento **Read** para **ANONYMOUS LOGON**.
4. Selecione a guia **Security Tab** 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 para **ANONYMOUS LOGON**.
5. Clique em **Avançado** para ativar **Compartilhamento de arquivos e impressoras**.
6. Adicione o nome da pasta compartilhada à **Política de Segurança de Acesso à Rede**.

**Nota:**

Reinicie sua máquina para que a alteração entre em vigor imediatamente.

### Atualizações de VDA a partir de um compartilhamento de arquivos local

1. Baixe o instalador do VDA e coloque-o no arquivo compartilhado.

**Nota:**

Com o Virtual Upgrade Service, você pode selecionar entre a faixa Current Release ou a faixa LTSR.

**Por exemplo:** Se o catálogo da máquina estiver definido como Versão atual 2311 e a versão do VDA for 2305, você deverá atualizar o VDA para a versão 2311.

- a) Navegue até a página **Downloads** em [, nosso site](#).
  - b) Selecione **Citrix Virtual Apps and Desktops** como produto.
  - c) Selecione **Citrix Virtual Apps and Desktops 7 2311, todas as edições**.
  - d) Selecione o instalador de VDA entre os componentes **que estão na ISO do produto, mas também são embalados separadamente** expansíveis.
2. Selecione o instalador de VDA relevante com base no tipo de catálogo.
    - Baixe o instalador VDA com sistema operacional multissessão **\*\* se o tipo de catálogo for \*\*multissessão**
    - Baixe o instalador VDA de OS **de sessão única** se o tipo de catálogo for **sessão única**
    - Baixe o instalador VDA **Single-session OS Core Services** se o tipo de catálogo for **Remote PC Access**

**Nota:**

A versão do instalador de compartilhamento de arquivos deve **exatamente** corresponder à versão da versão mais recente do instalador publicada pela VUS na nuvem.

### Solucionar problemas

- Para máquinas com o status “Estado de energia desconhecido”, consulte [CTX131267](#) para obter orientação.



- Para corrigir VMs que mostram continuamente um estado de energia desconhecido, consulte [Como corrigir VMs que mostram continuamente um estado de energia desconhecido](#).

## Para onde ir a seguir

Para obter informações sobre como gerenciar catálogos específicos de serviços em nuvem, consulte:

- [Gerencie um catálogo da 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 da VMware](#)

## Gerencie grupos de entrega

January 27, 2025

### Nota:

Você pode gerenciar a 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 abrange somente 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 definir outras configurações que não estão disponíveis ao criar um grupo de entrega.

As categorias de procedimentos incluem: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, “Impedir que os usuários se conectem às 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:

- [Os aplicativos](#) contêm informações sobre o gerenciamento de aplicativos em grupos de entrega.

- O gerenciamento de grupos de entrega exige as permissões de função integradas do Administrador do 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
- Gerencie grupos de entrega do Remote PC Access
- Organize grupos de entrega usando pastas
- Gerenciar a 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 esse grupo.

---

Coluna	Descrição
Grupo de entrega	O nome do grupo e o tipo de sessão. Os tipos de sessão incluem sistema operacional de sessão única e sistema operacional multissessão.
Entrega	O tipo de recursos fornecidos por esse grupo. Os valores possíveis incluem aplicativos, desktops e aplicativos e desktops. A “Atribuição estática de máquinas” aparece se o grupo de entrega consistir em máquinas dedicadas.
Sessão em uso	O número de máquinas que estão configuradas e o número de máquinas que estão no estado Desconectado.
Contagem alocada	O número de máquinas no catálogo atribuídas a um grupo de entrega.

Coluna	Descrição
Pasta	A localização do grupo na árvore <b>Delivery Groups</b> . 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 oferecer: aplicativos, desktops ou ambos.

Antes de alterar um aplicativo , **somente os desktops** ou **e os aplicativos** , digite somente para os desktops \*\*, exclua todos os aplicativos do grupo.</p>

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Tipo de entrega** , selecione o tipo de entrega que você deseja.
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 **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **StoreFront** , selecione ou adicione URLs do StoreFront. Esses URLs são usados 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 os endereços do 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 nos catálogos de máquinas contendo as máquinas usadas no grupo de entrega.

Antes de começar:

- Se você usa o Citrix Provisioning (antigo 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. Esse processo informa ao console o que precisa ser atualizado no grupo de entrega.
- Se você precisar continuar usando versões anteriores do VDA, os recursos mais novos 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 **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Alterar nível funcional** na barra de ação. A ação **Alterar nível funcional** aparece somente se forem detectados VDAs atualizados.
3. Clique em **Alterar**.

O display indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Em seguida, você pode cancelar a ação de alteração, resolver os problemas da máquina e, em seguida, executar a ação de alteração novamente.

Depois que a alteração for concluída, você poderá reverter as máquinas para seus estados anteriores. Selecione o grupo de entrega e, em seguida, selecione **Undo Functional Level Change** na barra de ação.

### Gerencie grupos de entrega do Remote PC Access

Se uma máquina em um catálogo de máquinas do Remote PC Access não estiver 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 catálogo de entrega do grupo ao máquina tem um valor prioritário. 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 do Remote PC Access tiver várias atribuições de grupo de entrega, o software selecionará a combinação com a maior prioridade. Use o SDK do PowerShell para definir esse valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas do Remote PC Access são associados a um grupo de entrega. Contas de máquinas ou unidades organizacionais adicionadas posteriormente ao catálogo podem ser adicionadas ao grupo de entrega. Essa associação pode ser ativada ou desativada.

Para adicionar ou remover uma associação de catálogo de máquinas do Remote PC Access a um grupo de entrega:

1. Selecione **Delivery Groups** no painel esquerdo.

2. Selecione um grupo de acesso remoto ao PC.
3. Na seção **Details**, clique na guia **Machine Catalogs** e selecione um catálogo Remote PC Access.
4. Para adicionar ou restaurar uma associação, clique em **Adicionar desktops**. Para remover uma associação, clique em **Remover associação**.

### Organize grupos de entrega usando pastas

Você pode criar pastas para organizar grupos de entrega para facilitar o acesso.

**Funções obrigatórias** Por padrão, você precisa ter a seguinte função incorporada para criar e gerenciar pastas de grupos 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 grupos de entrega. Para obter mais informações, consulte Permissões necessárias.

**Crie 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 **Machine Catalogs**, **Applications** e **Delivery groups** nodes) 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 **Delivery Groups** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar pasta** na barra **Action**.
3. Insira um nome para a nova pasta e clique em **Concluído**.

#### Dica:

Se você criar uma pasta em um local não desejado, poderá arrastá-la para o local correto.

### Mover um grupo de entrega

Você pode mover um grupo de entrega entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Delivery Groups** no painel esquerdo.

2. Visualize grupos por pasta. Você também pode ativar **Exibir todos os** acima da hierarquia de pastas para visualizar todos os grupos ao mesmo tempo.
3. Clique com o botão direito do mouse em um grupo e selecione **Move Delivery Group**.
4. Selecione a pasta para a qual você deseja mover o grupo e 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.

Lembre-se de que você pode excluir uma pasta somente se ela e suas subpastas não contiverem grupos de entrega.

Para gerenciar uma pasta, siga estas etapas:

1. Selecione **Delivery Groups** 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 **Move Folder**.
3. Siga as instruções na tela para concluir as etapas restantes.

**Permissões necessárias** A tabela a seguir lista as permissões necessárias para realizar ações nas pastas do grupo de entrega.

---

<b>Ação</b>	<b>Permissões necessárias</b>
Crie pastas de grupos de entrega	Criar pasta de grupo de entrega
Excluir pastas do grupo de entrega	Remover pasta do grupo de entrega
Mover pastas do grupo de entrega	Mover pasta do grupo de entrega
Renomear pastas de grupos de entrega	Editar pasta do grupo de entrega
Mover grupos de entrega para pastas	Editar pasta do grupo de entrega e editar propriedades do grupo de entrega

---

## Gerenciar a proteção de aplicativos

As informações a seguir são complementares à [App protection](#). Lembre-se dos seguintes detalhes:

- Você deve ter um direito válido à Proteção de Aplicativos. Para comprar o recurso App Protection, entre em contato com seu representante de vendas da Citrix.
- A proteção de aplicativos exige confiança em XML. Para ativar a confiança em XML, vá para **Configurações > Ativar confiança em XML**.
- Em relação à captura anti-tela:
  - No Windows e no macOS, somente a janela do conteúdo protegido está em branco. A Proteção de aplicativos está ativa quando uma janela protegida não é minimizada.
  - No Linux, toda a captura está em branco. A Proteção de aplicativos está ativa independentemente de uma janela protegida ser minimizada ou não.

Para escolher um método de proteção de aplicativos para um grupo de entrega, siga estas etapas:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ação.
3. Na página **App Protection**, você pode ativar **Anti-keylogging** e **Anti-captura de tela**.

## Usuários

- Alterar configurações do usuário
- Adicionar ou remover usuários

### Alterar as configurações do usuário em um grupo de entrega

O nome desta página aparece como **Configurações do usuário** ou **Configurações básicas**.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **User Settings** (ou **Basic Settings**), 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.

<b>Configuração</b>	<b>Descrição</b>
Descrição	O texto que o Citrix Workspace (ou StoreFront) usa e que os usuários veem.
Ativar grupo de entrega	Se o grupo de entrega está ativado.
Fuso horário	O fuso horário no qual as máquinas desse grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site. <b>Nota:</b> Alterar o fuso horário em um grupo de entrega pode reinicializar as máquinas desse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.
Ative o Secure ICA	Protege as comunicações de e para as máquinas no grupo de entrega usando o SecureICA, que criptografa o protocolo ICA. O nível padrão é 128 bits. O nível pode ser alterado usando o SDK. A Citrix recomenda usar mais métodos de criptografia, como 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 os usuários, consulte [Usuários](#).

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Users** :
  - Para adicionar usuários, clique em **Add** e, em seguida, especifique os usuários que deseja adicionar.
  - Para remover usuários, selecione um ou mais usuários e clique em **Remove**.
  - Marque ou desmarque a caixa de seleção para permitir o acesso de 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 contendo máquinas físicas com sistema operacional de sessão única, você pode importar informações do usuário de um arquivo.csv depois de criar o grupo de entrega. Você também pode exportar informações do 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 vírgula. As entradas **Machine Account** podem ser SID, FQDN ou pares de nomes de domínio e computador.

Para importar ou exportar informações do usuário:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Machine Allocation**, selecione **Import list** ou **Export list** 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.

## Máquinas

- Alterar atribuições de máquinas aos usuários
- 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
- Restrinja o acesso às máquinas
- Impedir que os usuários se conectem a uma máquina (modo de manutenção)
- Desligue e reinicie máquinas
- Crie e gerencie programações de reinicialização para máquinas
- Ativar agendamento de reinicialização único
- Máquinas gerenciadas por carga
- Máquinas com gerenciamento de energia

### Alterar atribuições de máquinas para usuários em um grupo de entrega

Você pode alterar as atribuições de máquinas com sistema operacional de sessão única provisionadas com o MCS. Você não pode alterar as atribuições para máquinas com sistema operacional multissessão ou máquinas provisionadas com o Citrix Provisioning.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Desktops** ou **Desktop Assignment Rules** (o título da página depende do tipo de catálogo de máquinas usado pelo grupo de entrega), 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.

### **Alterar o número máximo de máquinas por usuário em um grupo de entrega**

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Desktop Assignment Rules**, 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 **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Exibir máquinas** na barra de ação.
3. Selecione uma máquina e clique em **Atualizar máquinas** na barra de ação.

Para escolher uma imagem diferente, selecione **Imagem** e, em seguida, selecione um instantâneo.

Para aplicar 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 reinicialização da distribuição (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados sobre a reinicialização
- A mensagem que os usuários recebem

### **Adicionar, alterar ou remover uma restrição de tag para um desktop**

Adicionar, alterar e remover restrições de tags pode ter efeitos inesperados sobre quais desktops são considerados para lançamento. Analise as considerações e os cuidados em [Tags](#).

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Desktops**, selecione a área de trabalho e clique em **Editar**.

4. Para adicionar uma restrição de tag, selecione **Restringir lançamentos em 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 tags desmarcando **Restringir lançamentos em máquinas com essa 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

A remoção de uma máquina a exclui de um grupo de entrega. Ele não o exclui do catálogo de máquinas que o grupo de entrega usa. Portanto, essa máquina está disponível para ser atribuída 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 no 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 ação.
3. Certifique-se de que a máquina esteja desligada.
4. Selecione a máquina e clique em **Remover do Grupo de Entrega** na barra de ação.

Você também pode remover uma máquina de um grupo de entrega por meio da conexão que a máquina usa.

### Restringir o acesso às máquinas em um grupo de entrega

Qualquer alteração feita para restringir o acesso às máquinas em um grupo de entrega substitui as configurações anteriores, independentemente do método usado. Você pode:

- **Restrinja o acesso de administradores usando escopos de administração delegada:** Crie e atribua um escopo que permita aos administradores acessar todos os aplicativos e outro escopo que forneça acesso somente a determinados aplicativos. Para obter detalhes, consulte [Administração delegada](#).

- **Restrinja o acesso de usuários por meio de expressões de política do SmartAccess:** Use expressões de política para filtrar conexões de usuários feitas por meio do Citrix Gateway.
  1. Selecione **Delivery Groups** no painel esquerdo.
  2. Selecione um grupo e clique em **Editar** na barra de ação.
  3. Na página **Access Policy**, selecione **Connections through NetScaler Gateway**.
  4. Para escolher um subconjunto dessas conexões, selecione **Conexões que atendem a qualquer um dos seguintes filtros**. Em seguida, defina o site do Citrix Gateway e adicione, edite ou remova as expressões de política do SmartAccess para os cenários de acesso permitido ao usuário. Para obter detalhes, consulte a documentação do Citrix Gateway.
  5. 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.
- **Restrinja o acesso dos usuários por meio de filtros de exclusão:** Use filtros de exclusão nas políticas de acesso definidas no SDK. As políticas de acesso são aplicadas aos grupos de entrega para refinar as conexões. Por exemplo, você pode restringir o acesso à máquina a um subconjunto de usuários e especificar dispositivos de usuário permitidos. Os filtros de exclusão refinam ainda mais as políticas de acesso. Por exemplo, por motivos de segurança, você pode negar acesso a um subconjunto de usuários ou dispositivos. Por padrão, os filtros de exclusão estão desativados.

Por exemplo, um laboratório de ensino em uma sub-rede de rede corporativa que impede o acesso desse laboratório a um grupo de entrega específico. Independentemente de quem esteja usando as máquinas no laboratório, use o comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

Use o caractere curinga asterisco (\ \*) para corresponder a todas as tags que começam com a mesma expressão de política. Por exemplo, se você adicionar a tag `VPDesktops_Direct` a uma máquina e `VPDesktops_Test` a outra, definir a tag no script `Set-BrokerAccessPolicy` como `VPDesktops_*` aplicará o filtro às duas máquinas.

Se você estiver conectado usando um navegador da Web ou com o recurso de experiência do usuário do aplicativo Citrix Workspace ativado na loja, não poderá usar um filtro de exclusão de nome de cliente.

### **Impedir que os usuários se conectem a uma máquina (modo de manutenção) em um grupo de entrega**

Quando precisar interromper temporariamente novas conexões com máquinas, você 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 com sistema operacional multissessão está no modo de manutenção, os usuários podem se conectar às sessões existentes, mas não podem iniciar novas sessões.
- Quando uma máquina com sistema operacional de sessão única (ou um PC usando o Remote PC Access) está no modo de manutenção, os usuários não podem se conectar ou se reconectar. As conexões atuais permanecem conectadas até serem desconectadas ou desconectadas.

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 **Ativar o modo de manutenção** na barra de ação.

Para ativar o modo de manutenção para uma máquina, clique em **Exibir máquinas** na barra de ação. Selecione uma máquina e clique em **Ativar o modo de manutenção** na barra de ação.

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 **Desativar o modo de manutenção** na barra de ação.

As configurações de conexão de área de trabalho remota (RDC) do Windows também afetam se uma máquina com sistema operacional multissessão está no modo de manutenção. O modo de manutenção é ativado quando ocorre uma das seguintes situações:

- O modo de manutenção está ativado, conforme descrito anteriormente.
- O RDC está definido como **Não permitir conexões com este computador**.
- O RDC não está definido como **Não permitir conexões com este computador**. A configuração **Remote Host Configuration User Logon Mode** é **Permitir reconexões, mas evitar novos logons** ou **Permitir reconexões, mas evitar novos logons até que o servidor seja reiniciado**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, que afeta as máquinas desse catálogo.

### **Desligue e reinicie máquinas em um grupo de entrega**

Esse procedimento não é suportado para máquinas com acesso remoto ao PC.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Exibir máquinas** na barra de ação.
3. Selecione a máquina e clique em uma das seguintes entradas na barra de ação:

- **Desligamento forçado:** Desliga a máquina à força e atualiza a lista de máquinas.
- **Reiniciar:** Solicita que o sistema operacional seja desligado e, em seguida, inicie a máquina novamente. Se o sistema operacional não estiver em conformidade, a máquina permanecerá em seu estado atual.
- **Reinicialização forçada:** Desliga forçosamente o sistema operacional e reinicia a máquina.
- **Suspender:** Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
- **Desligar:** Solicita que o sistema operacional seja desligado.

Para ações sem força, se a máquina não for desligada em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, existe o risco de a máquina ser desligada antes da conclusão das atualizações.

A Citrix recomenda que você evite que usuários de máquinas com sistema operacional de sessão única selecionem **Desligar** em uma sessão. Consulte a documentação da política da Microsoft para obter detalhes.

Você também pode desligar e reiniciar máquinas em uma conexão .

### **Crie e gerencie programações de reinicialização para máquinas em um grupo de entrega**

#### **Nota:**

- Quando um cronograma de reinicialização é aplicado a um grupo de entrega com a Autoescala ativada, suas máquinas são simplesmente desligadas e deixadas para a Autoescala 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 a escala automática para ligar as máquinas.
- Alterar o fuso horário em um grupo de entrega pode reinicializar as máquinas desse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

Um cronograma de reinicialização especifica quando as máquinas em um grupo de entrega são reiniciadas periodicamente. Você pode criar uma ou mais agendas para um grupo de entrega. Um cronograma pode afetar:

- Todas as máquinas do grupo.
- Uma ou mais (mas não todas) máquinas do grupo. As máquinas são identificadas por uma etiqueta que você aplica à máquina. Isso é chamado de restrição de tag, porque a tag restringe uma ação somente aos itens que têm a tag.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você quer que todas as máquinas sejam reiniciadas uma vez por semana e que as máquinas usadas pela equipe de contabilidade sejam reiniciadas diariamente. Para fazer isso, configure um cronograma para todas as máquinas e outro cronograma somente para as máquinas na contabilidade.

Uma programação inclui o dia e a hora em que a reinicialização começa e a duração.

Você pode ativar ou desativar um agendamento. Desativar um cronograma pode ser útil ao testar, durante intervalos especiais ou ao preparar agendas antes que você precise delas.

Você não pode usar programações para ativação ou desligamento automatizados a partir do console de gerenciamento, apenas para reiniciar.

**Sobreposição de horários** Várias agendas podem se sobrepor. No exemplo acima, os dois cronogramas afetam as máquinas contábeis. Essas máquinas podem ser reiniciadas duas vezes no domingo. O código de agendamento foi projetado para evitar a reinicialização da mesma máquina com mais frequência do que o pretendido, mas não pode ser garantido.

- Se os horários coincidirem precisamente nos horários de início e duração, é mais provável que as máquinas sejam reiniciadas apenas uma vez.
- Quanto mais as programações diferirem nos horários de início e duração, é mais provável que ocorram várias reinicializações.
- O número de máquinas afetadas por um cronograma também afeta a chance de uma sobreposição. No exemplo, a programação semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que a programação diária para máquinas de contabilidade, dependendo da duração especificada para cada uma.

Para uma análise aprofundada dos cronogramas de reinicialização, consulte [Reboot schedule internals](#).

### Exibir programações de reinicialização

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Selecione a página **Restart Schedule**.

A página **Restart Schedule** contém as seguintes informações para cada agendamento configurado:

- Nome do cronograma.
- Restrição de tag usada, se houver.
- Com que frequência as reinicializações da máquina ocorrem.
- Se os usuários da máquina recebem uma notificação.
- Se a programação está ativada.

**Adicionar (aplicar) tags** Ao configurar uma programação de reinicialização que usa uma restrição de tag, certifique-se de que a tag tenha sido adicionada às máquinas que a programação 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 reinicialização pode especificar somente uma tag.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione o grupo que contém as máquinas controladas pela programação.
3. Clique em **Exibir máquinas** e selecione as máquinas às quais você deseja adicionar uma tag.
4. Clique em **Gerenciar tags** na barra de ação.
5. Se a tag existir, ative a caixa de seleção ao lado do nome da tag. Se a tag não existir, clique em **Create** e especifique o nome da tag. Depois que a tag for criada, ative a caixa de seleção ao lado do nome da tag recém-criada.
6. Clique em **Salvar** na caixa de diálogo **Manage Tags**.

### **Crie um cronograma de reinicialização**

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Restart Schedule**, clique em **Adicionar**.
4. Na página **Adicionar cronograma de reinicialização**:
  - Para ativar a programação, selecione **Sim**. Para desativar a programação, selecione **Não**.
  - Digite o nome e a descrição do cronograma.
  - Para **Restringir à tag**, aplique uma restrição de tag.
  - Para **Incluir máquinas no modo de manutenção**, escolha se deseja incluir máquinas que estão no modo de manutenção nesta programação. Para usar o PowerShell em vez disso, consulte [Reinicializações programadas para máquinas no modo de manutenção](#).
  - Para **Frequência de reinicialização**, 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 **Repetir a cada**, especifique com que frequência você deseja que a programação seja executada.
  - Para **Data de início**, especifique uma data de início para a primeira ocorrência da programação.



- Para **Comece a reiniciar em**, especifique, no formato de relógio de 24 horas, a hora do dia para iniciar a reinicialização.
- Para **, reinicie a duração:**
  - 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**.
  - Se você quiser usar a reinicialização natural, selecione **Reiniciar todas as máquinas depois de esgotar todas as sessões**.

Ao iniciar um cronograma de reinicialização configurado para usar o reinício 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:**

Você pode usar essa opção para máquinas com gerenciamento de energia e também para máquinas sem gerenciamento de energia.

- Em **Enviar notificação aos usuários**, escolha se deseja exibir uma mensagem de notificação nas máquinas aplicáveis antes do início da reinicialização. Por padrão, nenhuma mensagem aparece.
- Se você optar por exibir uma mensagem 15 minutos antes do início da reinicialização, poderá escolher (na 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.

```
1 If you want the message to include a countdown to restart, include the variable **%m%** . Unless you chose to restart all machines at the same time, the message appears on each machine at the appropriate time before the restart.
```

5. Clique em **Concluído** para aplicar as alterações e fechar a janela **Adicionar cronograma de reinicialização**.
6. Clique em **Aplicar** para aplicar as alterações que você fez e manter a janela aberta. Ou clique em **Salvar** para aplicar as alterações e fechar a janela.

**Reinicie após a drenagem** Outro valor de duração de reinicialização está disponível ao usar o PowerShell para criar ou atualizar um agendamento de reinicialização da máquina (`New-BrokerRebootScheduleV2` ou `Set-BrokerRebootScheduleV2`).

Quando você ativa o recurso de reinicialização após drenagem com o parâmetro `-UseNaturalReboot <Boolean>`, todas as máquinas são reiniciadas após esgotar todas as sessões. Quando o tempo de reinicialização é atingido, as máquinas são colocadas no estado de drenagem e reiniciadas quando todas as sessões são desconectadas.

Esse recurso é compatível com grupos de entrega contendo máquinas de sessão única ou multi-sessão. Você pode usar essa opção para máquinas com gerenciamento de energia e também para máquinas sem gerenciamento de energia.

Em um ambiente local, esse recurso é suportado somente ao usar o PowerShell. O recurso não está disponível no Web Studio.

### Editar, remover, ativar ou desativar um agendamento de reinicialização

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ação.
3. Na página **Reiniciar Programação**, marque a caixa de seleção de uma programação.
  - Para editar uma programação, clique em **Editar**. Atualize a configuração do agendamento, usando a orientação em Criar um cronograma de reinicialização.
  - Para ativar ou desativar um agendamento, clique em **Editar**. Marque ou desmarque a caixa de seleção **Habilitar agendamento de reinicialização**.
  - 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 programadas atrasadas devido à interrupção do banco de dados

#### Nota:

Esse recurso está disponível somente no PowerShell.

Se ocorrer uma interrupção do banco de dados do site antes do início de uma reinicialização programada para máquinas (VDAs) em um grupo de entrega, as reinicializações começarão quando a interrupção terminar. Isso pode ter resultados inesperados.

Por exemplo, digamos que você tenha programado a reinicialização de um grupo de entrega para ocorrer fora do horário de produção (começando às 03:00). Uma interrupção do banco de dados do site ocorre uma hora antes do início da reinicialização programada (02:00). A interrupção dura seis horas (até às 08:00). O cronograma de reinicialização começa quando a conexão entre o Delivery Controller e o banco de dados do site é restaurada. As reinicializações do VDA agora começam

cinco horas após a programação original, resultando na reinicialização dos VDAs durante o horário de produção.

Para ajudar a evitar essa situação, você pode usar o parâmetro `MaxOverTimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além da hora de início programada em que uma programação de reinicialização pode começar.

- Se a conexão com o banco de dados for restaurada dentro desse período (horário agendado + `maxOverTimeStartMins`), as reinicializações do VDA começarão.
- Se a conexão com o banco de dados não for restaurada dentro desse período, as reinicializações do VDA não começarão.
- Se esse 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. Esse recurso está disponível somente no PowerShell. Você não pode definir esse valor ao configurar um agendamento de reinicialização no Web Studio.

### Reinicializações programadas para máquinas em modo de manutenção

#### Nota:

Esse recurso está disponível somente no PowerShell. A opção `IgnoreMaintenanceMode` é compatível com o Citrix Virtual Apps and Desktops 7 2006 e versões posteriores.

Para indicar se um agendamento de reinicialização afeta máquinas que estão no modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria uma programação que reinicia as máquinas que estão no modo de manutenção (além das máquinas que não estão no modo de manutenção).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

O cmdlet a seguir modifica uma agenda de reinicialização existente.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

Para obter mais informações, consulte a ajuda do cmdlet. Esse recurso está disponível somente no PowerShell.

## Ativar agendamento de reinicialização único

Se você quiser habilitar o agendamento de reinicialização único usando o PowerShell, use os seguintes comandos `BrokerCatalogRebootSchedule` do PowerShell para criar, modificar e excluir um agendamento de reinicialização:

- Cronograma de reinicialização do Get-BrokerCatalog
- Cronograma de reinicialização do catálogo da New Broker
- Cronograma de reinicialização do catálogo Set-Broker
- Agenda de reinicialização do Remove-BrokerCatalog
- Cronograma de reinicialização do Renome-BrokerCatalog

Limitações:

- Um cronograma de reinicialização do catálogo associado a um catálogo sem um fuso horário configurado é criado, mas não é iniciado.
- Quando uma agenda de reinicialização do catálogo é criada, a agenda de reinicialização é executada somente nas VMs do catálogo pertencentes a um grupo de entrega.

Exemplo,

- Para criar um cronograma de reinicialização das VMs no catálogo chamado **BankTellers** para começar em 3 de fevereiro de 2022, entre 2h e 4h.

```
1 C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -  
CatalogName BankTellers -StartDate "2022-02-03" -StartTime  
"02:00" -Enabled $true -RebootDuration 120
```

- Criar um cronograma de reinicialização das VMs no catálogo com UID 17 para começar em 3 de fevereiro de 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM está configurada para exibir uma caixa de mensagem com o título **AVISO: Reinicialização pendente** e a mensagem **Salve seu trabalho** em cada sessão do usuário.

```
1 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 catálogo, reinicie a programação chamada **Old Name to New Name**.

```
1 C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -  
NewName "New Name"
```

- Para exibir todos os agendamentos de reinicialização do catálogo com o UID 1 e, em seguida, renomear o agendamento de reinicialização do catálogo com o UID 1 para **New Name**.

```
1 C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
  BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Para definir a programação de reinicialização do catálogo chamada **Accounting** para exibir uma mensagem com o título **WARNING: Reboot pending, e a mensagem, Save your work**, dez minutos antes da reinicialização de cada VM. A mensagem aparece em cada sessão do usuário nessa VM.

““

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage "Save your
work"-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
```

- To display all restart schedules that are disabled, and then enable all disabled restart schedules.

```
1 C:\PS> Get-BrokerCatalog RebootSchedule -Enabled $false | Set-
  BrokerCatalogRebootSchedule -Enabled $true
```

- To set the catalog restart schedule with UID 17 to display the message **Rebooting in %m% minutes** fifteen, ten, and five minutes before the restart of each VM.

```
1 C:\PS> Set-BrokerCatalogrebootSchedule 17 -WarningMessage "
  Reiniciando em %m% minutos." - Duração do aviso 15 -
  Intervalo de repetição do aviso 5
```

- To configure the time zone for the catalog named **MyCatalog**.

```
C:\PS> Set-BrokerCatalog - Nome "MyCatalog" -TimeZone <TimeZone>
```

## Máquinas gerenciadas por carga em grupos de entrega

Você só pode gerenciar e carregar máquinas com sistema operacional multissessão.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar nas condições atuais do ambiente. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** Uma máquina com sistema operacional multissessão é considerada para balanceamento de carga somente quando o modo de manutenção está desativado.
- **Índice de carga do servidor:** Determina a probabilidade de um servidor que fornece máquinas com sistema operacional multissessão receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações de 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 informando que o desktop ou o aplicativo não estão disponíveis ao iniciarem uma sessão.

Você pode monitorar o índice de carga na pesquisa do Director (Monitor), do Web Studio (Gerenciar) e no SDK.

Nas telas do console, para exibir a coluna **Server Load Index** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse no cabeçalho de uma coluna e selecione **Selecionar coluna**. Na categoria **Machine**, selecione **Load Index**.

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 login no servidor. (Essa configuração é equivalente à limitação de carga nas versões do XenApp 6.x.)

Quando todos os servidores estão na configuração de tolerância de logon simultâneo ou superior, 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 energeticamente somente máquinas virtuais com sistema operacional de sessão única, não máquinas físicas (incluindo máquinas de acesso remoto ao PC). Máquinas com sistema operacional de sessão única com recursos de GPU não podem ser suspensas, portanto, as operações de desligamento falham. Para máquinas com sistema operacional multissessão, você pode criar um cronograma de reinicialização.

Em grupos de entrega contendo máquinas agrupadas, as máquinas virtuais com sistema operacional de sessão única podem estar em um dos seguintes estados:

- Alocado aleatoriamente e em uso
- Não alocado e desconectado

Em grupos de entrega contendo máquinas estáticas, as máquinas virtuais com sistema operacional de sessão única podem ser:

- Alocado permanentemente e em uso
- Alocado permanentemente e desconectado (mas pronto)
- Não alocado e desconectado

Durante o uso normal, os grupos de entrega estáticos geralmente contêm máquinas alocadas permanentemente e não alocadas. Inicialmente, todas as máquinas não estão alocadas, exceto as alocadas manualmente quando o grupo de entrega foi criado. À medida que os usuários se conectam,

as máquinas são alocadas permanentemente. Você pode gerenciar totalmente as máquinas não alocadas nesses grupos de entrega, mas gerenciar apenas parcialmente as máquinas alocadas permanentemente.

- **Pools e buffers:** Para grupos de entrega agrupados 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 um estado ligado, prontas para os usuários se conectarem. Um usuário obtém uma máquina imediatamente após o login. O tamanho da piscina (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 em espera de máquinas não alocadas que são ativadas quando o número de máquinas no pool cai abaixo de um limite. O limite é uma porcentagem do tamanho do grupo de entrega. Para grandes grupos de entrega, um número significativo de máquinas pode ser ligado quando o limite é excedido. Portanto, planeje cuidadosamente os tamanhos dos grupos de entrega ou use o SDK para ajustar o tamanho padrão do buffer.

- **Temporizadores de estado de energia:** Você pode usar temporizadores de estado de energia para suspender as máquinas depois que os usuários se desconectarem por um determinado período de tempo. Por exemplo, as máquinas são suspensas automaticamente fora do horário comercial se os usuários forem desconectados por pelo menos 10 minutos.

Você pode configurar temporizadores para dias da semana 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 do pico. Você não tem o controle preciso que você tem com máquinas não alocadas sobre o número de máquinas que ficam disponíveis para compensar as máquinas que são consumidas.

### Gerencie e gerencie máquinas virtuais com sistema operacional de sessão única

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar grupo de entrega** na barra de ação.
3. Na página **Power Management**, selecione **Weekdays** em **Power manage machines**. Por padrão, os dias da semana são de segunda a sexta-feira.
4. Para grupos de entrega aleatórios, em **Máquinas a serem alimentadas em**, clique em **Editar** e especifique o tamanho do pool durante a semana. Em seguida, selecione o número de máquinas a serem ligadas.
5. Em **Horários de pico**, defina os horários de pico e fora de pico para cada dia.

6. Defina os temporizadores de estado de energia para horários de pico e fora de pico durante a semana: em **Durante o horário de pico > Quando desconectado**, especifique o atraso (em minutos) antes de suspender qualquer máquina desconectada no grupo de entrega e selecione **Suspender**. Em **Fora do horário de pico > Quando desconectado**, especifique o atraso antes de desligar qualquer máquina desconectada no grupo de entrega e selecione **Shutdown**. Esse cronômetro não está disponível para grupos de entrega com máquinas aleatórias.
7. Selecione **Weekend** em **Power Manage Machines** configure os horários de pico e os temporizadores de estado de energia para 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:

- Desligue, em vez de suspender, as máquinas em resposta aos temporizadores de estado de energia, ou se quiser que os temporizadores se baseiem em interrupções, em vez de desconexões.
- Altere as definições padrão de dias úteis e finais de semana.
- Desative o gerenciamento de energia. Veja [CTX217289](#).

### Gerencie a energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas

#### Importante:

Esse aprimoramento se aplica somente a máquinas VDI com sessões desconectadas. Ela não se aplica a máquinas VDI com sessões desconectadas.

Em versões anteriores, uma máquina VDI em transição para um período em que era necessária uma ação (ação de desconexão =”**Suspend**“ ou ”**Shutdown**“) permaneceu ligada. Esse cenário ocorria se a máquina se desconectasse durante um período (horários de pico ou fora de pico) em que nenhuma ação (ação de desconexão =”**Nada**“) era necessária.

Começando com o Citrix Virtual Apps and Desktops 7 1909, a máquina é suspensa ou desligada quando o tempo de desconexão especificado termina, dependendo da ação de desconexão configurada para o período de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega de 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](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 quando fazia a transição de pico para fora do pico. Começando com o Citrix Virtual Apps and Desktops 7 1909, as ações de política `offpeakDisconnectAction` e `offpeakDisconnectTimeout` são aplicadas à máquina VDI na transição do período. Como resultado, a máquina é desligada 10 minutos após a transição para fora do pico.

Se você quiser reverter ao comportamento anterior (ou seja, não realizar nenhuma ação em máquinas que fazem a transição de pico para fora do pico ou de fora do pico para pico com sessões desconectadas), faça o seguinte:

- Defina o valor do registro `LegacyPeakTransitionDisconnectedBehaviour` como `1`, o equivalente a `true`, que ativa o comportamento anterior. Por padrão, o valor é `0` ou `false`, que aciona ações de política de desconexão de energia na transição do período.
  - Caminho: `HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ DesktopServer`
  - Nome: `LegacyPeakTransitionDisconnectedBehavior`
  - Tipo: `REG_DWORD`
  - Dados: `0x00000001` (1)
- Defina a configuração usando o comando `Set-BrokerServiceConfigurationData` PowerShell. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações de política de energia possam ser aplicadas a ela durante a transição do período:

- Tenha uma sessão desconectada.
- Não tenha ações de poder pendentes.
- Pertença a um grupo de entrega de VDI (sessão única) que faz a transição para um período de tempo diferente.
- Faça uma sessão que se desconecte durante um determinado período de tempo (horários de pico ou fora de pico) e faça a transição para um período em que uma ação de energia seja atribuída.

### **Alterar a porcentagem de VDAs em um estado ativado para catálogos**

1. Ajuste os horários de pico para o grupo de entrega na seção **Gerenciamento de energia** para o grupo de entrega.
2. Anote o nome do Desktop Group.
3. Com privilégios de administrador, inicie o PowerShell e execute os seguintes comandos. Substitua “Nome do grupo de desktop” pelo nome do seu grupo de desktops que tem uma porcentagem alterada dos VDAs em execução.

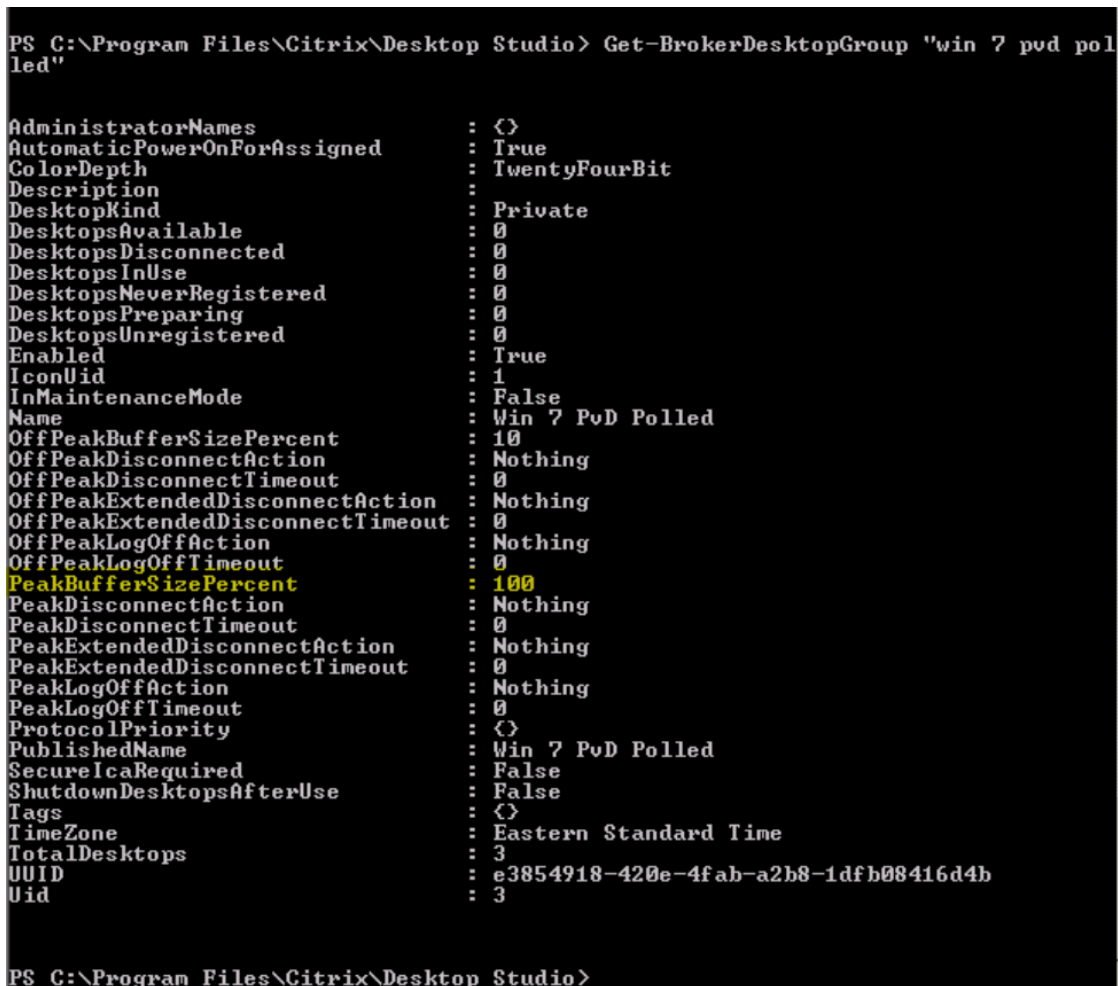
```
asnp Citrix*
```

```
# Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
100
```

Um valor de 100 significa que 100% dos VDAs estão prontos.

4. Verifique a solução executando:

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```



```
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerDesktopGroup "win 7 pvd pol
led"

AdministratorNames           : {}
AutomaticPowerOnForAssigned  : True
ColorDepth                   : TwentyFourBit
Description                   :
DesktopKind                   : Private
DesktopsAvailable            : 0
DesktopsDisconnected          : 0
DesktopsInUse                 : 0
DesktopsNeverRegistered      : 0
DesktopsPreparing            : 0
DesktopsUnregistered         : 0
Enabled                       : True
IconUid                       : 1
InMaintenanceMode            : False
Name                          : Win 7 PvD Polled
OffPeakBufferSizePercent     : 10
OffPeakDisconnectAction      : Nothing
OffPeakDisconnectTimeout     : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction          : Nothing
OffPeakLogOffTimeout         : 0
PeakBufferSizePercent       : 100
PeakDisconnectAction         : Nothing
PeakDisconnectTimeout        : 0
PeakExtendedDisconnectAction  : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction              : Nothing
PeakLogOffTimeout            : 0
ProtocolPriority              : {}
PublishedName                 : Win 7 PvD Polled
SecureIcaRequired             : False
ShutdownDesktopsAfterUse     : False
Tags                          : {}
TimeZone                      : Eastern Standard Time
TotalDesktops                 : 3
UUID                          : e3854918-420e-4fab-a2b8-1dfb08416d4b
Uid                           : 3

PS C:\Program Files\Citrix\Desktop Studio>
```

Pode levar até uma hora para que as alterações entrem em vigor.

Para desligar os VDAs após o usuário se desconectar, 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 se desconectarem, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin  
$True
```

## Sessões

- Encerre ou desconecte uma sessão ou envie uma mensagem aos usuários
- Configurar o pré-lançamento e a duração da sessão
- Controle a reconexão da sessão quando desconectado da máquina no modo de manutenção
- Configurar o roaming da sessão

### Sair ou desconectar uma sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **Exibir máquinas** na barra de ação.
3. No painel central, selecione a máquina, selecione **Exibir sessões** na barra de ação e, em seguida, selecione uma sessão.
  - Como alternativa, no painel central, selecione a guia **Sessão** e, em seguida, selecione uma sessão.
4. Para sair de uma sessão, selecione **Sair** na barra de ação. 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 **Desconectar** na barra de ação. Os aplicativos continuam sendo 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 com sistema operacional de sessão única para lidar automaticamente com sessões não utilizadas. Para obter detalhes, consulte Máquinas com gerenciamento de 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 **Exibir máquinas** na barra de ação.
3. No painel central, selecione uma máquina para a qual você deseja enviar uma mensagem.
4. Na barra de ação, selecione **Exibir sessões**.
5. No painel central, selecione todas as sessões e, em seguida, selecione **Enviar mensagem** na barra de ação.
6. Digite sua mensagem e clique em **OK**. Você pode especificar o nível de severidade, se necessário. As opções incluem **Critical, Question, Warning Information**.

Como alternativa, você pode enviar uma mensagem usando o Citrix Director. Para obter mais informações, consulte [Enviar mensagens para usuários](#).

### **Configurar o pré-lançamento da sessão e a permanência da sessão em um grupo de entrega**

Esses recursos são suportados somente em máquinas com sistema operacional multissessão.

Os recursos de pré-lançamento da sessão e prolongamento da sessão ajudam usuários específicos a acessar aplicativos rapidamente, iniciando sessões antes de serem solicitadas (pré-lançamento da sessão) e mantendo as sessões do aplicativo ativas após o usuário fechar todos os aplicativos (prolongamento da sessão).

Por padrão, o pré-lançamento da sessão e o prolongamento da sessão não são usados. Uma sessão começa (é iniciada) 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 oferecer suporte a aplicativos e as máquinas devem estar executando um VDA para sistema operacional multissessão, versão mínima 7.6.
- Esses recursos são suportados somente ao usar o aplicativo Citrix Workspace para Windows e também exigem configuração adicional do aplicativo Citrix Workspace. Para obter instruções, pesquise o pré-lançamento da sessão na documentação do produto para sua versão do aplicativo Citrix Workspace para Windows.
- O aplicativo Citrix Workspace para HTML5 não é suportado.
- Ao usar a pré-lançamento da sessão, se a máquina de um usuário for colocada no modo de suspensão ou hibernação, a pré-lançamento não funcionará (independentemente das configurações de pré-lançamento da sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário se desconectar do aplicativo Citrix Workspace, a sessão será encerrada e a pré-lançamento não se aplicará mais.
- Ao usar a pré-lançamento da sessão, as máquinas clientes 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 se desconectar.
- As sessões pré-lançadas e prolongadas consomem uma licença simultânea, mas somente quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. Por padrão, as sessões pré-lançadas e prolongadas não utilizadas são desconectadas após 15 minutos. Esse valor pode ser configurado no PowerShell (`cmdletnew/Set-BrokerSessionPrelaunch`).
- O planejamento e o monitoramento cuidadosos dos padrões de atividade de seus usuários são essenciais para adaptar esses recursos para se complementarem. 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 da sessão para um horário agendado do dia no aplicativo Citrix Workspace.

### **Por quanto tempo as sessões não utilizadas, pré-lançadas e prolongadas permanecem ativas**

Há 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 termine.

- **Tempo limite:** Um tempo limite configurado especifica o número de minutos, horas ou dias em que uma sessão não utilizada, pré-lançada ou prolongada, permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-lançadas terminarão antes que elas ofereçam ao usuário o benefício de um acesso mais rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de entrada do usuário poderão ser negadas porque o servidor não tem recursos suficientes.

Você pode ativar esse tempo limite somente no SDK (`cmdletnew/Set-BrokerSessionPreLaunch`), não no console de gerenciamento. Se você desabilitar o tempo limite, ele não aparecerá na tela do console desse grupo de entrega ou nas páginas **Editar Grupo de Entrega**.

- **Limites:** O encerramento automático das sessões pré-lançadas e persistentes com base na carga do servidor garante que as sessões permaneçam abertas pelo maior tempo possível, supondo que os recursos do servidor estejam disponíveis. Sessões pré-lançadas e prolongadas não utilizadas não causam conexões negadas porque elas são encerradas automaticamente quando são necessários recursos 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 estão no estado de pré-lançamento ou persistentes há mais tempo são encerradas. As sessões são encerradas uma a uma em intervalos de minutos até que a carga caia abaixo do limite. Embora o limite seja excedido, nenhuma nova sessão de pré-lançamento é iniciada.

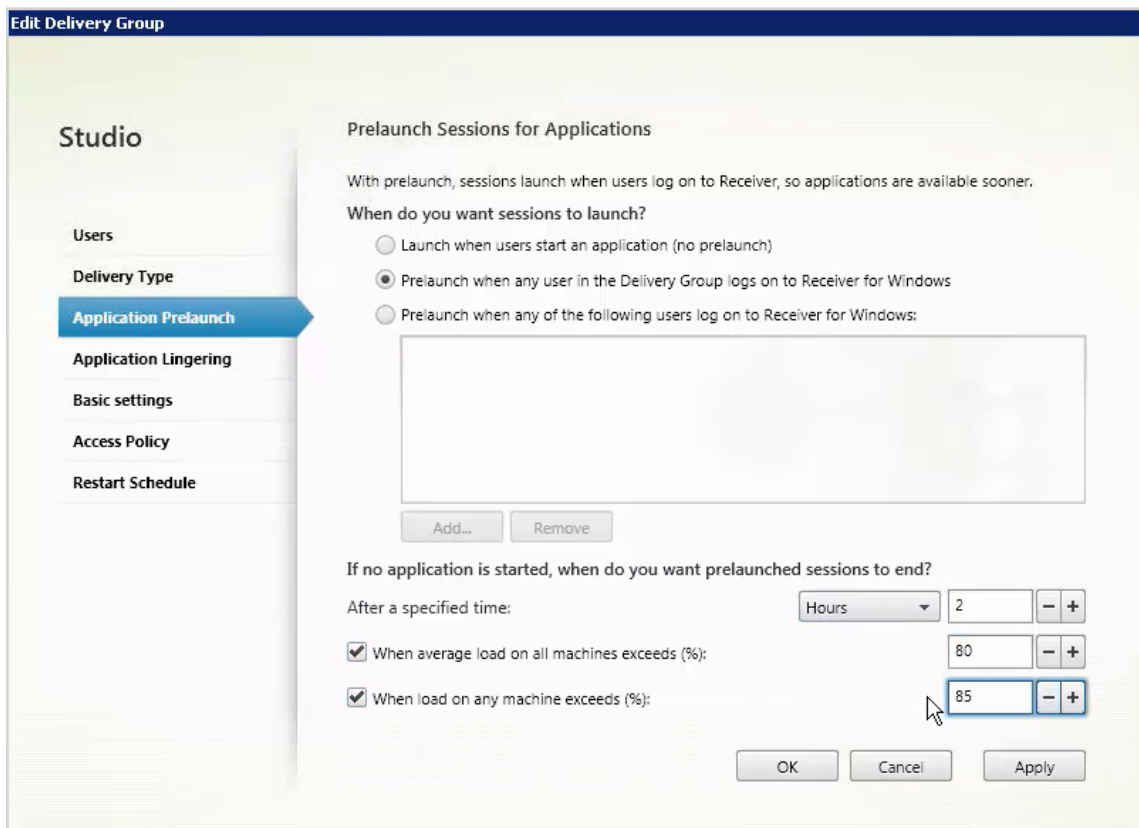
Servidores com VDAs que não foram registrados em um controlador e servidores em modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-lançamento e as sessões prolongadas terminem automaticamente para liberar capacidade.

### **Para ativar o pré-lançamento da sessão**

1. Selecione um grupo e clique em **Editar grupo de entrega** na barra de ação.

2. Na página **Pré-lançamento do Aplicativo** , ative o pré-lançamento da sessão escolhendo quando as sessões serão iniciadas:

- Quando um usuário inicia um aplicativo. Essa é a configuração padrão. O pré-lançamento da sessão está desativado.
- Quando qualquer usuário do grupo de entrega faz login no aplicativo Citrix Workspace para Windows.
- Quando qualquer pessoa em uma lista de usuários e grupos de usuários faz login no aplicativo Citrix Workspace para Windows. Certifique-se de especificar também usuários ou grupos de usuários se escolher essa opção.



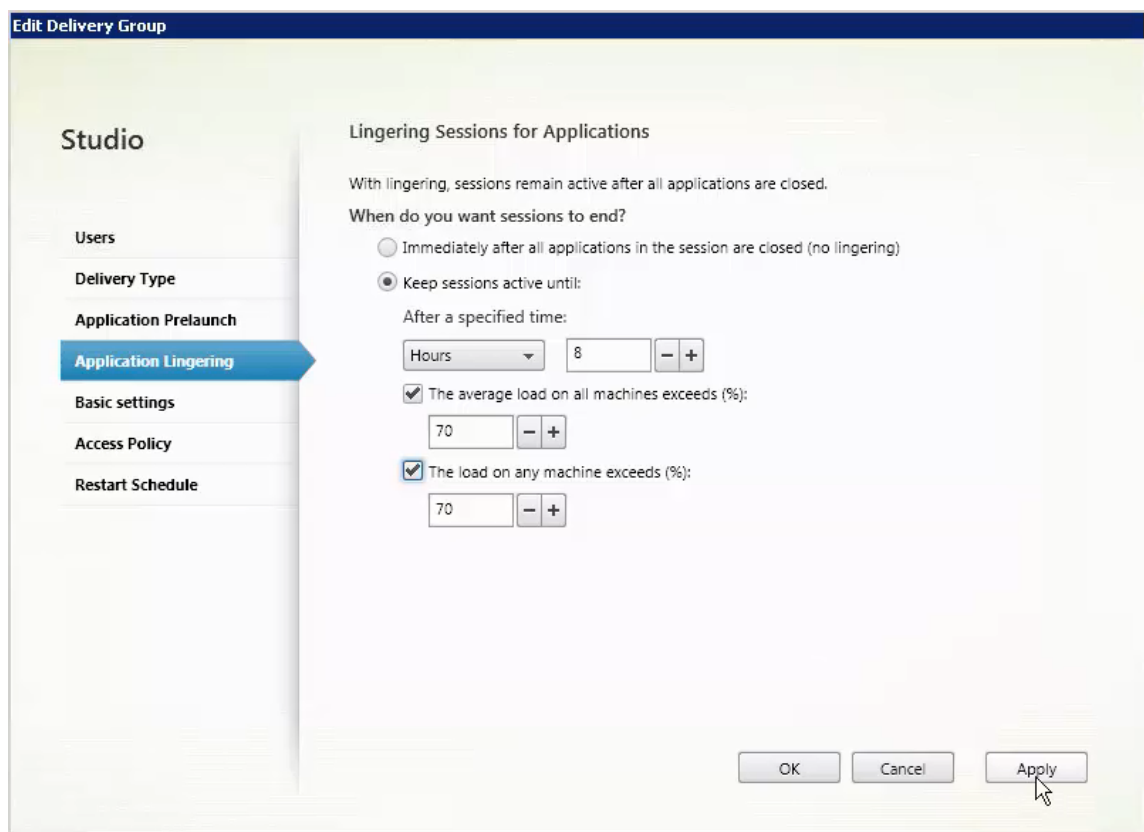
3. Uma sessão pré-lançada é substituída por uma sessão normal quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-lançada não for usada), as configurações a seguir afetarão por quanto tempo essa sessão permanecerá ativa.

- Quando decorre um intervalo de tempo especificado. 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 do grupo de entrega excede uma porcentagem especificada (1—99%).
- Quando a carga em qualquer máquina do grupo de entrega excede uma porcentagem especificada (1—99%).

Resumo: Uma sessão pré-lançada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicie um aplicativo, o tempo especificado passe ou um limite de carga especificado seja excedido.

### Para ativar o prolongamento da sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Editar grupo de entrega** na barra de ação.
3. Na página **Application Linging**, ative o prolongamento da sessão selecionando **Manter as sessões ativas até**.



4. Várias configurações afetam por quanto tempo uma sessão persistente permanece ativa se o usuário não iniciar outro aplicativo.
  - Quando decorre um intervalo de tempo especificado. 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 do grupo de entrega excede uma porcentagem especificada: 1—99%.
  - Quando a carga em qualquer máquina do grupo de entrega excede uma porcentagem especificada: 1—99%.

Resumo: Uma sessão prolongada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicie um aplicativo, o tempo especificado passe ou um limite de carga especificado seja excedido.

## Controle a reconexão da sessão quando desconectado da máquina no modo de manutenção

### NOTA:

Esse recurso está disponível somente no PowerShell.

Você pode controlar se as sessões que estão desconectadas em máquinas no modo de manutenção podem se reconectar às máquinas no grupo de entrega.

Antes da versão 2106, a reconexão não era permitida para sessões de desktop em pool de sessão única que haviam sido desconectadas das máquinas no 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 no 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 no modo de manutenção.

- Quando definido como verdadeiro, as sessões podem se reconectar às máquinas do grupo.
- Quando definidas como false, as sessões não podem se reconectar às máquinas do grupo.

Valores padrão:

- Sessão única: desativada
- Sessão múltipla: ativada

## Configurar o roaming da sessão

Por padrão, o roaming de sessões está habilitado para grupos de entrega. As sessões circulam entre os dispositivos do cliente com o usuário. Quando o usuário inicia uma sessão e depois muda para outro dispositivo, a mesma sessão é usada e os aplicativos ficam disponíveis simultaneamente nos dois dispositivos. Você pode visualizar os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo ou da existência de sessões atuais. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem. Como alternativa, 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 **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar grupo de entrega** na barra de ação.
3. Na página **Usuários**, ative o roaming de sessão marcando a caixa de seleção **As sessões roam com os usuários à medida que eles se movem entre os dispositivos**.
  - Quando ativada, se um usuário iniciar uma sessão de aplicativo e depois passar para outro dispositivo, a mesma sessão será usada e estará disponível em ambos os dispositivos. Quando desativada, a sessão não se desloca mais entre dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

**Configurar o roaming de sessão para desktops** Para configurar o roaming de sessão para um desktop, siga estas etapas:

1. No console, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ação.
3. Na página **Desktops**, selecione a área de trabalho e selecione **Edit**.
4. Ative o roaming da sessão marcando a caixa de seleção **Roaming da sessão**.
  - Quando ativada, se o usuário iniciar a área de trabalho e depois passar para outro dispositivo, a mesma sessão será usada e os aplicativos estarão disponíveis nos dois dispositivos. Quando desativada, a sessão não se desloca mais entre dispositivos.

Selecione **OK** para aplicar as alterações e fechar a janela.

## Solucionar problemas

- Os VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização de recursos disponíveis de outra forma. Há vários motivos pelos quais um VDA pode não estar registrado, muitos dos quais um administrador pode solucionar. A exibição de detalhes fornece informações sobre solução de problemas no assistente de criação de catálogos e depois de adicionar um catálogo a um grupo de entrega.

Depois de criar um grupo de entrega, o painel de detalhes de um grupo de entrega indica o número de máquinas que podem ser registradas, mas não estão. Por exemplo, uma ou mais máquinas estão ligadas e não estão no modo de manutenção, mas não estão atualmente registradas em um controlador. Ao visualizar uma máquina “não registrada, mas deveria estar”,

consulte a guia **Solução de problemas** no painel de detalhes para ver as possíveis causas e as ações corretivas recomendadas.

Para mensagens sobre o nível funcional, consulte [Versões do VDA e níveis funcionais](#).

Para obter informações sobre 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 tela de programas e recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas com o status **Power State Unknown**, consulte [CTX131267](#) para obter orientação.

## Remote PC Access

August 22, 2024

### Nota:

Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente 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 Remote PC Access é um recurso do Citrix Virtual Apps and Desktops que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

O Remote PC Access usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam áreas de trabalho e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos que os necessários para implantar o Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

O recurso consiste em um catálogo de máquinas do tipo **Remote PC Access** que proporciona a essa funcionalidade:

- Capacidade de adicionar máquinas especificando unidades organizacionais. Essa capacidade facilita a adição de PCs em massa.
- Atribuição automática do usuário com base no usuário que faz login no PC Windows do escritório. Oferecemos suporte a atribuições de usuário único e multiusuário. Por padrão, atribuímos automaticamente vários usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, entre no Web Studio, vá para **Settings** e desative a configuração **Enable automatic assignment of multiple users for Remote PC Access**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs físicos Linux
- PCs físicos em pool (isto é, aleatoriamente atribuídos, não dedicados)

#### Notas:

Para obter detalhes sobre as versões do SO com suporte, consulte os requisitos do sistema para o VDA para [SO de sessão única](#) e [Linux VDA](#).

Para implantações locais, o Remote PC Access é válido apenas para licenças do Citrix Virtual Apps and Desktops Advanced ou Premium. As sessões consomem licenças da mesma maneira que outras sessões do Citrix Virtual Desktops. No caso do Citrix Cloud, o Remote PC Access é válido para o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) e Workspace Premium Plus.

## Considerações

Embora todos os requisitos e considerações técnicas que se aplicam ao Citrix Virtual Apps and Desktops em geral também se apliquem ao Remote PC Access, alguns podem ser mais relevantes ou exclusivos para casos de uso de PC físico.

#### Importante:

Os sistemas físicos do Windows 11 (e alguns que executam o Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software do VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:

- Use a opção “/physicalmachine” juntamente com a opção “/remotepc” como parte da instalação da linha de comando do VDA
- Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada acima não tenha sido usada  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`  
- Nome: ForceEnableRemotePC

- Tipo: DWORD
- Dados: 1

## Considerações sobre implantação

Ao planejar a implantação do Remote PC Access, adote algumas medidas gerais.

- Você pode adicionar o Remote PC Access a uma implantação existente do Citrix Virtual Apps and Desktops. Antes de escolher essa opção, considere o seguinte:
  - Os Delivery Controllers ou os Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os bancos de dados locais do site e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os VDAs existentes e os novos VDAs do Remote PC Access ultrapassam o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs no escritório por meio de um processo automatizado. A seguir estão as opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: [Instale VDAs usando SCCM](#).
  - Scripts de implantação: [Instale VDAs usando scripts](#).
- Veja as [Considerações de segurança do Remote PC Access](#).

### Nota:

Ao projetar o acesso ao PC remoto, você deve considerar o número de monitores físicos conectados à GPU no PC remoto e atualmente configurados/operacionais. Mesmo que o monitor não seja usado na sessão Citrix, mas seja detectado pela GPU, a presença do monitor é computada no limite máximo de monitores suportados pela GPU.

## Considerações do catálogo de máquinas

O tipo de catálogo de máquinas exigido depende do caso de uso:

- Catálogo de máquinas de Remote PC Access
  - PCs Windows dedicados
  - PCs Windows multiusuário dedicados Esse caso de uso se aplica a PCs físicos de escritório que vários usuários podem acessar remotamente em turnos diferentes.

- PCs Windows em pool. Esse caso de uso se aplica a PCs físicos que vários usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas com SO de sessão única
  - Estático - PCs Linux dedicados
  - Aleatório - PCs Linux em pool

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.
- Ao escolher as UOs em que as contas da máquina residem, selecione UOs de nível inferior para obter maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de bancos/caixas/guichês, selecione **Tellers** para obter maior granularidade. Caso contrário, você pode selecionar **Officers** ou **Bank** baseado nas exigências.
- Mover ou excluir UOs depois de atribuídas a um catálogo de máquinas de Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Portanto, tenha o cuidado de planejar adequadamente para que as atualizações de atribuição da unidade organizacional a catálogos de máquina sejam contabilizadas no plano de alteração do Active Directory.
- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas por causa da estrutura de unidade organizacional, 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 da área de trabalho estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo da máquina juntamente com as atribuições do usuário está disponível em [GitHub](#).
- Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Remote PC Access**.

## Considerações do Linux VDA

Estas considerações são específicas para o Linux VDA:

- Use o Linux VDA em máquinas físicas somente no modo não 3D. Devido a limitações do driver do NVIDIA, a tela local do PC não pode ser desligada e exibe as atividades da sessão quando o modo HDX 3D está ativado. Mostrar essa tela é um risco de segurança.
- Use catálogos de máquina do tipo SO de sessão única para máquinas físicas Linux.
- A atribuição automática de usuário não está disponível para máquinas Linux.

- Se os usuários já estiverem conectados em seus PCs localmente, as tentativas de iniciar os PCs a partir do StoreFront falharão.
- Opções de economia de energia não estão disponíveis para máquinas Linux.

## Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e as considerações para PCs físicos.

- Não há suporte para:
  - Chaveadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo notebooks e PCs All-in-One e NVIDIA Optimus.
  - Máquinas de inicialização dupla.
- Conecte o teclado e o mouse diretamente ao PC. Esses periféricos poderão se tornar indisponíveis se forem conectados ao monitor ou a outros componentes que podem ser desligados ou desconectados. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desative os componentes.
- Os PCs devem ser ingressados em um domínio do Active Directory Domain Services
- A Inicialização Segura é suportada apenas no Windows 10 e Windows 11.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é recomendada para ter-se maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:
  1. Defina as configurações de energia para deixar o adaptador sem fio ligado.
  2. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registra até que o usuário faça logon. O PC não está disponível para acesso remoto até que um usuário tenha feito logon.
  3. Certifique-se de que os Delivery Controllers ou os Cloud Connectors possam ser acessados da rede Wi-Fi.
- Você pode usar o Remote PC Access em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:
  1. Desative o recurso de hibernação.
  2. Desative o recurso de suspensão.
  3. Defina a ação de fechar a tampa como **Não fazer nada**.
  4. Defina a ação “pressionar o botão de energia” como **Desligar**.

5. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Remote PC Access é suportado em dispositivos Surface Pro com Windows 10. Siga as mesmas instruções para laptops mencionadas anteriormente.
- Se estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixa o laptop, o VDA se registra novamente nos Delivery Controllers ou Cloud Connectors por Wi-Fi. No entanto, quando você reencaixa o laptop, o VDA não muda para a conexão com fio, a menos que você desconecte o adaptador de conexão sem fio. Alguns dispositivos fornecem funcionalidade interna para desconectar o adaptador de conexão sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador de conexão sem fio. Revise as considerações de Wi-Fi mencionadas anteriormente.

Faça o seguinte para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

1. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão**, e defina **Suspender** como **Nunca**.
  2. Em **Gerenciador de dispositivos > Adaptadores de rede > Adaptador Ethernet** vá para **Gerenciamento de energia** e desmarque **O computador pode desligar o dispositivo para economizar energia**. Assegure que **Permitir que este dispositivo acorde o computador** esteja selecionado.
- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, o recurso aparece como indisponível se já estiver sendo usado por outro usuário.
  - Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

## Sequência de configuração

Esta seção contém uma visão geral de como configurar o Remote PC Access ao usar o catálogo da máquinas do tipo **Remote PC Access**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte [Criar catálogos de máquina](#).

1. Somente site local –Para usar o recurso Wake on LAN integrado, configure os pré-requisitos descritos em [Wake on LAN](#).
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para o Remote PC Access:
  - a) Selecione o tipo de site **Remote PC Access**.
  - b) Em **Power Management**, escolha se deseja ativar ou desabilitar o gerenciamento de energia para o catálogo de máquinas Remote PC Access. Você pode alterar essa configuração

posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte [Wake on LAN](#).

- c) Forneça as informações nas páginas **Users** e **Machine Accounts**

Ao concluir essas etapas, é criado um catálogo de máquinas chamado **Remote PC Access Machines** e um grupo de entrega chamado **Remote PC Access Desktops**.

3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:
  - a) Crie um catálogo de máquinas do tipo **Remote PC Access** (página Operating System do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte [Criar catálogos de máquinas](#). Tenha o cuidado de atribuir a unidade organizacional correta para que os PCs de destino sejam disponibilizados para uso com o Remote PC Access.
  - b) Crie um grupo de entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um grupo de entrega, consulte [Criar grupos de entrega](#). Certifique-se de atribuir o grupo de entrega a um grupo do Active Directory que contém os usuários que exigem acesso a seus PCs.
4. Implantar o VDA nos PCs do escritório.

- Recomendamos usar o instalador de VDA básico de SO de sessão única (VDAWorkstation-CoreSetup.exe).
- Você também pode usar o instalador de VDA completo de sessão única (VDAWorkstation-Setup.exe) com a opção `/remotepc/physicalmachine`, que chega ao mesmo resultado que o uso do instalador de VDA básico.

**Nota:**

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.

- Ative a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto por meio do Citrix Director. Para isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte [Instalar usando a linha de comando](#).
- Para poder ver as informações de duração de logon no Director, você deve usar o instalador de VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Para incluir esse componente, use a opção `/includeadditional`. Para obter detalhes, consulte [Instalar usando a linha de comando](#).
- Para obter informações sobre como implantar o VDA usando o SCCM, consulte [Instalar VDAs usando SCCM](#).



- Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte [Instalar VDAs usando scripts](#).

Depois que você concluir com êxito as etapas 2 a 4, os usuários são atribuídos automaticamente às suas próprias máquinas quando fazem logon localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente usado para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace está disponível em <https://www.citrix.com/downloads/> ou nas lojas de aplicativos para dispositivos móveis com suporte.

## Recursos gerenciados através do registro

### Cuidado:

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

## Desativar atribuições automáticas de multiusuário

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 Remote PC Access entre em um estado de suspensão, adicione a configuração de registro ao VDA e reinicialize a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra no modo de suspensão depois que o timer pré-configurado de inatividade expira. Depois que a máquina acorda, ela se registra novamente no Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dados: 1

## Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é desconectada automaticamente quando um usuário local inicia uma sessão na máquina (pressionando CTRL+ALT+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e reinicialize a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Dados: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é confirmada dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dados:
  - 1 - O usuário remoto sempre tem prioridade se não responder à mensagem na interface do usuário dentro do período de tempo limite especificado. Esse comportamento é o padrão se esse parâmetro não estiver configurado.
  - 2 - O usuário local tem prioridade.

O tempo limite padrão para impor o modo Remote PC Access é de 30 segundos. Você pode configurar esse tempo limite, mas não o defina abaixo de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dados: número de segundos do tempo limite em valores decimais

Quando um usuário quiser forçar o acesso ao console, o usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local da sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon no PC enquanto estiver em uso por um usuário remoto, o usuário remoto receberá uma mensagem. A mensagem pergunta se deve permitir ou negar a conexão do usuário local. Permitir que a conexão desconecta a sessão do usuário remoto.

## Log de gerenciamento de sessão

O Remote PC Access agora tem recursos de log que registram quando alguém tenta acessar um PC com uma sessão ativa do ICA. Isso permite que você monitore seu ambiente em busca de atividades indesejadas ou inesperadas e seja capaz de auditar esses eventos se precisar investigar incidentes.

Os eventos são registrados no log usando o Visualizador de Eventos do Windows e estão em **Applications and Services > Citrix > HostCore > ICA Service > Admin**.

Há três eventos distintos que são registrados no log ao usar o Remote PC Access.

### 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: Application and Services
- 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:

```
1 Ctrl+Alt+Del has been pressed on the endpoint.  
2 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:

```
1 Ctrl+Alt+Del has been pressed on the endpoint.  
2 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:

```
1      Ctrl+Alt+Del has been pressed on the endpoint.
2      The session management behavior is set to notify the
       remote user.
3      The user preference is set to local user.
```

### Evento de desconexão de sessão remota

Este evento aparece quando a sessão remota é desconectada por diferentes motivos.

#### Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 46, 47, 48
- Fonte: ICA Service

**ID do evento 46** Este ID de evento aparece quando a sessão remota é desconectada e quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:

```
1      The remote session for <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:

```
1      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:

```
1 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: Application and Services
- ID do evento: 49
- Fonte: ICA Service

**ID do evento 49** Este ID de evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

- Mensagem:

```
1 The remote session for <remoteUserName> has been forcibly
disconnected.
```

#### Wake on LAN

O Remote PC Access suporta Wake on LAN, o que dá aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs no escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina for desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede em que o PC reside quando instruído pelo Delivery Controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura extras ou soluções de terceiros para a entrega dos pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN legado baseado em SCCM. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte [Wake on LAN —SCCM integrado](#).

#### Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes sobre a capacidade de suporte, consulte os [Requisitos do sistema para VDA](#).
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows

### Configurar o Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops no local, a configuração do Wake on LAN integrado só será suportada usando o PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas Remote PC Access se ainda não tiver um.
2. Crie a conexão de host Wake on LAN se ainda não tiver uma.

**Nota:**

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. Obtenha o identificador exclusivo da conexão de host Wake on LAN.
4. Associe a conexão de host Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host Wake on LAN:

```
1 # Load Citrix SnapIns
2 Add-PSSnapIn -Name "*citrix*"
3
4 # Provide the name of the Wake on LAN host connection
5 [string]$connectionName = "Remote PC Access Wake on LAN"
6
7 # Create the hypervisor connection
8 $hypHc = New-Item -Path xdhyp:\Connections `
9             -Name $connectionName `
10            -HypervisorAddress "N/A" `
11            -UserName "woluser" `
12            -Password "wolpwd" `
13            -ConnectionType Custom `
```

```
14         -PluginId VdaWOLMachineManagerFactory `
15         -CustomProperties "<CustomProperties></CustomProperties
16         >" `
17         -Persist
18 $bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionId
19     $hypHc.HypervisorConnectionId
20 # Wait for the connection to be ready before trying to use it
21 while (-not $bhc.IsReady)
22 {
23
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionId
26     $hypHc.HypervisorConnectionId
27 }
```

Quando a conexão do host estiver pronta, execute os seguintes comandos para obter o identificador exclusivo de conexão do host:

```
1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid
```

Depois de obter o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo da máquinas do Remote PC Access:

```
1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
2 RemotePCHypervisorConnectionId $hypUid
```

### Considerações de design

Ao planejar o uso do Wake on LAN com Remote PC Access, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host Wake on LAN.
- Para que um PC acorde outro PC, os dois PCs devem estar na mesma sub-rede e usar a mesma conexão de host Wake on LAN. Não importa se os PCs estão no mesmo catálogo de máquinas ou em catálogos diferentes.
- As conexões de host são atribuídas a zonas específicas. Se a sua implantação contém mais de uma zona, você precisa de uma conexão de host Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Os pacotes mágicos são transmitidos usando o endereço de transmissão global 255.255.255.255. Certifique-se de que o endereço não esteja bloqueado.
- Deve haver pelo menos um PC ligado na sub-rede –para cada conexão Wake on LAN –para conseguir acordar as máquinas nessa sub-rede.

## Considerações operacionais

Veja as considerações a seguir para usar o recurso Wake on LAN:

- O VDA deve se registrar pelo menos uma vez antes que o PC possa ser ativado usando o recurso Wake on LAN integrado.
- Wake on LAN só pode ser usado para acordar PCs. Ele não suporta outras ações de energia, como reinicializar ou desligar.
- 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 você estiver usando o Citrix Virtual Apps and Desktops no local.
- Os pacotes mágicos são enviados de uma destas duas maneiras:
  1. Quando um usuário tenta iniciar uma sessão no PC e o VDA não está registrado
  2. Quando um administrador envia manualmente um comando de envio de energia a partir do Web Studio ou do PowerShell
- Como o Delivery Controller não tem conhecimento do estado de energia de um PC, o Web Studio exibe **Not Supported** 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 a SCCM

O Wake on LAN integrado a SCCM é uma opção alternativa de Wake on LAN para Remote PC Access que só está disponível com o Citrix Virtual Apps and Desktops local.

### Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN integrado a SCCM:

- Citrix Virtual Apps and Desktops 1912 ou posterior
- PCs físicos:
  - VDA versão 1912 ou posterior
  - Windows 10. Para obter detalhes sobre a capacidade de suporte, consulte os [Requisitos do sistema para VDA](#).
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou posterior



## Configurar Wake on LAN integrado a SCCM

Conclua os seguintes pré-requisitos:

1. Configure o SCCM 2012 R2, 2016 ou 2019 dentro da organização. Em seguida, implante o cliente SCCM em todas as máquinas de Remote PC Access, dando tempo suficiente para que o ciclo de inventário do SCCM agendado seja executado, ou force um manualmente, se necessário.
2. Para dar suporte ao proxy de ativação, ative a opção no SCCM. Para cada sub-rede na organização que contém PCs que usam o recurso Remote PC Access Wake on LAN, certifique-se de que três ou mais máquinas possam servir como máquinas sentinelas.
3. Para obter suporte a pacotes mágicos, configure roteadores de rede e firewalls para permitir que os pacotes mágicos sejam enviados usando uma transmissão direcionada por sub-rede ou unicast.
4. Configure o Wake on LAN nas configurações BIOS/UEFI de cada PC.
5. Implante o VDA nos PCs físicos se ainda não tiver feito.

Depois de tratar dos pré-requisitos, execute 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 **Remote Tools Operator**.
2. Selecione a conexão no Web Studio e, em seguida, selecione **Edit Connection** e clique em **Advanced**.
3. Selecione a opção apropriada para lidar com Wake on LAN:
  - Se estiver usando o proxy de ativação, selecione a primeira opção: **Microsoft System Center Configuration Manager Wake-up proxy**.
  - Se estiver usando pacotes mágicos, selecione a segunda opção: **Wake on LAN packets transmitted by the Delivery Controller**.
    - Selecione o método de transmissão apropriado: **subnet-directed broadcasts** ou **unicast**.

Depois de criar a conexão de host, associe a conexão a um catálogo Remote PC Access:

- Se você estiver criando um novo catálogo Remote PC Access, na página **Operating System** 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 Wake on LAN a um catálogo Remote PC Access existente:

1. No Web Studio, vá para o nó **Machine Catalogs**, selecione o catálogo da máquinas e, em seguida, selecione **Edit Machine Catalog**.
2. Selecione a guia **Power Management** e escolha **Yes** para permitir o gerenciamento de energia do catálogo de máquinas.
3. Selecione a conexão apropriada na lista suspensa e clique em **OK**.

## Solucionar problemas

### Desligamento do monitor não funciona

Se o monitor local do PC Windows não for desligado enquanto houver uma sessão HDX ativa (o monitor local exibir o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê prioridade maior ao Citrix Indirect Display Driver (IDD) do que ao driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para obter mais detalhes sobre as prioridades do adaptador de exibição e criação de monitor, consulte o artigo [CTX237608](#) do Knowledge Center.

### A sessão desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão ativada

A notificação de gerenciamento de sessão controlada pelo valor do registro **SasNotification** funciona somente quando o modo Remote PC Access está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

## Informações de diagnóstico

As informações de diagnóstico sobre o Remote PC Access são gravadas no log de Eventos de Aplicativos do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas, descartando-se as mensagens duplicadas.

- 3300 (informativo): máquina adicionada ao catálogo
- 3301 (informativo): máquina adicionada ao grupo de entrega
- 3302 (informativo): máquina atribuída ao usuário
- 3303 (erro): exceção

## Gerenciamento de energia

Se o gerenciamento de energia do Remote PC Access estiver ativado, as transmissões direcionadas por sub-rede não iniciarão máquinas que estejam em uma sub-rede diferente daquela do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando transmissões direcionadas por sub-rede e o suporte AMT não estiver disponível, tente o método Wake-up proxy ou Unicast. Certifique-se de que essas configurações estejam ativadas nas propriedades avançadas para a conexão de gerenciamento de energia.

## A sessão remota ativa registra a entrada local da tela sensível ao toque

Quando o VDA habilita o modo Remote PC Access, a máquina ignora a entrada local da tela sensível ao toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

## Mais recursos

Veja a seguir outros recursos para Remote PC Access:

- Orientação sobre o projeto da solução: [Remote PC Access Design Decisions](#)

- Exemplos de arquiteturas do Remote PC Access: [Reference Architecture for Citrix Remote PC Access Solution](#).

## Atualize e migre

January 24, 2025

### Introdução

A atualização altera sua implantação no Citrix Virtual Apps and Desktops 7 **Current Release (CR)** sem precisar configurar novas máquinas ou sites. Isso é conhecido como atualização in-loco.

A atualização oferece acesso aos recursos e tecnologias mais recentes para os quais você está qualificado. As atualizações também podem conter correções, esclarecimentos e aprimoramentos de versões anteriores.

### Visão geral do upgrade

1. Leia o artigo [Atualizar uma implantação](#) antes de começar a atualização. Essa é a principal fonte de informações para aprender como se preparar e implementar uma atualização.
2. Certifique-se de que as datas atuais do Customer Success Services sejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo [sobre licenças de renovação do Customer Success Services](#).
3. Complete a orientação de preparação.
4. Execute instaladores para atualizar os componentes principais.
5. Atualize os bancos de dados do sistema e o site.
6. Atualize VDAs em imagens (ou diretamente em máquinas).
7. Atualize outros componentes.

Cada etapa de preparação e atualização está detalhada em [Atualizar uma implantação](#).

### Versões que você pode atualizar

Você pode fazer o upgrade para o Citrix Virtual Apps and Desktops 2402 LTSR a partir de:

- Aplicativos e desktops virtuais 2203 LTSR com ou sem CUs, até e incluindo CU5
- Aplicativos e desktops virtuais 1912 LTSR com ou sem CUs, até e incluindo CU9
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

Nota:

- Antes de iniciar o processo de atualização, a Citrix recomenda que os clientes testem a atualização em um ambiente controlado e verifiquem se ela atende aos requisitos específicos. Além disso, aconselhamos a revisão de toda a documentação relevante do produto, incluindo a lista de descontinuação e os problemas conhecidos, para garantir uma transição perfeita. 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 logo atingirá sua fase de fim de vida útil. Para obter mais informações sobre a lista de versões suportadas, consulte [Matriz de produtos](#).

## Perguntas frequentes

Esta seção responde a algumas perguntas frequentes sobre a atualização do Citrix Virtual Apps and Desktops.

- **Qual é a ordem correta para atualizar meu ambiente de aplicativos e desktops virtuais?**

Para obter uma ilustração e uma descrição da sequência de atualização recomendada, consulte [Sequência de atualização](#) e [Procedimento de atualização](#).

- **Meu site tem vários controladores de entrega (em zonas diferentes). O que acontece se eu atualizar somente alguns deles? Preciso atualizar todos os controladores no site durante a mesma janela de manutenção?**

A melhor prática é atualizar 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 atualize metade dos Controllers, atualize o site e, em seguida, atualize os Controllers restantes. Para obter detalhes, consulte o procedimento de atualização .

- **Posso ir diretamente para a versão mais recente ou preciso fazer atualizações incrementais?**

Quase sempre é possível atualizar para a versão mais recente e pular as versões intermediárias, a menos que seja explicitamente declarado no artigo **What's new** sobre a versão para a qual você está atualizando.- **Um cliente pode fazer o upgrade de um ambiente Long Term Service Release (LTSR) para uma versão atual?**

Sim Os clientes não precisam permanecer em uma versão de serviço de longo prazo por um período prolongado. Os clientes podem migrar um ambiente LTSR para uma versão atual, 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, todos os recursos da versão mais recente podem não estar disponíveis. Para obter mais informações, consulte [Considerações sobre ambientes mistos](#).

- **Com que frequência uma versão atual deve ser atualizada?**

As versões atuais atingem o fim da manutenção (EOM) 6 meses após a data de lançamento. A Citrix recomenda que os clientes adotem a versão atual mais recente. Os lançamentos atuais chegam ao fim da vida útil (EOL) 18 meses após a data de lançamento.- **O que é recomendado: atualizar para LTSR ou CR?**

As versões atuais (CRs) oferecem os recursos e funcionalidades mais recentes e inovadores de virtualização de aplicativos, desktops e servidores. Isso permite que você permaneça com tecnologia de ponta e à frente da concorrência.

As versões de serviço de longo prazo (LTSRs) são ideais para ambientes de produção de grandes empresas que preferem manter a mesma versão básica por um longo período.

- **Preciso atualizar minhas licenças?**

Certifique-se de que a data da licença atual não tenha expirado e seja válida para a versão para a qual você está atualizando. Veja [CTX111618](#). Para obter informações sobre renovação, consulte [Licenças de renovação do Customer Success Services](#).

- **Quanto tempo leva um upgrade?**

O tempo necessário para atualizar uma implantação varia, dependendo da infraestrutura e da rede. Portanto, não podemos fornecer uma hora exata.

- **Quais são as melhores práticas?**

Certifique-se de entender e seguir a orientação de preparação .

- **Quais sistemas operacionais são compatíveis?**

O artigo [Requisitos do sistema](#) da versão para a qual você está atualizando lista os sistemas operacionais compatíveis.

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 compatíveis, além de links para problemas conhecidos.

- **Quando minha versão entrará em EOL?**

Verifique a matriz de produtos .

- **Quais são os problemas conhecidos com a versão mais recente?**

- [Aplicativos e desktops virtuais Citrix](#)
- [Vitrine](#)
- [Provisionamento Citrix](#)
- [Servidor de licenças Citrix](#)
- [Aplicativo Citrix Workspace para Windows](#)

## **Mais informações Long Term Service Release (LTSR) As atualizações de implantação usam atualizações cumulativas (CUs). Uma UC atualiza os componentes básicos do LTSR, e cada UC inclui seu próprio metainstaller**

Cada UC tem documentação dedicada. Por exemplo, para o LTSR 2203, verifique o link na página **What's new** do LTSR para ver a última UC. Cada página da UC inclui informações sobre a versão suportada, instruções e um link para o pacote de download da UC.

## **Migrar**

### **Migre 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 obter mais informações, consulte [Migrar para a nuvem](#).

### **Migração legada**

A migração move os dados de uma implantação anterior para uma versão mais recente. O processo inclui a instalação de componentes mais novos e a criação de um novo site, a exportação de dados da fazenda antiga e a importação dos dados para o novo site.

Não há ferramentas ou scripts compatíveis para migrar versões do XenApp e XenDesktop ou migrar versões anteriores do Citrix Virtual Apps and Desktops. *A atualização é compatível com as versões do Citrix Virtual Apps and Desktops descritas nesta documentação do produto.*

Para ver o conteúdo de migração anterior do XenApp 6.x, consulte o seguinte. Nem os scripts nem os artigos são suportados ou mantidos.

- Os scripts de migração de código aberto para as versões do XenApp 6.x estão disponíveis em <https://github.com/citrix/xa65migrationtool>. A Citrix não oferece suporte nem mantém esses scripts de migração.
- [Mudanças na versão 7.x](#)
- [Atualize um funcionário do XenApp 6.5 para um novo VDA](#)
- [Migre o XenApp 6.x](#)

## Atualizar uma implantação

January 24, 2025

### Nota:

Este artigo aborda atualizações para implantações envolvendo o Web Studio. Para obter informações sobre atualizações envolvendo o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

### Introdução

Você pode atualizar determinadas implantações para versões mais recentes sem precisar primeiro configurar novas máquinas ou sites. 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 fazer o upgrade para qualquer uma das versões do Citrix Virtual Apps and Desktops, certifique-se de que as datas atuais do Customer Success Services sejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo [sobre licenças de renovação do Customer Success Services](#).

Para iniciar uma atualização, você executa o instalador a partir da nova versão para atualizar os componentes principais, VDAs e alguns outros componentes instalados anteriormente. Em seguida, você atualiza os bancos de dados e o site.

Você pode atualizar qualquer componente que possa ser instalado com o instalador completo do produto (e os instaladores autônomos do VDA), se houver uma versão mais recente fornecida. Para outros componentes que não estão instalados com o instalador completo do produto (como Citrix Provisioning and 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. O procedimento de atualização contém detalhes de cada etapa no diagrama.

[Diagrama de fluxo da sequência de atualização](#)



**Nota:**

Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer tarefa relacionada ao grupo de provisionamento e 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 Hybrid Rights são licenças de assinatura por prazo que são fornecidas, além da assinatura do serviço em nuvem, quando um cliente faz a transição ou troca de uma licença perpétua para uma assinatura de serviço em nuvem. Você também pode comprar um complemento Hybrid Rights com suas assinaturas de DaaS.

Se você tiver uma licença Hybrid Rights com um atributo SaaS, ao atualizar para o Citrix Virtual Apps and Desktops LTSR 2203 e posterior, você se torna 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 servidor de licenças 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 o atributo SaaS:

**Nota:**

- Você recebe um e-mail com um novo código de licença. Para obter mais informações, consulte [Use o código de acesso à licença](#).
- Suas licenças existentes foram rescindidas. As licenças rescindidas devem ser excluídas dos servidores de licenças, seguidas pela instalação de uma nova licença. Para obter mais informações, consulte [Excluindo arquivos de licença](#).

1. Acesse o portal [citrix.com](https://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 Incrementos.

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
VENDOR_STRING=;LT=Retails;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS;SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
Systems Inc." SN=RetailSSaaS SIGN="..."
```

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 broker para definir a edição e o modelo e, em seguida, iniciar a atualização local. Para obter mais informações sobre os comandos do Broker, consulte a seção [Broker PowerShell SDK](#).

Para obter mais informações sobre o suporte à nuvem pública com as versões atuais e de serviços de longo prazo do Citrix Virtual Apps and Desktops, 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 License Server), 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 completa do instalador do produto, faça login 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 [Instale usando a linha de comando](#).

## Etapa 1: Preparar

Antes de começar um upgrade, verifique se você está pronto. Leia e conclua todas as tarefas necessárias:

- Remova PVD, AppDisks e hosts não suportados
- VDAs que têm componentes PVD ou AppDisk
- Limitações
- Considerações sobre ambientes mistos
- Sistemas operacionais anteriores
- Preparação
- Testes preliminares no local
- Verificação da versão do SQL Server

## **Etapa 2: Atualizar o servidor de licenças**

Se a instalação tiver uma nova versão do software Citrix License Server, atualize esse componente primeiro antes de qualquer outro componente.

Se você ainda não determinou com o se o seu Servidor de Licenças é compatível com a nova versão, é essencial que você execute o instalador no Servidor de Licenças 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 **Extend deployment**.
- 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: Upgrade 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 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 com os controladores restantes. Pode haver momentos em que o site tenha capacidade reduzida porque há menos controladores disponíveis. A atualização causa apenas uma breve interrupção no estabelecimento de novas conexões de clientes 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 seu site tiver apenas um controlador, ele ficará inoperante durante a atualização.

Testes preliminares no local são executados no primeiro controlador, 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.

#### **Nota:**

Depois de atualizar o Web Studio, as informações da 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, acesse o servidor Web Studio, abra o Gerenciador de Serviços de Informações da Internet (IIS), navegue até 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 o banco de dados e o site**

#### **Nota:**

Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer tarefa relacionada ao grupo de provisionamento e 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 obter 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 Atualize 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 administrador do 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 ativam e desativam 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 Atualize o banco de dados e o site manualmente.

- Se você tiver uma implantação em várias zonas 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 da atualização. Consulte CTX135207. Durante uma atualização do banco de dados, os serviços do produto são desativados. Durante esse período, os controladores não podem intermediar novas conexões para o site, portanto, planeje com cuidado.

### **Atualize 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 continua.

### **Atualize 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 com o Servidor de Licenças e solicita confirmação.
3. Confirme se 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 atualização da versão do produto, esse script não será gerado. Por exemplo, se o esquema do banco de dados de registro não mudar, o script `UpgradeLoggingDatabase.sql` não será gerado.

4. Execute os scripts a seguir na ordem mostrada.
  - `DisableServices.ps1`: O usuário do Studio executa esse script do PowerShell em um controlador para desativar os serviços do produto.
  - `UpgradeSiteDatabase.sql`: O administrador do banco de dados executa esse script SQL no servidor que contém o banco de dados do site
  - `UpgradeMonitorDatabase.sql`: O administrador do banco de dados executa esse script SQL no servidor que contém o banco de dados Monitor.
  - `UpgradeLoggingDatabase.sql`: O administrador do banco de dados executa esse script SQL no servidor que contém o banco de dados do Configuration Logging. Execute esse script somente se esse banco de dados mudar (por exemplo, depois de aplicar um hotfix).

- [EnableServices.ps1](#): O usuário do Studio executa esse script do PowerShell em um controlador para habilitar os serviços do produto.

Depois que a atualização do banco de dados for concluída e os serviços do produto forem habilitados, o Studio testa automaticamente o ambiente e a configuração e, em seguida, gera um relatório HTML. Se forem identificados problemas, você poderá restaurar o backup do banco de dados. Depois de resolver os problemas, você pode atualizar o banco de dados novamente.

5. Depois de 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** *site-name* no painel de navegação. Na guia **Tarefas comuns**, selecione **Atualizar os controladores de entrega restantes**.

### Nota:

Para disponibilizar o **Upgrade restante dos Delivery Controllers**, crie pelo menos um catálogo de máquinas e um grupo de entrega para o site.

Depois de 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 criar um ID de zona, caso ele não exista.

## Etapa 11: atualizar os 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 em máquinas que contêm VDAs.

Se você usou o Machine Creation Services e uma imagem mestre para criar máquinas, acesse 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 grupos de entrega

- [Atualize catálogos que usam máquinas com VDAs atualizados.](#)
- [Atualize catálogos que usam máquinas com VDAs atualizados.](#)
- [Atualize grupos de entrega 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:

- [Vitrine](#)
- [DNA do aplicativo](#)
- [Camadas de aplicativos Citrix](#)
- [Pacote de otimização HDX RealTime](#)
- [Gerenciamento de perfil](#)
- [Provisionamento Citrix](#)
- [Gravação da sessão](#)
- [Gerenciamento do ambiente de trabalho](#)

Se você precisar substituir o software Microsoft SQL Server Express LocalDB por uma versão posterior, consulte [Substituir o SQL Server Express LocalDB](#).

### Atualização do Dbschema

Quando você atualiza 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 RTM	2203 CU1	2203 CU2	2203 CU3
7.15 RTM/ CU	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU1		Site	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU2			Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU3				Site; Monitor; config	Site; Monitor; config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU4					Site; Config	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU5						Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU6						Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
1912 CU7						Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging	Site; Monitor; config; logging
2203 RTM							Config	Config	Config
2203 CU1								Config	Config
2203 CU2									Config

Definição dos termos:

- **Site:** Site Datastore. A atualização do Dbschema é feita no Site Datastore.
- **Monitor:** Monitore o Datastore. A atualização do Dbschema é feita no Monitor Datastore.
- **Configuração:** Tabela de configuração. A versão do Desktop Studio, as informações de licenciamento ou ambas são atualizadas na tabela de configuração.
- **Registro:** Registrando o Datastore. A atualização do Dbschema é feita no Logging Datastore.

## Atualize os VDAs para 2203 ou posterior

Se o componente Personal vDisk (PvD) já tiver sido instalado em um VDA, esse VDA não poderá 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 **Additional Components**.
- Na linha de comando, a opção `/baseimage` instalou o PvD. Se você especificou essa opção ou usou um script que continha essa opção, o PvD foi instalado.

Se você não sabe se o seu VDA tem o PvD instalado, execute o instalador do novo VDA (2203 ou posterior) na máquina ou na 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 confirme que você deseja fechar o instalador.
  - Na CLI, o comando simplesmente falha com a mensagem exibida.
- Se o PvD não estiver instalado, a atualização prosseguirá.

## O que fazer

Se o VDA não tiver o PvD instalado, siga o procedimento normal de atualização.

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 seus computadores Windows 10 (1607 e anteriores, sem atualizações), o VDA 7.15 LTSR é a versão mais recente com suporte.

### Nota:

*Posso usar o Personal vDisk com desktops Windows 7 no XenApp e no XenDesktop 7.15 LTSR?*

A Citrix excluiu o Personal vDisk (PvD) do XenApp e do XenDesktop 7.6 LTSR, anunciados 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 do XenDesktop 7.15 LTSR.



No entanto, para ajudar os clientes com implantações PvD existentes no Windows 7 a migrarem 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 do XenDesktop 7.15 LTSR até 14 de janeiro de 2020. O componente PvD será removido das CUs LTSR e não será suportado após 14 de janeiro de 2020. Além disso, o uso do PvD para Windows 7 após 14 de janeiro de 2020 tornará os sites LTSR não compatíveis. Além disso, o PvD para Windows 10 continua excluído do 7.15 LTSR. Portanto, os clientes não devem usá-lo em seus sites 7.15 LTSR.

## Remova PvD, AppDisks e hosts não suportados

As seguintes tecnologias e tipos de host não são suportados nas implantações da versão atual do Citrix Virtual Apps and Desktops 7:

- **Personal vDisks (PvD)** para armazenar dados ao lado das VMs dos usuários em catálogos. O recurso da camada de personalização do usuário agora lida com a persistência do usuário.
- **AppDisks** para gerenciar aplicativos usados em grupos de entrega.
- **Tipos de host:** Azure Classic, CloudPlatform (o produto Citrix original).
  - Para os tipos de host suportados nesta versão, consulte [Requisitos do sistema](#).
  - Para obter informações sobre formas alternativas de continuar usando o ARM e a 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 depois de remover itens que usam essas tecnologias. Se sua implantação atual usa conexões de hospedagem em nuvem pública (por exemplo, AWS), certifique-se de ter uma Licença de Direitos Híbridos antes de fazer o upgrade. Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença de Direitos Híbridos, a atualização é pausada ou interrompida e uma mensagem explicativa é exibida. Os registros 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, os MSIs relacionados podem ter sido incluídos em uma instalação ou atualização anterior do VDA. Antes de atualizar seus VDAs para a versão 2006 (ou uma versão compatível 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 obter detalhes, consulte [Atualizando VDAs que têm 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 grupos de entrega.

Para remover o 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. Do Studio, [exclua todos os catálogos](#) contendo máquinas que usam PvD.

**Atualizações de VDA:** A atualização de implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA o fazem. Para obter detalhes, consulte [VDAs que têm componentes PvD ou AppDisks](#).

Se você planeja usar o App Layering em vez do PvD, consulte [Migrando o PvD para o App Layering](#) para obter informações sobre a movimentação de dados.

### Remover AppDisks

Uma atualização de implantação não pode continuar até que você remova os AppDisks de todos os grupos de entrega que os usam e, em seguida, remova os próprios AppDisks.

1. Selecione **Delivery Groups** no painel de navegação do Studio.
2. Selecione um grupo e clique em **Gerenciar AppDisks** no painel Ação.
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 de implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA o fazem. 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 compatível posterior) não pode continuar se o site tiver conexões com tipos de host não suportados, como Citrix CloudPlatform ou Microsoft Azure Classic. Conclua as tarefas a seguir antes de tentar uma atualização.

Do estúdio:

- [Exclua todas as conexões](#) com 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.

### VDA's que têm 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.

#### Nota:

Ao atualizar para a versão 1912, você precisava desinstalar o VDA atual e instalar o novo VDA. Nesta versão, você será perguntado se 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 de VDA, a página **Additional Components** continha a opção **Citrix AppDisk/ Personal vDisk**. A 7.15 LTSR e as versões 7.x anteriores habilitaram essa opção por padrão. Portanto, se você aceitou os padrões (ou ativou explicitamente a opção em qualquer versão que a oferecesse), esse componente foi instalado.
- CLI: especificar a 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 prosseguirá 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 serão removidos automaticamente e a atualização continuará.
- CLI: Para evitar falhas no comando, inclua as seguintes opções no comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

## Limitações

As seguintes limitações se aplicam aos upgrades:

- **Instalação seletiva de componentes:** Se você instalar ou atualizar algum componente para a nova versão, mas optar por não atualizar outros componentes (em máquinas diferentes) que precisem de atualização, o Studio o lembra. 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 em que o Studio está instalado. O Studio não permitirá que você continue gerenciando 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 prévia de tecnologia:** Você não pode atualizar de uma versão de lançamento antecipado, prévia de tecnologia ou versão prévia.
- **Componentes em sistemas operacionais anteriores:** Você não pode instalar os VDAs atuais em sistemas operacionais que não são mais suportados pela Microsoft ou pela Citrix. Para obter mais informações, consulte Sistemas operacionais anteriores.
- **Ambientes/sites mistos:** Se você precisar continuar executando 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 nem especifica o produto (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) que foi definido durante a instalação.

## Considerações sobre ambientes mistos

Ao fazer o upgrade, a Citrix recomenda que você atualize todos os componentes e VDAs para poder acessar todos os recursos novos e aprimorados em sua edição e versão.

Por exemplo, embora você possa usar os VDAs atuais em implantações contendo versões anteriores do Controller, os novos recursos da versão atual podem não estar disponíveis. Problemas de registro do 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 da 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 do VDA e níveis funcionais](#).

### **Vários sites com versões diferentes**

Quando seu ambiente contém sites com diferentes versões do 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 do produto. Para obter detalhes, consulte a documentação do [StoreFront](#).

Em um ambiente misto, continue usando as versões Studio e Director para cada versão, mas certifique-se de que versões diferentes estejam instaladas em máquinas separadas.

### **Sistemas operacionais anteriores**

Digamos que você tenha instalado uma versão anterior de um componente em uma máquina que estava executando uma versão compatível do sistema operacional (SO). Agora, você deseja usar uma versão mais recente do componente, mas esse sistema operacional não é mais compatível com a versão atual do componente.

Por exemplo, suponha que você tenha instalado um servidor VDA em uma máquina Windows Server 2008 R2. Agora você quer atualizar esse VDA para a versão atual, mas o Windows Server 2008 R2 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. (Isso não afeta a aplicação de CUs a uma versão LTSR.)

Siga os links para saber quais sistemas operacionais são compatíveis:

- Citrix Virtual Apps and Desktops (versão atual):
  - [Controlador de entrega, estúdio, diretor, VDAs, servidor de impressão universal](#)
  - [Serviço de autenticação federada](#)
  - 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 UC. (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. Indica a última versão válida do componente suportada por cada sistema operacional 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	Component/feature	Última versão válida	A instalação/atualização não foi possível
Windows 7 LTSR	Componentes do Windows 7	Windows 7 LTSR	Componentes do Windows 7
Windows 8	Componentes do Windows 8	Windows 8	Componentes do Windows 8
Windows 10	Componentes do Windows 10	Windows 10	Componentes do Windows 10
Windows Server 2008 R2	Componentes do Windows Server 2008 R2	Windows Server 2008 R2	Componentes do Windows Server 2008 R2
Windows Server 2012	Componentes do Windows Server 2012	Windows Server 2012	Componentes do Windows Server 2012
Windows Server 2016	Componentes do Windows Server 2016	Windows Server 2016	Componentes do Windows Server 2016

O Windows XP e o Windows Vista não são válidos para nenhum componente ou tecnologia 7.x.

\ \* Aplica-se ao Delivery Controller, Studio, Director e VDAs.

### O que você pode fazer

Você tem escolhas. Você pode:

- Continue com o sistema operacional atual
- Recrie a imagem ou atualize a máquina
- Adicione novas máquinas e, em seguida, remova as máquinas antigas

**Continue com o sistema operacional atual** Esses métodos são viáveis para VDAs. Se quiser continuar usando máquinas com o sistema operacional anterior, você pode escolher uma das seguintes opções:

- Continue usando a versão do componente instalado.

- Faça o download da versão válida mais recente do componente e atualize o componente para essa versão. (Isso pressupõe que a versão mais recente do componente válido ainda não esteja instalada.)

Por exemplo, você tem um VDA 7.14 em uma máquina Windows 7 SP1. A última versão válida do VDA em máquinas com sistema operacional Windows 7 é o XenApp e o XenDesktop 7.15 LTSR. Você pode continuar usando o 7.14 ou baixar um VDA 7.15 LTSR e depois atualizar seu VDA para essa versão. Essas versões anteriores do VDA funcionam em implantações contendo Delivery Controllers com versões mais recentes. Por exemplo, um VDA de 7,15 LTSR pode se conectar a um controlador Citrix Virtual Apps and Desktops 7 1808.

**Recrie a imagem ou atualize a máquina** Esses métodos são viáveis para VDAs e outras máquinas que não têm componentes principais (como Delivery Controllers) instalados. Escolha uma das seguintes opções:

- Depois de tirar a máquina de serviço (ativando o modo de manutenção e permitindo que todas as sessões sejam fechadas), você pode recriá-la para uma versão compatível do sistema operacional Windows e, em seguida, instalar a versão mais recente do componente.
- Para atualizar o sistema operacional sem refazer a imagem, desinstale o software Citrix antes de atualizar o sistema operacional (isso inclui atualizações internas para seu sistema operacional). Por exemplo, do Windows 10 versão 1903 ao Windows 10 versão 1909). Caso contrário, o software Citrix não será suportado. Em seguida, instale o novo componente.
- Para atualizar o sistema operacional em uma máquina VDA sem refazer a imagem, você deve primeiro instalar a versão do VDA compatível com o sistema operacional para o qual você está atualizando ou atualizar o VDA após atualizar o sistema operacional. Caso contrário, o software Citrix não será suportado. Você pode atualizar para as seguintes versões mínimas do sistema operacional ao realizar uma atualização no local sem desinstalar o VDA:
  - Windows 11 com atualização cumulativa [2023-07 para Windows 11 \(KB5028185\)](#) ou posterior instalada (compilação 22621.1992 ou posterior).
  - Windows 10 com [2023-07 Atualização dinâmica para Windows 10 \(KB5028311\)](#) instalada.
- Se a versão do Windows para a qual você planeja atualizar não estiver alinhada com a diretriz mencionada acima, desinstale o VDA antes de atualizar o sistema operacional e, em seguida, instale uma versão compatível do VDA após a conclusão da atualização do sistema operacional.

**Adicione novas máquinas e, em seguida, remova as máquinas antigas** Esse método é viável se você precisar atualizar o sistema operacional em máquinas contendo um Delivery Controller ou outro componente principal.

A Citrix recomenda que todos os controladores em um site tenham o mesmo sistema operacional. A sequência de atualização a seguir minimiza o intervalo em que controladores diferentes têm sistemas

operacionais diferentes.

1. Faça um instantâneo 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. Por exemplo, instale um controlador em duas máquinas Windows Server 2016.
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. Por exemplo, remova dois Controllers em duas máquinas Windows Server 2008 R2. Siga as recomendações para remover os Controladores em [Delivery Controllers](#).

## Preparação

Antes de iniciar um upgrade, revise as informações a seguir e conclua as tarefas necessárias.

### Nota:

Embora a atualização de VDAs ocorra posteriormente na sequência de atualização, é uma boa ideia escolher um instalador e revisar o procedimento antes de iniciar a atualização, para saber o que esperar.

## Escolha um instalador e uma interface

Use o instalador completo do produto a partir da ISO do produto para atualizar os componentes. Você pode atualizar os VDAs usando o instalador completo do produto ou um dos instaladores autônomos do VDA. Todos os instaladores oferecem interfaces gráficas e de linha de comando.

Para obter mais informações, consulte [Installers](#).

**Especificações da instalação:** Depois de concluir qualquer trabalho de preparação e estar 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).

- [Instale/atualize os componentes principais usando a interface gráfica](#)
- [Instale/atualize os componentes principais usando a linha de comando](#)
- [Instale/atualize VDAs usando a interface gráfica](#)
- [Instale/atualize 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 de VDA completo do produto ou o instalador `VDAWorkstationSetup.exe` para atualizar o VDA, os componentes que foram originalmente excluídos poderão ser instalados, a menos que você os omita ou exclua expressamente da atualização.



Ao atualizar um VDA para a versão atual, ocorre uma reinicialização da máquina durante o processo de atualização. (Esse 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 registro do site, do monitoramento e da configuração. Siga as instruções em [CTX135207](#). Se algum problema for descoberto após a atualização, você poderá restaurar o backup.

Para obter informações sobre a atualização de versões do SQL Server que não são mais suportadas, consulte [Verificação de versão do SQL Server](#). (Isso se refere ao SQL Server que é usado para os bancos de dados de registro do site, do monitor e da 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 deverá 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 o SQL Server Express LocalDB](#).

### **Certifique-se de que seu licenciamento Citrix esteja atualizado**

Para uma visão abrangente do gerenciamento do Citrix Licensing, consulte [Ativar, atualizar e gerenciar as licenças Citrix](#).

Você pode usar o instalador completo do produto para atualizar o Servidor de Licenças. Ou você pode baixar e atualizar os componentes da licença separadamente. Veja [Upgrade](#).

Antes de fazer o upgrade, certifique-se de que a data do Customer Success Services /Software Maintenance/Subscription Advantage seja válida para a nova versão do produto. A data deve ser pelo menos 2021.11.15.

### **Certifique-se de que seu Citrix License Server seja compatível**

Certifique-se de que seu Citrix License Server seja compatível com a nova versão. Há duas maneiras de fazer isso:

- Antes de atualizar qualquer outro componente Citrix, execute o instalador [XenDesktopServerSetup.exe](#) a partir do layout ISO na máquina que contém um Delivery Controller. Se houver algum problema de incompatibilidade, o instalador o reporta 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`. O display indica se o Servidor de Licenças é compatível. Se o Servidor de Licenças for incompatível, atualize o servidor de licenças.

### **Faça backup de todas as modificações do StoreFront**

Antes de iniciar uma atualização, se você tiver feito modificações nos arquivos em `C:\inetpub\wwwroot\Citrix\&#060; StoreName&#062;\ 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.

### **Feche aplicativos e consoles**

Antes de iniciar uma atualização, feche todos os programas que possam causar bloqueios de arquivos, incluindo consoles de administração e sessões do PowerShell.

Reiniciar a máquina garante que todos os bloqueios de arquivos sejam eliminados e que não haja atualizações pendentes do Windows.

Antes de iniciar uma atualização, interrompa e desative qualquer serviço de agente de monitoramento de terceiros.

### **Verifique se você tem as permissões adequadas**

Além de ser usuário do domínio, você deve ser administrador local nas máquinas em que está atualizando os componentes do produto.

O banco de dados do site e o site podem ser atualizados automática 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 [Databases](#).

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 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 de modelos e atualize hipervisores, se necessário
- Conclua todas as outras tarefas de preparação ditadas pelo seu plano de continuidade de negócios.

## Testes preliminares no local

Quando você atualiza os Delivery Controllers e um site, os 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 registro de configuração pode ser acessado
- Certifique-se de ter uma Licença de Direitos Híbridos se quiser adicionar conexões de host em nuvem pública (por exemplo, AWS). Caso contrário, o teste preliminar do site será pausado ou interrompido e uma mensagem explicativa será exibida.

Depois que os testes forem executados, você poderá ver um relatório dos resultados. Em seguida, você pode corrigir os 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 site.

O relatório contendo os resultados do teste é um arquivo HTML ([PreliminarySiteTestResult.html](#)) no mesmo diretório dos registros de instalação. Esse arquivo é criado se não existir. Se o arquivo existir, seu conteúdo será sobrescrito.

### Execute os testes

- Quando você usa a interface gráfica do instalador para atualizar, o assistente inclui uma página na qual você pode iniciar os testes e depois exibir o relatório. Depois que os testes forem executados e você tiver visualizado o relatório e resolvido os problemas encontrados, você poderá executar novamente os testes. Quando os testes forem concluídos com êxito, clique em Avançar para continuar com o assistente.
- Quando você usa a interface de linha de comando para atualizar, os testes são executados automaticamente. Por padrão, se um teste falhar, a atualização não será executada. Depois de visualizar o relatório e resolver problemas, execute o comando novamente.

A Citrix recomenda sempre executar os testes preliminares do local e, em seguida, resolver quaisquer problemas antes de continuar com o controlador e a atualização do site. O benefício potencial vale a pena dedicar alguns minutos para realizar os testes. No entanto, você pode ignorar essa ação recomendada.

- Ao atualizar com a interface gráfica, você pode optar por pular os testes e continuar com a atualização.
- Ao atualizar a partir da linha de comando, você não pode pular os testes. Por padrão, uma falha no teste do site faz com que o instalador falhe, sem realizar a atualização. Na maioria dos

casos, se você incluir a opção `/ignore_site_test_failure`, qualquer falha no teste será ignorada e a atualização continuará. (Consulte Verificação da versão do SQL Server para ver as exceções.)

### **Ao atualizar vários controladores**

Quando você inicia uma atualização em um Controller e, em seguida, inicia um upgrade de outro Controller no mesmo site (antes da conclusão da primeira atualização):

- Se os testes preliminares do site tiverem sido concluídos no primeiro Controlador, a página de testes preliminares do site não aparecerá no assistente do outro Controlador.
- 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 do outro Controller. No entanto, se os testes no primeiro Controlador terminarem, somente os resultados do primeiro Controlador serão retidos.

### **Falhas de teste não relacionadas à integridade do site**

- Se os testes preliminares do local falharem devido à memória insuficiente, disponibilize mais memória e execute novamente os testes.
- Se você tiver permissão para atualizar, mas não executar testes do site, os testes preliminares do site falharão. Para resolver isso, execute novamente o instalador 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 registro de sites, monitores e configurações. Atualizar uma implantação Citrix com uma versão do SQL Server que não é mais suportada pode resultar em problemas de funcionalidade, e o site não terá suporte.

Para saber quais versões do SQL Server são compatíveis com a versão Citrix para a qual você está atualizando, consulte o artigo [System requirements](#) dessa versão.

Ao atualizar um controlador, o instalador Citrix verifica a versão atualmente instalada do SQL Server usada para os bancos de dados de registro do site, do monitor e da configuração.

- Se a verificação determinar que a versão atualmente instalada do SQL Server não é uma versão suportada na versão Citrix para a qual você está atualizando:

- Interface gráfica: a atualização é interrompida com uma mensagem. Clique em **Eu entendo** e, em seguida, clique em **Cancelar** para fechar o instalador Citrix. (Você não pode continuar com a atualização.)
- Interface de linha de comando: o comando falha (mesmo se você incluiu 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 puder determinar qual versão do SQL Server está instalada atualmente, veja se 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 atualmente instalada do SQL Server for suportada, clique em **Eu entendo** para fechar a mensagem e, em seguida, clique em **Avançar** para continuar com a atualização do Citrix.
    - \* Se a versão atualmente instalada do SQL Server não for suportada, clique em **Eu entendo** para fechar a mensagem e, em seguida, clique em **Cancelar** para finalizar a atualização do Citrix. Atualize seu SQL Server para uma versão compatível e, em seguida, inicie a atualização do Citrix novamente.
  - Interface de linha de comando: o comando falha com uma mensagem. Depois de fechar a mensagem:
    - \* Se a versão atualmente instalada do SQL Server for suportada, execute o comando novamente com a opção `/ignore_db_check_failure`.
    - \* Se a versão atualmente instalada do SQL Server não for suportada, atualize seu SQL Server para uma versão compatível. Execute o comando novamente para iniciar a atualização do Citrix.

### Atualizando o SQL Server

Se você abrir novos servidores do SQL Server e migrar o banco de dados do site, as cadeias de conexão deverão ser atualizadas.

Se o site atualmente usa o SQL Server Express para o banco de dados do site (que a 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 cadeias de conexão.

Para obter mais informações, consulte [Configurando cadeias de conexão](#) e a documentação do produto Microsoft SQL Server.

## Substitua o SQL Server Express LocalDB

O Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o Local Host Cache usa de forma independente. O cache de host local não exige nenhum componente do SQL Server Express além do SQL Server Express LocalDB.

Se você instalou uma versão do Delivery Controller anterior à 1912 e depois atualizou sua implantação para a versão 1912 ou posterior, a Citrix não atualiza automaticamente a versão do SQL Server Express LocalDB. Por que não? Porque você pode ter componentes não Citrix que dependem do SQL Server Express LocalDB. Se você tiver componentes que não sejam da Citrix que estejam usando o SQL Server Express LocalDB, certifique-se de que a atualização do SQL Server Express LocalDB não interrompa esses componentes. Para atualizar (substituir) a versão do SQL Server Express LocalDB, siga as orientações nesta seção.

- **Ao atualizar os Delivery Controllers para as versões 2402 LTSR ou posteriores do Citrix Virtual Apps and Desktops:** A versão suportada é o SQL Server Express LocalDB 2022.

### Nota:

As versões 2017, 2019 e 2022 do SQL Server Express LocalDB são todas compatíveis entre si. Portanto, não é obrigatório atualizar o SQL Server Express LocalDB para que o LHC funcione.

O que você precisa:

- A mídia de instalação do Citrix Virtual Apps and Desktops contendo uma cópia do Microsoft SQL Server Express LocalDB 2022.
- A ferramenta [PsExec](#) da caixa de ferramentas Windows Sysinternals que você pode baixar da Microsoft. Consulte o documento da Microsoft [PsExec v2.43](#).

Procedimento:

1. Conclua a atualização de seus componentes, bancos de dados e site do Citrix Virtual Apps and Desktops. (Essas atualizações do banco de dados afetam os bancos de dados do site, do monitoramento e do registro de configurações. Eles não afetam o banco de dados do Local Host Cache que usa o SQL Server Express LocalDB.)
2. Faça login no Delivery Controller que está sendo usado para recriar o banco de dados do LHC.
3. Nesse Delivery Controller, baixe [PsExec](#) da Microsoft e coloque-o em `C:\Temp`.
4. Pare o Citrix High Availability Service.

- Abra o prompt de comando, navegue até `C:\Temp`, em seguida, execute o seguinte comando para elevar a conta do prompt de comando com serviço de rede:

```
1 psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
```

- Execute `whoami` para confirmar se o prompt de comando está sendo executado como a conta do Serviço de Rede. Você deve obter a seguinte saída: `nt authority\networkservice`.
- Use o prompt de comando para navegar até a instância SQL LocalDB:

- Se estiver atualizando do SQL LocalDB 2014:

```
1 cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

- Se estiver atualizando do SQL LocalDB 2017:

```
1 cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

- Se estiver atualizando do SQL LocalDB 2019:

```
1 cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

- Pare e exclua a instância SQL LocalDB: `CitrixHA`.

```
1 SqlLocalDB stop CitrixHA
2
3 SqlLocalDB delete CitrixHA
```

- Remova os arquivos relacionados em `C:\Windows\ServiceProfiles\NetworkService`.

```
1 HADatabaseName.*
2 HADatabaseName_log.*
3 HAImportDatabaseName.* (if exists)
4 HAImportDatabaseName_log.* (if exists)
```

- Desinstale seu SQL LocalDB SQL Server Express existente do servidor usando o recurso do Windows para remover programas.
- Instale o SQL Server Express LocalDB 2022. Na pasta **Support > SQLLocalDB** na mídia de instalação do Citrix Virtual Apps and Desktops, clique duas vezes em `sqllocaldb.msi`. Uma reinicialização pode ser solicitada para concluir a instalação. O novo SQL LocalDB reside em `C:\Program Files\Microsoft SQL Server\160\Tools\Binn`.
- Inicie o Citrix High Availability Service no Delivery Controller onde você desinstalou a versão antiga do SQL LocalDB.
- No prompt de comando, execute `SqlLocalDB i` para confirmar se `CitrixHA` foi criado novamente ou não.

14. Repita as etapas nos controladores de entrega restantes.
15. Certifique-se de que o banco de dados do Local Host Cache seja criado em cada Delivery Controller. Isso confirma que o Serviço de Alta Disponibilidade (corretor secundário) pode assumir o controle, se necessário.
  - a) No servidor do controlador, navegue até `C:\Windows\ServiceProfiles\NetworkService`.
  - b) Verifique se `HadatabaseName.mdf` e `HadatabaseName_log.ldf` foram criados.

## Secure HDX (versão prévia)

November 5, 2024

O Secure HDX é uma solução de criptografia em nível de aplicativo (ALE) que impede que qualquer elemento de rede no caminho de tráfego possa inspecionar o tráfego HDX. Ele faz isso fornecendo uma verdadeira criptografia de ponta a ponta (E2EE) no nível do aplicativo entre o aplicativo Citrix Workspace (cliente) e o VDA (host da sessão) usando a criptografia AES-256-GCM.

### Importante:

O Secure HDX está atualmente em versão prévia. Esse recurso é fornecido sem suporte e ainda não é recomendado para uso em ambientes de produção. Para enviar feedback ou relatar problemas, use [neste formulário](#).

## Requisitos do sistema

A lista a seguir mostra os requisitos do sistema para usar o Secure HDX.

- Plano de controle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 ou posterior
- Host da 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
- Nível de acesso
  - Espaço de trabalho Citrix
  - Citrix StoreFront 2402 ou posterior

## Configuração

O Secure HDX está desativado por padrão. Você pode configurar esse recurso usando a configuração Secure HDX na política da Citrix:

**Secure HDX:** Define se o recurso deve ser ativado para todas as sessões, somente para conexões diretas, ou desabilitá-lo.

## Considerações

A seguir estão as considerações sobre o uso do 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.
- Atualmente, a continuidade do serviço não é compatível com o Secure HDX. Se você tiver o Service Continuity ativado em seu ambiente Citrix Cloud, não poderá acessar nenhum host de sessão que tenha o Secure HDX ativado se houver uma interrupção do serviço em nuvem.
- 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, poderá configurar o Secure HDX para ser ativado somente para conexões diretas.
- Se você usa o SmartControl, observe que o uso do Secure HDX impede que o SmartControl funcione, pois o NetScaler não consegue inspecionar o tráfego HDX criptografado. Se você precisar usar o SmartControl, poderá configurar o Secure HDX para ser ativado somente para conexões diretas.
- O Multi-Stream ICA não é suportado quando o Secure HDX está ativado.

- Se você usar soluções de terceiros que dependam da inspeção do tráfego HDX, elas não funcionarão mais se você habilitar o Secure HDX, pois o tráfego HDX é criptografado.
- Se você tiver o Secure ICA ativado nos grupos de entrega nos quais deseja ativar o Secure HDX, primeiro desative o Secure ICA (Editar configurações do usuário do grupo de entrega >).

## Solução de problemas

Para confirmar se 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 na sessão e execute `ctxsession.exe -v`. Se o Secure HDX estiver em uso, a criptografia ICA exibirá `SecureHDX AES-256 GCM`.

```
PS C:\Users\ > ctxsession -v
Session Id 1:
Transport Protocols:  UDP -> DTLS -> CGP -> ICA
  Local Address:      :55000
  Remote Address:     :65469
  Client Address:     :53637
Security Protocol:    DTLS 1.2
Security Cipher:      256 bit AES
Cipher Strength:      256 bits
ICA Encryption:       SecureHDX AES-256 GCM
Rendezvous Version:  None
HDX Direct State:    Connected - External
Reducer Version:     4.0

EDT Reliable Statistics:
  Bandwidth 94.516 Mbps, RTT 34.538 ms, EDT MTU: 1480

EDT Unreliable Statistics:
  Bandwidth 7.544 Kbps, RTT 1 us, EDT MTU: 1480

EDT Reliable Basic FEC Statistics:
  Bandwidth 92.090 Mbps, RTT 7.980 ms, EDT MTU: 1480

ICA Statistics:
  SentBandwidth (bps) = 4968
  HDX Latency = 31
  IcaBufferLength = 1436
```

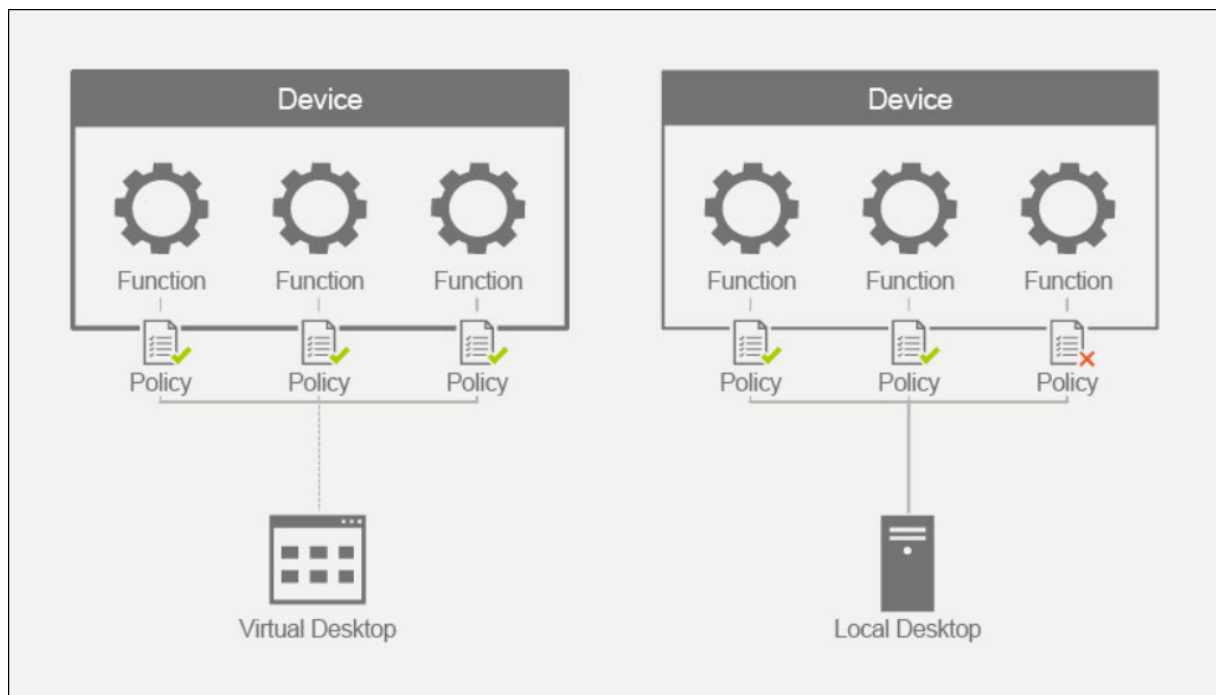
## Quando o Secure HDX não é ativado na sessão

- Certifique-se de que a versão do VDA em uso ofereça suporte ao recurso de acordo com os requisitos do sistema.
- Confirme se você tem uma política aplicada ao VDA que habilita o Secure HDX e se não há outras políticas com maior prioridade desativando o recurso.
- Se o dispositivo cliente estiver se conectando por meio do NetScaler Gateway ou do Gateway Service, certifique-se de que o Secure HDX não esteja definido 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.

## Dispositivos compostos e divisão de dispositivos

November 5, 2024

Um dispositivo USB composto é um único dispositivo que funciona como vários dispositivos USB independentes conectados a um computador. Ele tem um único conector USB, mas pode expor várias 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 será considerada definitiva para o dispositivo composto e o dispositivo será negado. Se a primeira correspondência de uma função (interface) for uma regra de Permissão, o dispositivo host continuará comparando as regras com a 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 somente para a área de trabalho local, caso contrário, o dispositivo será remoto para a área de trabalho virtual. Se nenhuma correspondência for encontrada, serão usadas as regras padrão.



Podemos dividir o dispositivo composto usando as regras apropriadas na política de regras de redirecionamento de dispositivos (versão 2) para permitir somente a funcionalidade específica de um dispositivo composto. Por exemplo, podemos querer usar apenas as funções HID de uma chave FIDO2, mas não a funcionalidade do cartão inteligente. Nesse caso, definiríamos as regras conforme ilustrado abaixo:

1. Conexão: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey série 5 permitiu funções

FIDO2 HID.

2. Negar: VID=1050 PID=0407 split=01 intf=02 # Função do cartão inteligente Yubikey série 5 bloqueada.

**Dica:**

Ao criar novas regras de política, consulte os [USB Class Codes](#), disponíveis no site da USB.

## Configurando um teclado de assinatura

1. Instale o driver de dispositivo apropriado no host do VDA.
2. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.
3. Edite a configuração de política **Client USB Device Redirection rules (Version 2)**.
  - a) Defina as informações **VID** e **PID** para o bloco de assinatura que precisa ser redirecionado 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 dispositivos USB do cliente**.
  - a) Defina o modo junto com outras informações do dispositivo. Por exemplo: dispositivo Mode=00000004 VID=06A8 PID=0057 class=03 #Input 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 os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
7. Edite 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 os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, os lançamentos de sessão subsequentes farão com que o dispositivo seja 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 o redirecionamento USB

1. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.

2. Os teclados Bloomberg 5 são definidos por padrão na configuração da política **Client USB Redirection Rules (Versão 2)** e nenhuma ação administrativa adicional é necessária.
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 os 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 os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, as chaves da Bloomberg serão apresentadas automaticamente nas sessões HDX subsequentes e não exigirão nenhuma ação adicional do usuário final.

## Configurando uma chave FIDO2 usando o redirecionamento USB

A Citrix recomenda usar o redirecionamento FIDO2 para usar as chaves FIDO2 em suas sessões HDX. No entanto, pode haver situações em que você precise redirecionar as chaves FIDO2 usando o redirecionamento USB. Isso inclui cenários em que o redirecionamento FIDO2 não está disponível porque o recurso não é suportado pelo cliente, pelo VDA ou pelo sistema operacional (por exemplo, Windows Server 2016).

Também pode haver situações em que a tecla tenha vários modos ativados, mas você só deseja permitir um subconjunto deles em suas sessões HDX. Por exemplo, talvez você queira permitir FIDO2 e OTP, mas bloquear o cartão inteligente.

As etapas a seguir ilustram como você pode configurar uma chave FIDO2 usando o redirecionamento USB (Yubikey vid=1050, pid=0407).

1. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.
2. Edite a configuração de política das regras de redirecionamento de dispositivos USB do cliente **(Versão 2)**.
  - a) Defina as informações **VID** e **PID**, bem como a configuração do dispositivo dividido para que a chave FIDO2 seja redirecionada na sessão e clique em **Salvar**.
  - b) **Connect:** VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey série 5 permitia funções FIDO2 HID.
  - c) **Deny:** VID=1050 PID=0407 split=01 intf=02 # Função do cartão inteligente Yubikey série 5 bloqueada.

1

Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.

1

Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

1

Edite a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.

1

Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, os teclados FIDO2 serão apresentados automaticamente nas sessões HDX subsequentes e não exigirão nenhuma ação adicional do usuário final.

## Configurando um mouse 3D usando o redirecionamento USB

Atualmente, os drivers de mouse espacial 3DConnexion são suportados apenas em sistemas operacionais de estações de trabalho (Win 10 e Win11). Eles não funcionam no sistema operacional do 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 [mais recente do Windows](#) no host VDA.
2. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.
3. Edite a configuração de política das regras de redirecionamento de dispositivos USB do cliente **(Versão 2)**.
  - a) Defina as informações **VID** e **PID** para o bloco de assinatura que precisa ser redirecionado e clique em **Salvar**. Por exemplo: **Connect: VID=046D PID=C016 #SpaceMouse Enterprise**

1

Edite a configuração de política **Regras de otimização de dispositivos USB do cliente**.

- ```
1 1. Defina o modo junto com outras informações do dispositivo. Por exemplo: dispositivo Mode=00000004 VID=046D PID=C016 class=03 #Input operando no modo de captura
```

1

Edite a configuração de política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.

1

Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

1

Edite a configuração de política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.

1

Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

### **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 e, ao mesmo tempo, oferecer ao usuário final a opção de redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.
2. Edite a configuração de política **Client USB Device Redirection rules (Version 2)**.
  - a) Adicione as informações **VID** e **PID** dos dois dispositivos a serem redirecionados com a regra de dispositivo apropriada na sessão e clique em **Salvar**.
  - b) **Permitir microfone de fala**: VID=0911 PID=0c1c #Phillips.
  - c) **Connect**: VID=06A8 PID=0043 class=03 # Bloco de assinatura USB Topaz
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 os 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 os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Depois que essas configurações forem definidas, o teclado de assinatura Topaz HSB será apresentado automaticamente nas 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 ative o redirecionamento no Connection Center ou na guia Dispositivos do CDViewer.

## Configuração de redirecionamento USB herdada

November 5, 2024

Se você estiver usando algum componente anterior 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 **Policies**.
2. Clique em **Criar política** e expanda as políticas de dispositivos USB **ICA >**.
3. Edite a política de redirecionamento de dispositivos 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 comparado a cada regra de política USB sucessivamente até que uma correspondência seja encontrada. A primeira partida para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de permissão, o dispositivo correspondente poderá ser redirecionado para a área de trabalho virtual. Se a primeira correspondência for uma regra de negação, o dispositivo correspondente estará disponível somente no desktop local. Se nenhuma correspondência for encontrada, serão usadas as regras padrão.

#### Definindo a política no DDC:

1. Abra as políticas **do Citrix Web Studio** e clique na guia **Policies**.
2. Clique em **Criar política** e expanda as políticas de dispositivos USB **ICA >**.
3. Edite as regras de redirecionamento de dispositivos USB do cliente **\*\***.



4. Defina o valor com base nos exemplos fornecidos na descrição de cada dispositivo USB que precisa ser redirecionado e clique em Salvar. Por exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Classe=08 subclasse=05 # Armazenamento em massa

**Observação:**

Se um administrador da Citrix marcar Usar valor padrão e clicar em Salvar, as regras padrão podem ser encontradas no seguinte registro no VDA.

**Cuidado!:**

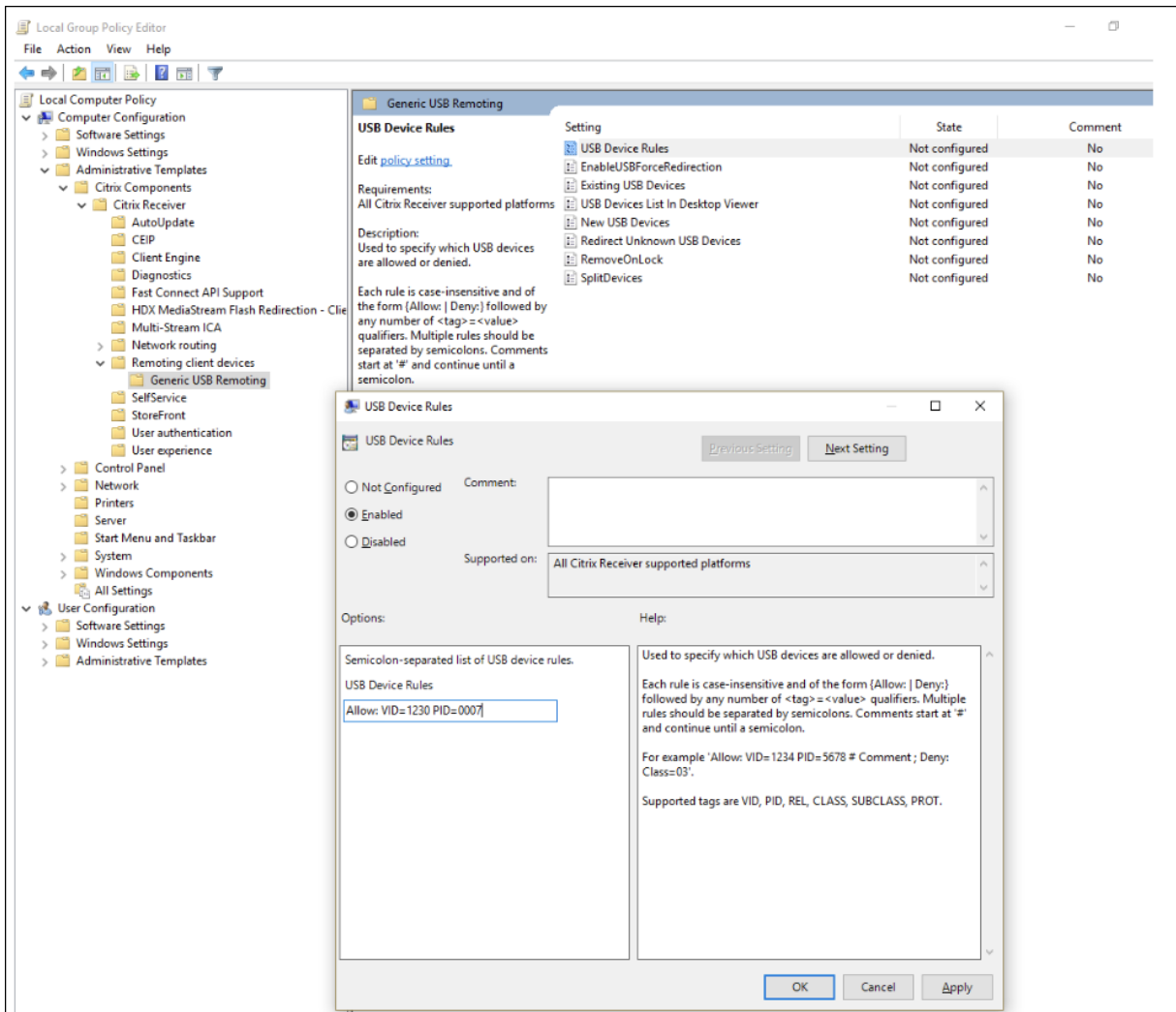
Consulte a isenção de responsabilidade no final deste artigo antes de usar o Editor do Registro. `HKLM\ SOFTWARE\ Wow6432Node\ Citrix\ Portica\ GenericUSB\ DeviceRules`

**Usando GPOs no cliente:**

1. Abra o **Local Group Policy Editor** e acesse **Administrative Templates > Citrix Components > Citrix Receiver > Dispositivos clientes remotos > Generic USB Remoting**.
2. Abra a configuração **USB Device Rules** e ative a configuração. Adicione a regra Dispositivo USB como neste exemplo, A regra Permitir: VID=1230 PID=0007 permite o dispositivo com ID do fornecedor 1230 e ID do produto 0007.

**Observação:**

Use a regra Permitir: vid=XXXX PID=xxxx quando um dispositivo específico precisar estar no topo da lista de regras do dispositivo.



**Observação:**

Uma ferramenta como USBView ou até mesmo a barra de ferramentas de conexão pode ser usada para determinar os detalhes do dispositivo, como VID e PID (inclua SS aqui).

**Configurar o redirecionamento automático de dispositivos USB**

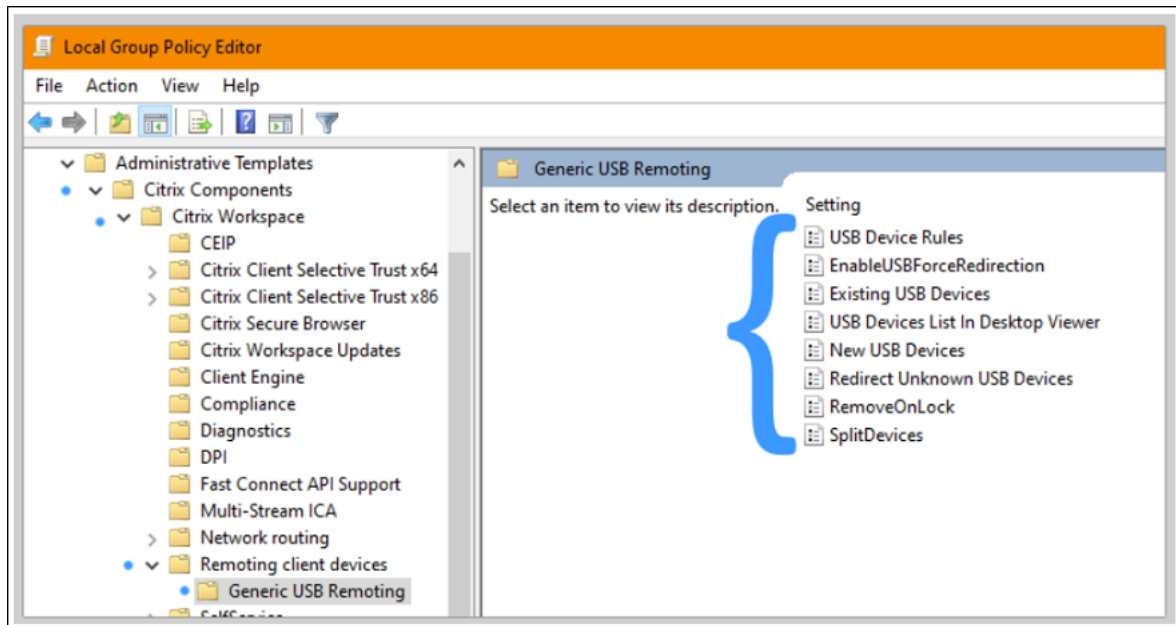
Os dispositivos USB são redirecionados automaticamente quando o suporte a USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar dispositivos USB automaticamente. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que dispositivos USB sejam listados ou redirecionados, use a configuração de política DeviceRules no ponto de extremidade do cliente.

Esta política pode ser definida no cliente usando um GPO, um registro do lado do cliente, usando as Preferências do Citrix Workspace ou a guia Conexões no CDViewer. Todos esses métodos estão

descritos abaixo:

### Usando GPOs no cliente:

1. Abra o **Local Group Policy Editor** e acesse **Administrative Templates > Citrix Components > Citrix Receiver > Dispositivos clientes remotos > Generic USB Remoting**.
2. Abra **New USB Devices**, selecione **Enabled** e clique em **OK**.
3. Abra **Existing USB Devices**, selecione **Enabled** e clique em **OK**.



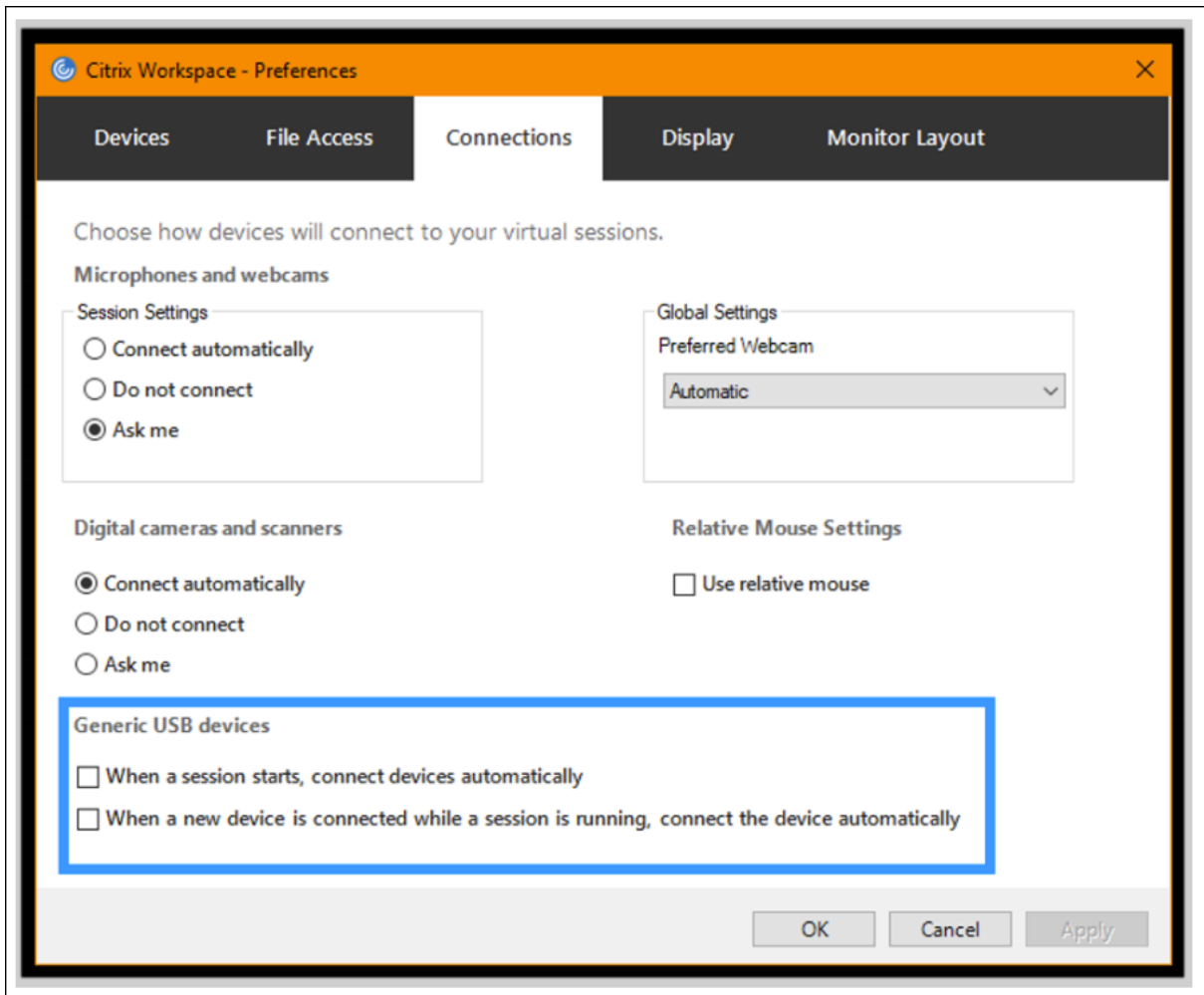
### Usando o Citrix Connection Center:

1. Vá para **Preferências do Citrix Workspace > Conexões**.
2. As seguintes opções devem ser selecionadas:
  - a) When a session starts, connect devices automatically
  - b) When a new device is connected while a session is running, connect the device automatically.
3. Clique em **OK**.

### Usando a barra de ferramentas CDViewer Connection:

1. Após o início de uma sessão, clique no menu suspenso **CDViewer** e selecione a guia **Citrix Workspace Preferences > Connections**.
2. As seguintes opções devem ser selecionadas:
  - a) When a session starts, connect devices automatically
  - b) When a new device is connected while a session is running, connect the device automatically.

3. Clique em **Aplicar** e **OK** para salvar a política.



Para as configurações baseadas no cliente, as chaves do registro são definidas para o dispositivo cliente no seguinte local:

**Cuidado!:**

Consulte a isenção de responsabilidade 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 e, ao mesmo tempo, oferecer ao usuário final a opção de redirecionar o outro dispositivo. A seguir estão as etapas para configurar dois dispositivos com regras diferentes.

1. Ative a configuração de política **Client USB Device Redirection** no **Citrix Web Studio**.
2. Edite a configuração **das regras** do dispositivo USB no GPO do lado do cliente.
  - a) Abra o **Local Group Policy Editor** e acesse **Administrative Templates > Citrix Components > Citrix Receiver > Dispositivos clientes remotos > Generic USB Remoting**.
  - b) Abra a configuração **USB Device Rules** e ative 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 **Connect: VID=06A8 PID=0043** redirecionará automaticamente o dispositivo com **ID do fornecedor 06A8** e **ID do produto 0043**, desde que as políticas de redirecionamento automático mencionadas na etapa 3 estejam definidas.
    - c) **Permitir microfone de fala:** VID=0911 PID=0c1c #Phillips.
    - d) **Connect:** VID=06A8 PID=0043 class=03 # Bloco de assinatura USB Topaz
3. Abra o **Local Group Policy Editor** e acesse **Administrative Templates > Citrix Components > Citrix Receiver > Dispositivos clientes remotos > Generic USB Remoting**.
4. Abra **New USB Devices**, selecione **Enabled** e clique em **OK**.
5. Abra **Existing USB Devices**, selecione **Enabled** e clique em **OK**.

Depois que essas configurações forem definidas, o teclado de assinatura Topaz será redirecionado automaticamente para dentro da sessão HDX e uma ação adicional do usuário final será necessária (selecione a opção Redirecionar no Centro de Conexões ou na guia Dispositivos de Visualização de CD) para redirecionar o microfone de fala Phillips na sessão.

#### **Observação:**

As configurações acima nas etapas 2 e 3 podem ser aplicadas diretamente no valor de registro do lado do cliente **DeviceRules** sob a chave GenericUSB (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB), mas essa não é a forma recomendada.

## **Otimização para Microsoft Teams (novo)**

August 22, 2024

A Microsoft lançou uma nova versão do Microsoft Teams (Teams 2.x) para ambientes VDI. A Citrix agora oferece suporte à otimização para essa nova versão do Teams. Esta documentação se concentra principalmente na Otimização do Citrix HDX com o novo Teams e oferece informações essenciais para a transição para a Otimização do Microsoft SlimCore.

## Terminologia e transição

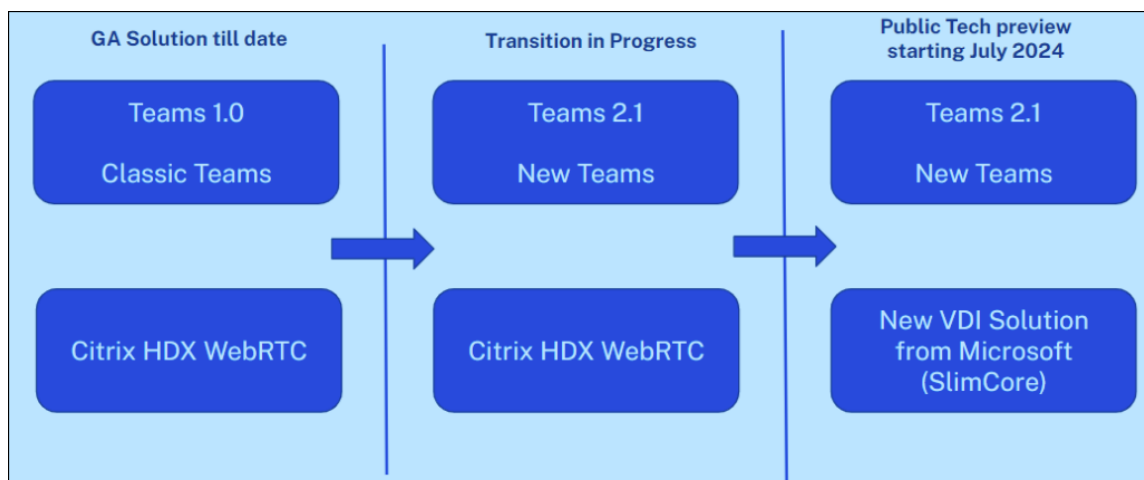
### Transição para o Microsoft Teams

Atualmente, existem duas transições no espaço do Microsoft Teams:

- **Transição do Teams Clássico para o Novo Teams:** essa transição é para clientes nativos e de VDI
  - O Teams Clássico chegará ao fim do suporte e ao fim da vida útil. Para obter informações sobre o cronograma dessa transição, consulte [Fim da disponibilidade do cliente Teams clássico](#).
  - A documentação completa para a implantação do Novo Teams está disponível em [Novo Teams para VDI](#).
- **Transição da Otimização do Citrix HDX para a Otimização do Microsoft SlimCore:** essa transição é específica para ambientes VDI.
  - Apresentamos os termos **VDI 1.0** e **VDI 2.0** para diferenciarmos entre a otimização existente com o Citrix HDX e a nova solução VDI da Microsoft.
  - Coloquialmente, VDI 1.0 se refere à Otimização do Citrix HDX e VDI 2.0 se refere à nova solução VDI para Teams (Otimização do Microsoft SlimCore).

### Cronogramas

- Para obter mais informações sobre o cronograma de fim da vida útil do Teams Clássico, consulte [Fim da disponibilidade do cliente Teams clássico](#).
- Para participar da prévia pública da otimização do SlimCore, os administradores devem mover os usuários para o canal público de prévia, conforme descrito [neste artigo](#)



## Principais distinções

---

### Otimização do Citrix HDX

A otimização é uma solução combinada da Citrix e da Microsoft e usa um canal virtual criado pela Citrix.

O descarregamento de mídia é feito pelo [HdxRtcEngine](#) que reside no aplicativo Citrix Workspace.

Nenhum componente adicional é necessário no endpoint, exceto a instalação do aplicativo Citrix Workspace.

Disponível em plataformas de endpoint: Windows, macOS, Linux e ChromeOS.

Os novos recursos são gerenciados em conjunto entre a Citrix e a Microsoft.

### Otimização do Microsoft SlimCore

A solução de otimização é de propriedade e gerenciada pela Microsoft e usa canais virtuais criados pela Microsoft.

O descarregamento de mídia é feito pelo mecanismo de mídia Microsoft SlimCore.

Componente adicional: o **plug-in Teams VDI** precisa ser implantado no endpoint por vários meios. Esse plug-in gerencia o download e as atualizações do mecanismo SlimCore.

Disponível em plataformas de endpoint: Windows até a data.

Os novos recursos são gerenciados pela Microsoft. Os usuários têm acesso a alguns [novos recursos](#) não disponíveis com a Otimização do Citrix HDX.

---

## Interoperabilidade e roaming

A otimização do Citrix HDX (WebRTC) e a otimização do Microsoft SlimCore podem existir em paralelo, no entanto, o novo cliente Teams pode ser otimizado com apenas uma das formas por vez.

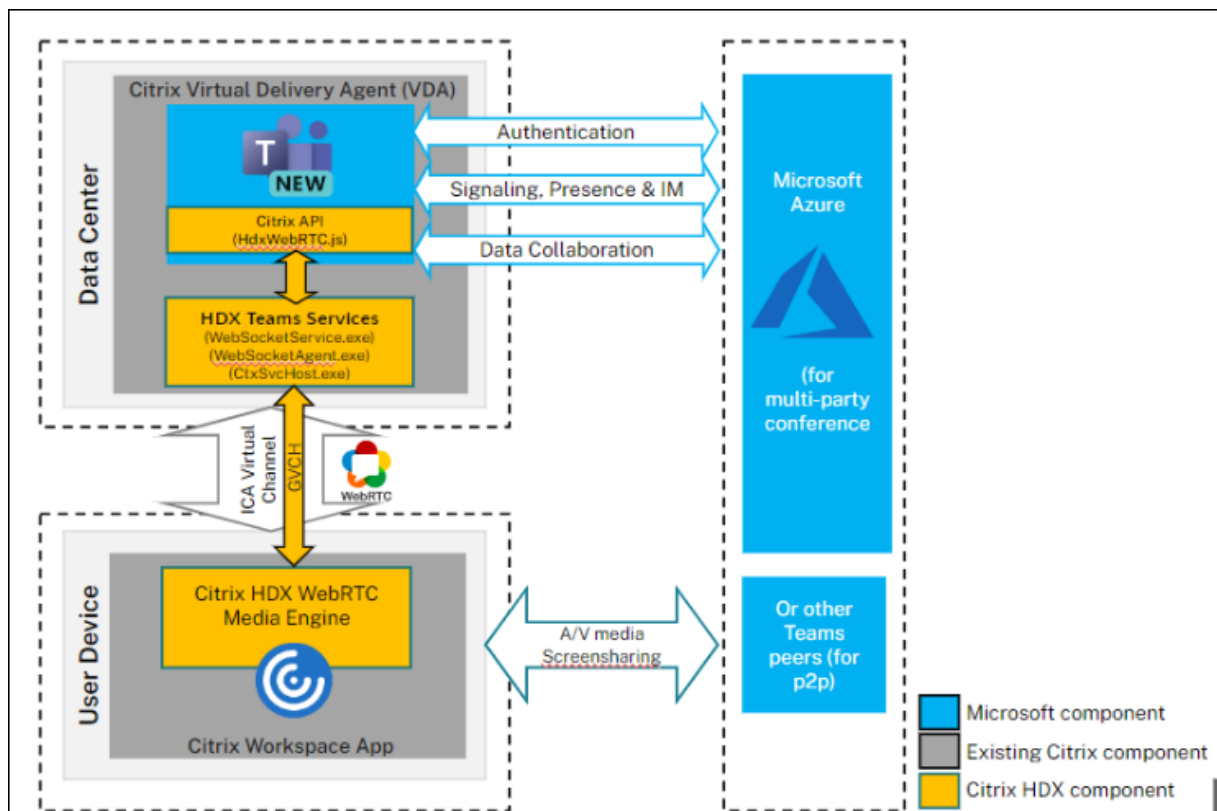
- O Novo Teams carrega o WebRTC ou o SlimCore em tempo de execução. Em tempo de execução, uma decisão é tomada na seguinte ordem: SlimCore > WebRTC > Redirecionamento padrão de áudio/vídeo.
- O processo de seleção não é dinâmico. Por exemplo: caso o Novo Teams comece a otimizar com o SlimCore e ocorra um problema, ele volta ao redirecionamento padrão de áudio/vídeo. É necessário reiniciar o aplicativo Teams para, em seguida, passar pelo processo de tomada de decisão e otimizar com o WebRTC.
- O mesmo cenário se aplica aos cenários de roaming. Por exemplo: se um usuário se conecta a partir de um endpoint com a otimização do SlimCore e faz roaming para um endpoint sem o plug-in (ou) um endpoint Mac/Linux, o Teams opera o redirecionamento padrão de áudio/vídeo. É necessário reiniciar o aplicativo Teams para voltar à otimização do WebRTC.

- Os cenários de roaming entre endpoints que já estão otimizados para o SlimCore estão integrados.

## Otimização do Citrix HDX

August 22, 2024

No Citrix HDX (Otimização de WebRTC), o mecanismo de mídia (HdxRtcEngine) no endpoint responsável por lidar com a mídia descarregada é incorporado ao aplicativo Citrix Workspace e a instalação do aplicativo Citrix Workspace também instala automaticamente o mecanismo.



## Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para oferecer suporte ao novo cliente Teams. Observe que, nas versões mínimas, algumas correções críticas de erros ou recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as correções e os recursos mais recentes.



## Sistemas operacionais VDI

Para obter informações detalhadas, consulte as recomendações fornecidas na documentação da [Microsoft](#).

### Nota:

- Não há suporte para o Windows Server 2016. A Citrix recomenda que você planeje suas atualizações adequadamente.
- Como as versões são atualizadas com frequência, as versões mencionadas aqui podem entrar em fim de vida útil. Portanto, consulte as páginas do ciclo de vida do produto do [aplicativo Citrix Workspace](#) e do [Citrix Virtual Apps and Desktops](#) para garantir que você esteja usando versões compatíveis de diferentes componentes.
- Se você usa o Citrix Virtual Apps and Desktops 1912 LTSR, a Citrix recomenda planejar uma atualização, pois sua vida útil será encerrada 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 qualquer versão 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 |

---

## Deployment

1. Instale o novo cliente do Teams na VDI. Para obter informações detalhadas, consulte [Implantar novo Teams para VDI](#).
2. Configure a seguinte chave de registro no VDA para otimizar o novo Teams.
  - **Localização:** `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
  - **Chave (REG\_Multi\_SZ):** `ProcessWhitelist`
  - **Valor:** `msedgewebview2.exe`

**Nota:**

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 do registro do `msedgewebview2.exe`, pois ela está listada como permitida por padrão.

3. Certifique-se de que a política de [redirecionamento do Microsoft Teams](#) esteja habilitada. Essa política está ativada por padrão.
4. Nenhuma configuração adicional é necessária no lado do cliente. Siga as instruções do assistente para instalar o aplicativo Citrix Workspace.

### **App Layering**

O novo Microsoft Teams mudou seu método de instalação e agora é instalado em C:\Program Files\WindowsApps. Para oferecer suporte a essa alteração, você deve executar o App Layering versão 2403.2 ou posterior. Você pode baixar um disco de atualização na página de [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 atual da versão mínima para o Citrix Profile Management é 2402 LTSR (ou) 2203 LTSR CU5+.

### **Considerações sobre rede**

Os requisitos de rede para o Novo Teams não diferem do Teams Clássico. Portanto, consulte a seção [Requisitos de rede](#) na documentação do Teams Clássico.

### **Matriz de recursos e compatibilidade de versões**

Como as versões são atualizadas com frequência, algumas versões mais antigas mencionadas aqui podem chegar ao fim da vida útil. Portanto, consulte as páginas do ciclo de vida do produto do [Aplicativo Citrix Workspace](#) e do [Citrix Virtual Apps and Desktops](#) para garantir que você esteja usando versões compatíveis de diferentes componentes.

**Nota:**

- As versões mencionadas aqui são as versões mínimas nas quais há suporte para o recurso específico (ou) a versão mínima na qual há suporte para o Novo Teams, a que for maior.
- O Citrix Virtual Apps and Desktops 1912 LTSR CU8+ indicado na seção de versões mínimas não está sendo mencionado na tabela abaixo, pois chegará ao fim de sua vida útil em dezembro de 2024. No entanto, ainda é uma versão com suporte até então.
- Os 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) | Aplicativo Citrix Workspace para Mac (versão mínima) | Aplicativo Citrix Workspace para Linux (versão mínima) | Aplicativo Citrix Workspace para ChromeOS (versão mínima) |
|----------------------------------------|-------------------------------------|----------------------------------------------------------|------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------|
| Áudio/vídeo (P2P e conferência)        | 2203 LTSR (qualquer CU),<br>2212 CR | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | 2301                                                      |
| Compartilhamento de tela               | 2203 LTSR (qualquer CU),<br>2212 CR | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | 2301                                                      |
| i. Borda vermelha do indicador de tela | 2203 LTSR (qualquer CU),<br>2212 CR | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | Não                                                       |
| ii. Limitar captura ao Desktop Viewer  | 2203 LTSR (qualquer CU),<br>2212 CR | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | Não                                                       |
| iii. Multimonitor                      | 2203 LTSR (qualquer CU),<br>2212 CR | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | Não                                                       |
| DTMF                                   | N/A                                 | 2203 LTSR CU mais recente,<br>2302 CR                    | 2302                                                 | 2207                                                   | 2301                                                      |

| Recurso                                       | VDA (versão mínima)              | Aplicativo Citrix Workspace para Windows (versão mínima) | Aplicativo Citrix Workspace para Mac (versão mínima) | Aplicativo Citrix Workspace para Linux (versão mínima) | Aplicativo Citrix Workspace para ChromeOS (versão mínima) |
|-----------------------------------------------|----------------------------------|----------------------------------------------------------|------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------|
| Suporte ao servidor proxy                     | N/A                              | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2207                                                   | 2305                                                      |
| Compartilhamento de aplicativos               | 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                                                      |
| Dar o controle                                | N/A                              | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2207                                                   | Não                                                       |
| Solicitar o controle                          | N/A                              | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2207                                                   | 2303                                                      |
| Várias janelas                                | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2207                                                   | 2303                                                      |
| Transcrições de reuniões                      | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2207                                                   | 2303                                                      |
| Desfoque de fundo                             | 2203 LTSR (qualquer CU), 2212 CR | 2203 LTSR CU mais recente, 2302 CR                       | 2302                                                 | 2212                                                   | 2303                                                      |
| Compartilhamento de tela (com App Protection) | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2309.1 CR                                     | 2308                                                 | 2311                                                   | Não                                                       |

| Recurso                       | VDA (versão mínima)              | Aplicativo Citrix Workspace para Windows (versão mínima) | Aplicativo Citrix Workspace para Mac (versão mínima) | Aplicativo Citrix Workspace para Linux (versão mínima) | Aplicativo Citrix Workspace para ChromeOS (versão mínima) |
|-------------------------------|----------------------------------|----------------------------------------------------------|------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------|
| Simulcast                     | 2203 LTSR (qualquer CU), 2212 CR | 2402 LTSR, 2305 CR                                       | 2305                                                 | 2305                                                   | 2312                                                      |
| Toque secundário              | 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 Novo Teams, consulte [CTX253754](#), [Solução de problemas do Microsoft Teams](#). Para obter as atualizações mais recentes sobre qualquer coisa relacionada ao Novo Teams, consulte [CTX585013](#).

## Limitações conhecidas

### Limitações no aplicativo Citrix Workspace

- Suporte a HID - Não há suporte para atender e encerrar chamadas. Aumentar e diminuir volume têm suporte.
- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.
- Limitações de compartilhamento do áudio do sistema
  - O áudio não pode ser compartilhado usando esse recurso ao compartilhar a tela com aplicativos ou guias redirecionados por RAVE e BCR.
  - Esse recurso tem suporte somente em áreas de trabalho publicadas.

### **Limitações no VDA**

- Não há suporte para o Novo Teams como um aplicativo publicado (integrado)
  - Corrigido no CVAD 2402 LTSR, 2203 LTSR CU5 e superior
- Quando você define a configuração de DPI alto do aplicativo Citrix Workspace como Sim, a janela de vídeo redirecionado aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum valor acima de 100%.

### **Limitação no aplicativo Citrix Workspace e no VDA**

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume no computador cliente, não no VDA.

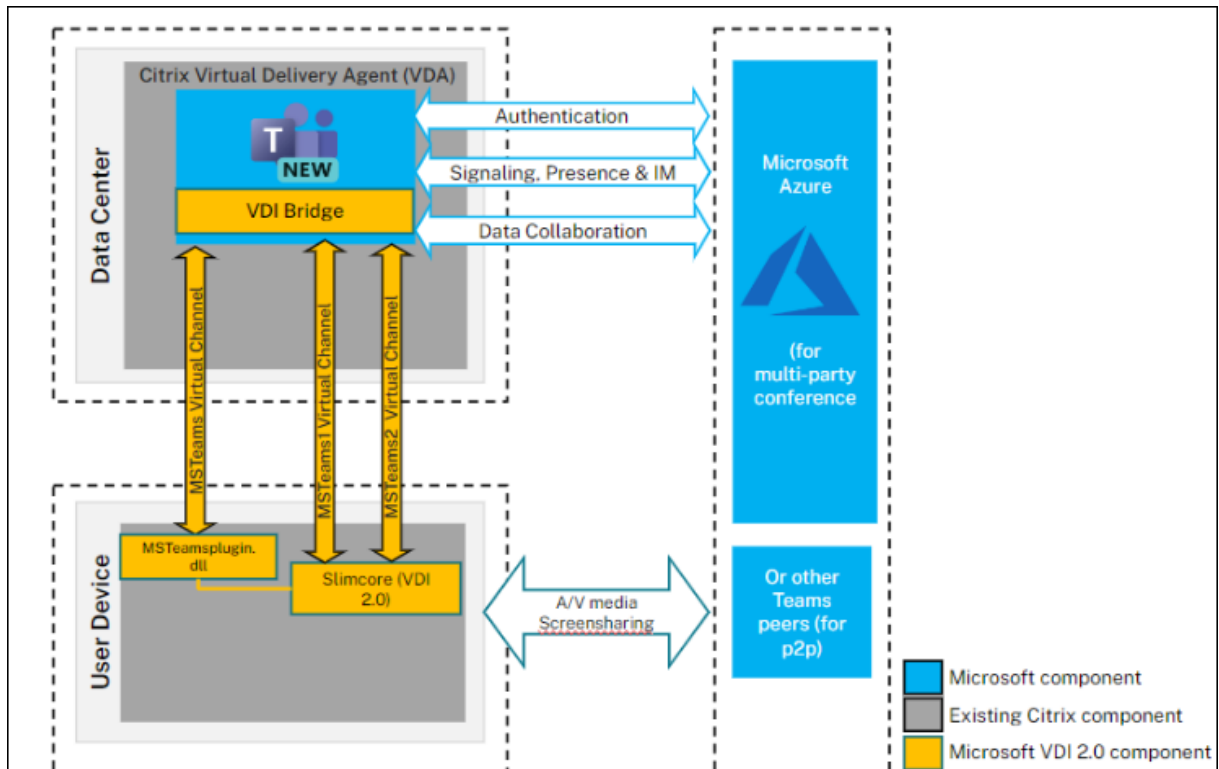
Para obter mais detalhes sobre as limitações da Microsoft, consulte [Recursos sem suporte na VDI](#).

## **Otimização do Microsoft SlimCore**

August 22, 2024

Na nova solução de VDI para o Teams, a Microsoft aproveitou o SDK do Canal Virtual da Citrix para criar canais virtuais personalizados e, no lado do endpoint, a Microsoft está usando o SlimCore, o mecanismo de mídia que alimenta o Microsoft Teams (cliente nativo) atualmente. Nessa otimização, o SlimCore seria responsável por gerenciar a mídia descarregada em vez do HdxRtcEngine. Os canais virtuais personalizados que a Microsoft criou serviriam como canal de comunicação entre o Teams na VDI e o mecanismo de mídia SlimCore.

Para obter mais informações, consulte [Nova solução de VDI para o Teams](#) e [O futuro do Microsoft Teams](#).



## Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para oferecer suporte à Otimização do Microsoft Teams SlimCore. Observe que, nas versões mínimas, algumas correções críticas de erros ou recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as correções e os recursos mais recentes.

## Virtual Delivery Agent (VDA)

### Nota:

Se você estiver usando a versão 2203 LTSR CU2 ou abaixo (ou) 2303 CR ou abaixo, consulte [CTX682593](#) para entender as limitações dessas versões e planejar sua atualização para as versões mínimas mencionadas abaixo para obter suporte para a Otimização do SlimCore.

### Versões mínimas

2203 LTSR CU3; 2305 CR

### Versões recomendadas

2203 LTSR CU5+ (ou) 2402 LTSR e qualquer versão CR acima

## Aplicativo Citrix Workspace (CWA)

### Nota:

Atualmente, a Otimização do SlimCore está disponível apenas para endpoints do Windows.

---

| Versões mínimas                                      | Versões recomendadas               |
|------------------------------------------------------|------------------------------------|
| Windows 2203 LTSR (CU mais recente); Windows 2302 CR | Windows 2402 LTSR; Windows 2405 CR |

---

Para obter recomendações sobre as versões mínimas do Teams, os requisitos do sistema operacional do endpoint e os requisitos de hardware, consulte a documentação da [Microsoft](#).

## Componentes

- vdiBridge do Novo Teams - Este é o módulo de canal virtual do lado do servidor
- Canal virtual (VC) personalizado - Este é o VC personalizado de propriedade do Microsoft Teams
- Plug-in - dll do VC do lado do cliente. Esse plugin é responsável pelo download e limpeza do SlimCore
- SlimCore - Mecanismo de mídia específico do sistema operacional

## Deployment

1. Certifique-se de ter a nova versão do Microsoft Teams, conforme recomendado em [Pré-requisitos](#).
2. Configure a política de lista de permissões de canais virtuais para permitir canais virtuais específicos do Microsoft Teams. Esses canais virtuais são necessários para que o novo cliente Teams possa se conectar ao plug-in do lado do cliente. Para obter mais informações sobre a lista de permissões de canais virtuais, consulte [Segurança de canais virtuais](#).

Para a Otimização do SlimCore, o Novo Microsoft Teams precisa de três canais virtuais personalizados. Use os curingas para permitir canais virtuais do `ms-teams.exe` executáveis e personalizados:

- ```
1 MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
2 MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
3 MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```



**Nota:**

- Os curingas da política de lista de permissões de canais virtuais estão disponíveis no CVAD 2203 LTSR CU2 e superior (ou) no Citrix Virtual Apps and Desktops 2206 CR e superior.
- As máquinas VDA devem ser reiniciadas para que a política entre em vigor.
- O caminho para a instalação do MTeams muda, pois é um aplicativo MSIX e, portanto, curingas são necessários. Certifique-se de incluir as linhas exatas recomendadas acima na lista de permissões

3. Ative a política do Novo Teams, se necessário, para um grupo de usuários específico (ela é ativada por padrão em nível global)
4. Implante [MTeamsplugin](#) em seus endpoints. Consulte a seção Opções para instalar o plugin MTeams para obter informações detalhadas. Para otimizar com o SlimCore nos endpoints da Citrix, a Citrix oferece várias maneiras para os clientes implantarem o [MTeamsplugin](#).
5. Consulte a documentação da [Microsoft](#) para obter mais etapas relacionadas à preparação e ao registro do SlimCore, pois pode haver casos que podem bloquear a instalação do pacote MSIX do novo mecanismo de mídia.

### Opções para instalar o plug-in MTeams

Independentemente do método de instalação, o plug-in MSI detecta automaticamente a pasta de instalação do aplicativo Citrix Workspace e coloca o MsTeamsPluginCitrix.dll nessa localização:

Localizações do plug-in dll quando o plug-in é instalado por meio das opções abaixo com a instalação do administrador do aplicativo Citrix Workspace:

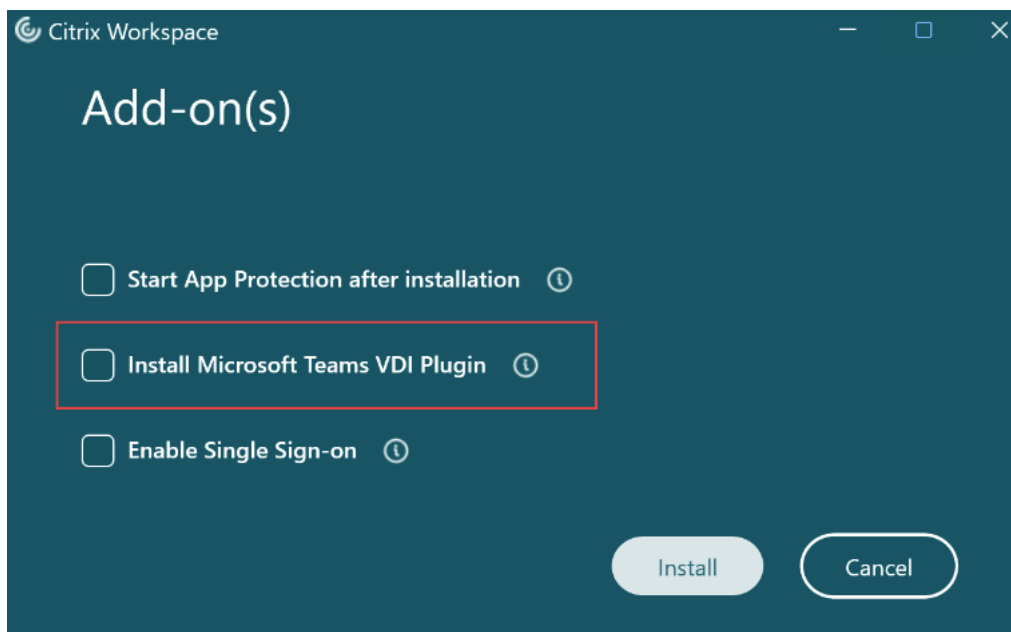
- 64 bits: C:\Program Files (x86)\Citrix\ICA Client
- 32 bits: C:\Program Files\Citrix\ICA Client

**Nota:**

- Certifique-se de que o aplicativo Citrix Workspace esteja instalado no modo de administrador. Isso garante que os canais virtuais sejam abertos corretamente.
- A instalação do plug-in será interrompida se nenhum aplicativo Citrix Workspace for encontrado no endpoint
- Para as experiências de primeira execução, duas reinicializações do aplicativo Teams são necessárias para entrar na Otimização do SlimCore. Para obter mais informações, consulte [Verificação da otimização do endpoint](#).

### Opção 1: implantar o plug-in por meio da instalação do aplicativo Citrix Workspace

- O plug-in MTeams pode ser instalado por meio da interface do usuário durante a nova instalação ou atualização manual.



- Você também pode instalar o plug-in MTeams por meio da instalação da linha de comando
  - Use a seguinte opção de linha de comando: `/InstallMSTeamsPlugin`  
Exemplo: `CitrixWorkspaceApp.exe /installMSTeamsPlugin`
- Para uma nova instalação, o requisito mínimo é: aplicativo Citrix Workspace para Windows 2402 LTSR. Para cenários de atualização em vigor, o requisito mínimo é: aplicativo Citrix Workspace para Windows 2405 CR.

### Opção 2: baixe o plug-in MSI diretamente

Se você não estiver usando as versões mais recentes nas quais a instalação do plug-in por meio do CWA é compatível, poderá baixar o plug-in MSI [aqui](#) e implantá-lo usando ferramentas como o SCCM, além de qualquer versão existente do aplicativo Citrix Workspace compatível.

### Opção 3: implantar o plug-in usando o Global App Configuration Service

O Global App Configuration Service ajuda você a gerenciar as configurações do aplicativo para endpoints gerenciados e não gerenciados e agora você também pode implantar o plug-in Teams em seus endpoints por meio do GACS.

Consulte a documentação de [Gerenciamento de plug-ins do Microsoft Teams](#) para obter detalhes sobre como gerenciar o plug-in Teams por meio do GACS.

### **Considerações sobre rede**

Para a Otimização do SlimCore, consulte [Considerações sobre rede](#) na documentação da Microsoft para obter os detalhes necessários.

### **Matriz de recursos e compatibilidade de versões**

Com a Otimização do SlimCore, como os recursos e a implementação da solução VDI são de propriedade da Microsoft, consulte a [documentação da Microsoft](#).

### **Solução de problemas e outras considerações**

Para o Novo Teams com a Otimização do Microsoft SlimCore, consulte a documentação da [Microsoft](#).

### **Limitações conhecidas**

Com a Otimização do SlimCore, como os recursos e a implementação da solução VDI são de propriedade da Microsoft, consulte os [problemas conhecidos](#) documentados pela Microsoft.

## **Otimização para Microsoft Teams (clássico)**

September 11, 2024

#### **Nota:**

O novo Microsoft Teams 2.1 agora está disponível para VDA. Essa versão do Microsoft Teams é compatível com a Otimização do Microsoft Teams da Citrix usando WebRTC. Para obter mais informações sobre a otimização para o Novo Teams, consulte [Novo MS Teams](#)

A partir do Citrix Virtual Apps and Desktops 2402, você não precisa configurar manualmente a entrada do registro do `msedgewebview2.exe`, pois ela está listada como permitida por padrão.

Os aplicativos publicados agora são compatíveis com o novo Microsoft Teams.

A Citrix oferece otimização para Microsoft Teams baseados em desktop usando o Citrix Virtual Apps and Desktops e o aplicativo Citrix Workspace. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

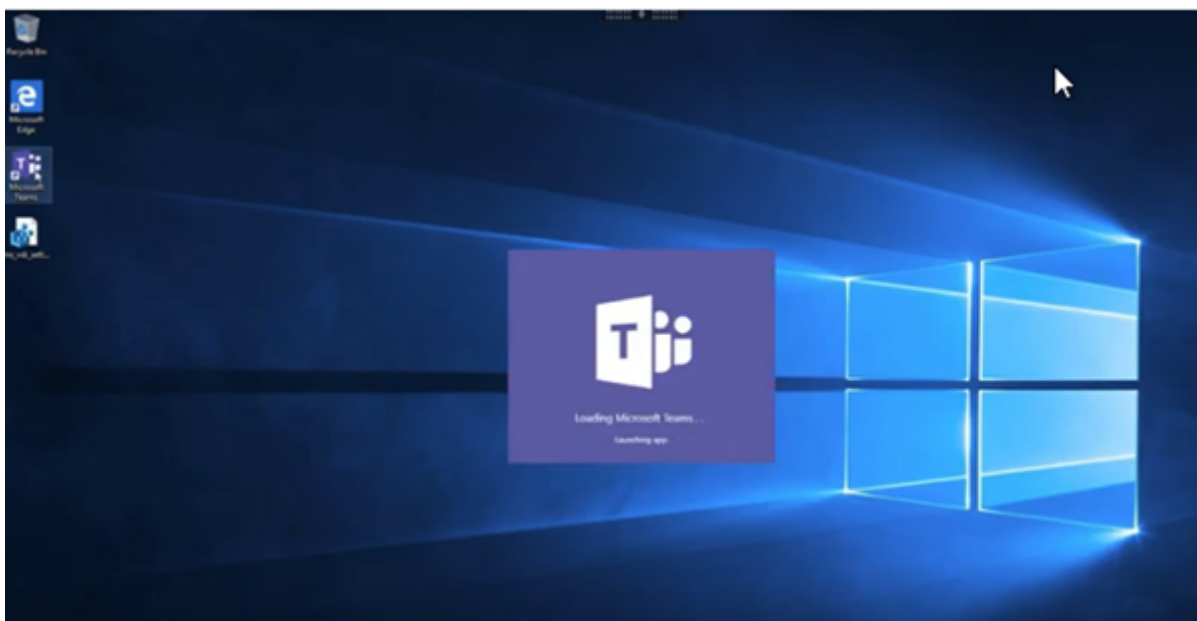
Nossa otimização para o Microsoft Teams inclui serviços HDX do lado do VDA e API para fazer interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O ponto de extremidade decodifica e renderiza a multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem de forma nativa no aplicativo hospedado pelo Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O **CTXMTOP** é um comando e controle de canal virtual. Isso significa que não há troca de mídia entre o aplicativo Citrix Workspace e o VDA.

Apenas a busca de cliente/renderização do cliente está disponível.

Esta demonstração de vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



## Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam o uso da versão mais recente disponível do Microsoft Teams e que a mantenham atualizada.

As versões do aplicativo de desktop Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas.

Versões não suportadas do aplicativo de desktop Microsoft Teams mostram uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte [Histórico de atualizações do aplicativo Microsoft Teams \(Desktop e Mac\)](#).

Recomendamos que você siga as [diretrizes de instalação em todo o computador do Microsoft Teams](#). Evite usar o instalador .exe que instala o Microsoft Teams no AppData. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` da linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1  
ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Quando você define esse parâmetro, o Instalador de Todo o Computador do Microsoft Teams aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro `ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` somente em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não é atualizado automaticamente sempre que há uma nova versão. Recomendamos esse modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou áreas de trabalho fora de catálogos aleatórios/agrupados do Windows Server ou Windows 10. Para obter mais informações, consulte [Instalar o Microsoft Teams usando MSI](#) (seção Instalação da VDI).

Suponha que você tem um ambiente VDI persistente dedicado do Windows 10. Você deseja que o aplicativo Microsoft Teams atualize automaticamente e prefere que o Microsoft Teams instale por usuário em `Appdata/Local`. Nesse caso, use o instalador .exe ou o MSI sem `ALLUSER=1`.

**Nota:**

Recomendamos instalar o VDA antes de instalar o Microsoft Teams na golden image. Esta ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA foi, desinstale e reinstale o Microsoft Teams.

## Para Remote PC Access

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior depois de instalar o VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte

o VDA conforme o esperado. A versão 1.4.00.22472 ou posterior inclui lógica aumentada executada no momento da inicialização do Microsoft Teams e no momento do login para a detecção do VDA. Essas versões também incluem a identificação do tipo da sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem não detectar e desativar determinados recursos ou elementos da interface do usuário. Por exemplo, salas simultâneas, janelas pop-out de reuniões e chats, ou reações da reunião.

#### **Importante:**

Quando você faz roaming de uma sessão local para uma sessão HDX com o Microsoft Teams ainda aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar com o HDX corretamente.

Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Quando estiver trabalhando no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do Remote PC Access (HDX ou local). Isso porque o Microsoft Teams só pode avaliar o modo VDI no momento da inicialização do aplicativo, não quando ele já está sendo executado em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-out, salas simultâneas ou reações à reunião.

### **Para App Layering**

Se estiver usando o Citrix App Layering para gerenciar instalações do VDA e do Microsoft Teams em camadas diferentes, você deve criar uma chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em [Multimídia](#).

### **Recomendações de gerenciamento de perfis**

Recomendamos usar o instalador em toda o computador para ambientes Windows Server e VDI em pool no Windows 10.

Quando o sinalizador **ALLUSER =1** é passado para o MSI a partir da linha de comando (o instalador em todo o computador), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~ 300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600—700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

**Importante:**

Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e setup.json em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em: `HKEY_LOCAL_MACHINE \SOFTWARE\ WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

Um logon de usuário subsequente aciona a instalação final em **AppData**, em vez disso.

**Instalador em toda a máquina**

Veja a seguir um exemplo de pastas, atalhos de área de trabalho e registros criados com a instalação de um instalador do Microsoft Teams em todo o computador em uma VM de 64 bits do Windows Server 2016:

*Pasta:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\\AppData\Roaming\Microsoft\Teams`

*Atalho da área de trabalho:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Registro:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: Teams
- Tipo: REG\_SZ
- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

**Nota:**

A localização do registro varia de acordo com os sistemas operacionais subjacentes e o número de bits.

**Recomendações, em Recommendations**

- Recomendamos desativar o início automático excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do dia de trabalho) sobrecarreguem a CPU da VM.

- Se o Virtual Desktop não tiver uma GPU/vGPU, recomendamos a configuração **Desabilitar a aceleração de hardware GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração ("`disableGpu`": `true`) é armazenada 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 o **CPU Spikes Protection** para gerenciar o consumo do processador para o Microsoft Teams.

## Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação é diferente. Todos os arquivos são colocados em AppData.

*Pasta:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Atalho da área de trabalho:*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"
```

*Registro:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

## Melhores práticas

As recomendações de melhor prática baseiam-se nos cenários de caso de uso.

O uso do Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente de dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as informações específicas do usuário apropriadas são armazenadas em cache durante a sessão do usuário. Por exemplo, as informações específicas do usuário incluem dados do usuário, perfil e configurações. Sincronize os dados nessas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

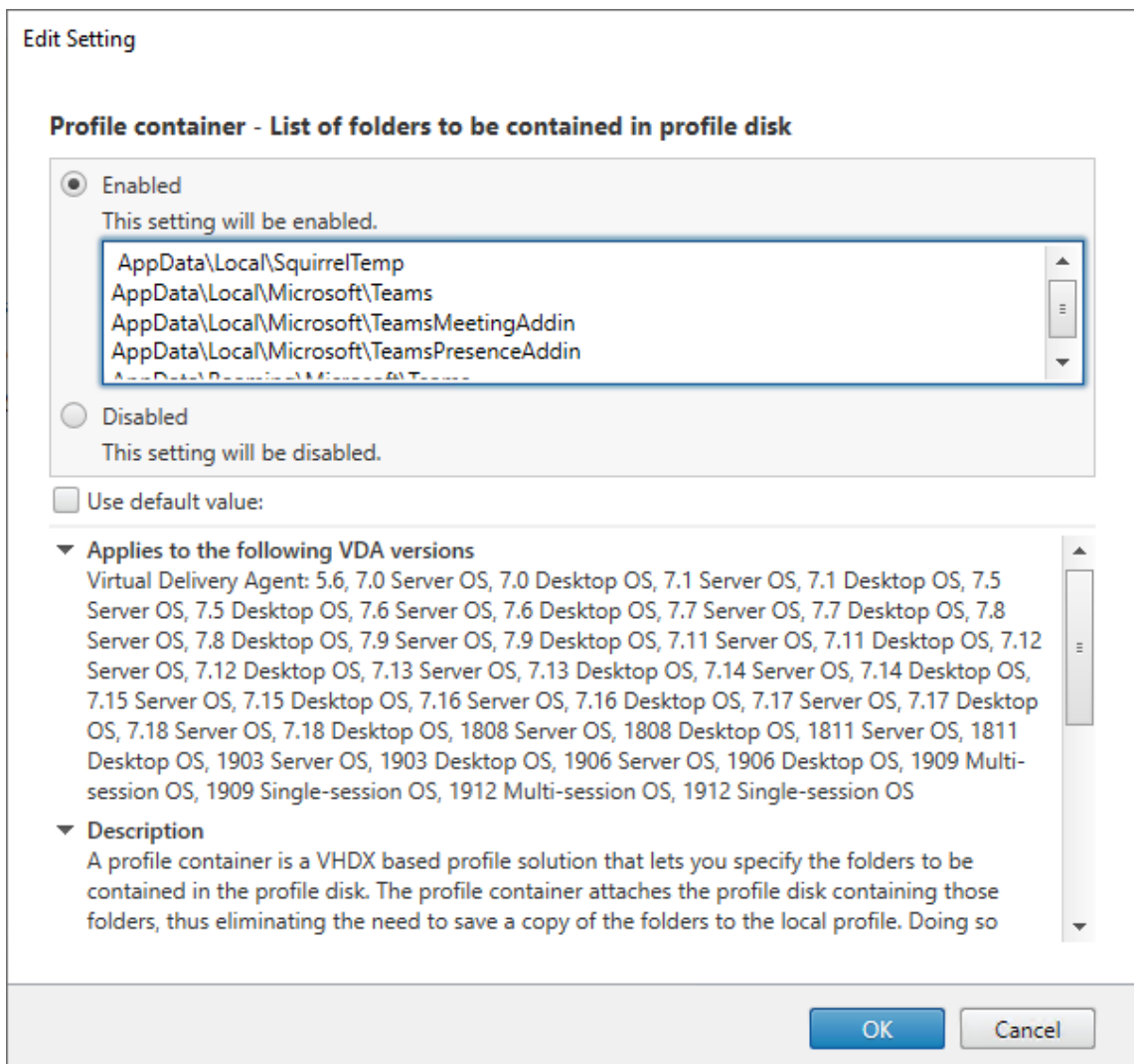


**Lista de exclusão de conteúdo armazenado em cache do Microsoft Teams para configuração não persistente** Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams, conforme descrito na documentação da [Microsoft](#). Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais a configuração não persistente.

**Caso de uso: cenário de sessão única** Nesse cenário, o usuário final usa o Microsoft Teams em um local de cada vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Por exemplo, em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop e o Microsoft Teams é implantado na área de trabalho virtual como um aplicativo.

Recomendamos ativar o contêiner Citrix Profile e redirecionar diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador de toda a máquina do Microsoft Teams (**ALLUSER=1**) na imagem de ouro.
2. Ative o Citrix Profile Management e configure o armazenamento de perfis de usuário com as permissões apropriadas.
3. Ative a seguinte configuração de política do Profile Management: **File system > Synchronization > Profile container –Lista de pastas que devem estar no disco de perfil.**



Liste todos os diretórios por usuário nesta configuração. Você também pode configurar essas configurações usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

## Requisitos do sistema

### Versão mínima recomendada - Delivery Controller (DCs) 1906.2

Se você estiver usando uma versão anterior, consulte [Ativar a otimização do Microsoft Teams](#):

Sistemas operacionais compatíveis:

- Windows Server 2022, 2019, 2016, 2012R2, edições Standard e Datacenter, e com a opção Server Core

## **Versão mínima - Virtual Delivery Agents (VDAs) 1906.2**

Sistemas operacionais compatíveis:

- Windows 11
- Windows 10 64 bits, versões 1607 e posteriores. Os aplicativos hospedados na máquina virtual são compatíveis com o aplicativo Citrix Workspace para Windows 2109.1 ou versões posteriores
- Windows Server 2022, 2019, 2016 e 2012 R2 (edições Standard e Datacenter)

Requisitos:

- BCR\_x64.msi - o MSI que contém o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não a exclua.

## **Versão recomendada —aplicativo Citrix Workspace para Windows mais recente CR e versão mínima - Citrix Workspace app 1907 para Windows**

- Windows 11.
- Windows 10 (edições de 32 bits e 64 bits, incluindo edições Embedded) (suporte para Windows 7 interrompido na versão 2006) (suporte para Windows 8.1 interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSC (v1607) e 2019 LTSC (v1809).
- Arquiteturas do processador (CPU) suportadas: x86 e x64 (o ARM não é suportado).
- Requisito de ponto de extremidade: CPU dual-core de aproximadamente 2,2 a 2,4 GHz que pode dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs de núcleo duplo ou quádruplo com velocidades de base mais baixas (~ 1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Clientes finos HP verificados: t630/t640, t730/t740, mt44/mt45.
- Clientes finos Dell verificados: 5070, 5470 Mobile TC e AIO.
- Clientes finos 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de pontos de extremidade verificados, consulte [Clientes finos](#).
- O aplicativo Citrix Workspace requer um mínimo de 600 MB de espaço livre em disco e 1 GB de RAM.
- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se não está 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 começam no modo otimizado no aplicativo Citrix Workspace não têm a opção de desativar o Microsoft Teams.

### **Versão mínima - aplicativo Citrix Workspace 2006 para Linux**

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 da autenticação:

- Biblioteca Libsecret
- Biblioteca libunwind-12. Para obter mais informações, consulte [Adding the libunwind-12 library dependency for llvm-12](#).

Hardware:

- CPU dual-core mínima de 1,8 GHz que possa dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com uma velocidade base de 1,8 GHz e uma alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de pontos de extremidade verificados, consulte [Clientes finos](#).

Para obter mais informações, consulte [Pré-requisitos para instalar o aplicativo Citrix Workspace](#).

Você pode desativar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é VDWEBRTC=On. Depois que a atualização for concluída, reinicie a sessão. (É necessária permissão raiz).

### **Versão mínima - Aplicativo Citrix Workspace 2012 para Mac**

Sistemas operacionais compatíveis:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 ou posterior.
- macOS Monterey.

Recursos suportados:

- Áudio

- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

**Nota:**

O aplicativo Citrix Viewer requer acesso às preferências de segurança e privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência no **menu Apple > Preferências do sistema > Segurança e privacidade > guia Privacidade > Screen recording** e selecionam **Citrix Viewer**.

A otimização do Microsoft Teams funciona por padrão se o usuário tiver o aplicativo Citrix Workspace 2012 ou posterior e o macOS 10.15.

Se você deseja desativar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

**Versão mínima –Versão mais recente do aplicativo Citrix Workspace para ChromeOS em execução na versão mais recente do ChromeOS**

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core de 2,4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desativada por padrão. Consulte estas [configurações](#) para obter instruções sobre como ativá-la.

**Escalabilidade de um único servidor**

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) são suportados em um único host físico. Isso é comumente chamado de Citrix Virtual Apps and Desktops Single Server Scalability (SSS). No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade do usuário. A ideia é descobrir quantos usuários ou máquinas virtuais podem ser executados em um único equipamento de hardware executando um hipervisor principal.

**Nota:**

Esta seção inclui uma orientação para fazer uma estimativa de SSS. A orientação é de alto nível e pode não ser necessariamente específica para sua situação ou ambiente exclusivo. A única maneira de realmente entender o Citrix Virtual Apps and Desktops SSS é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda seguir essa orientação e essas regras simples para fazer uma estimativa rápida apenas da SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar equipamentos de hardware ou tomar qualquer decisão financeira.

**Hardware (sistema em teste)**

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máximo Turbo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- 6 TB de armazenamento SSD RAID 0 local (11 discos)

**Software**

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando o Citrix Virtual Apps and Desktops 2106  
VMware ESXi 6.7

**Terminologia**

- Carga de trabalho do Knowledge Worker: inclui Acrobat Reader, Freemind/Java, Photo viewer, Edge e aplicativos MS Office, como Excel, Outlook, PowerPoint e Word.
- Baseline: os testes de escalabilidade do servidor são executados com a carga de trabalho do Knowledge Worker (sem o Microsoft Teams).
- Carga de trabalho do Microsoft Teams: carga de trabalho típica do Knowledge Worker + Microsoft Teams.

**Como é realizado o teste de estresse no Microsoft Teams**

- O Microsoft Teams é otimizado com o HDX. Portanto, todo o processamento multimídia é descarregado para o ponto de extremidade ou cliente e não faz parte da medição.

- Todos os processos do Microsoft Teams são interrompidos ou eliminados antes do início da carga de trabalho.
- Abra o Microsoft Teams (inicialização a frio).
- Meça o tempo gasto pelo Microsoft Teams para carregar e capturar o foco da janela principal do Microsoft Teams.
- Alterne para a janela de bate-papo usando atalhos de teclado.
- Alterne para a janela do calendário usando atalhos de teclado.
- Envie a mensagem de bate-papo para um usuário específico usando atalhos de teclado.
- Alterne para a janela do Microsoft Teams usando atalhos de teclado.

## Resultados

- 40% de impacto na escalabilidade com o Microsoft Teams Workload (81 usuários), quando comparado ao Baseline (137 usuários).
- Aumentar a capacidade do servidor em ~40% (na CPU) restaura o número de usuários como com a carga de trabalho Baseline.
- 20% de memória extra necessária com o Microsoft Teams Workload, quando comparado ao Baseline.
- Aumento do tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% em gravações de IOPS, aumento de ~100% em leituras de IOPS. O Microsoft Teams pode ter um impacto significativo em um ambiente com armazenamento mais lento.

## Matriz de recursos e compatibilidade de versões

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo			Aplicativo
			Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Citrix Workspace para ChromeOS (versão mínima)
Áudio/Vídeo (P2P e conferência)	Versão atual menos 90 dias	1906	1907	2009	2004	2105.5

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	2012	2006	2105.5
i. Indicador de tela Borda vermelha	Versão atual menos 90 dias	1906	2002	2012	2006	Não
ii. Limitar captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	2012	2006	Não
iii. Multi-monitor	Versão atual menos 90 dias	1912 CU6+	2106 (1)	2106	2106	Não
DTMF	Versão atual menos 90 dias	N/A	2102	2101	2101	2111.1
Suporte a Proxy Server	Versão atual menos 90 dias	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Compartilhamento de aplicativos	Versão atual menos 90 dias	2109	2109.1	2203.1	2209	Não
Legendas ao vivo	Versão atual menos 90 dias	N/A (4)	2109.1	2109	2109	2303



Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
e911 dinâmico	Versão atual menos 90 dias	N/A	2112.1	2112	2112	2112
Dar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	Não	Não
Solicitar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	2203	2303
Várias janelas	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Transcrições de reuniões	Versão atual menos 90 dias	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Desfoque do fundo	Versão atual menos 90 dias	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer somente no modo de tela cheia. SHIFT+F2 não é suportado.
2. Negociar/Kerberos, NTLM, Basic e Digest. Pac os arquivos também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, a legenda ao vivo só funcionará se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 para Linux ou 2112 para Windows. Isso ocorre porque as legendas ao vivo se comportam de maneira diferente se o Microsoft Teams está no modo de IU de Janela única ou no modo Várias janelas.
5. O modo Várias janelas foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

**Nota:**

- Todos os recursos listados no **aplicativo Citrix Workspace para Windows 1912 CU6 (ou posterior)** são aplicáveis ao aplicativo Citrix Workspace para Windows 2203.1 LTSR CU1.
- A Microsoft preteriu o suporte ao modo Janela única no Microsoft Teams. Para ajustar-se às normas, você deve atualizar seu VDA para 1912 CU6+ LTSR e o aplicativo Citrix Workspace para 2203 CU2+ ou superior, que oferece suporte ao modo Várias janelas.

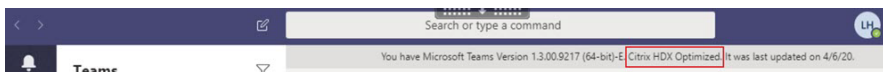
## Ativar a otimização do Microsoft Teams

Para habilitar a otimização para o Microsoft Teams, use a política Gerenciar console descrita na política de [redirecionamento do Microsoft Teams](#). Essa política está **ATIVADA** por padrão. Além da ativação dessa política, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima necessária. Se você habilitou a política e a versão do aplicativo Citrix Workspace for suportada, **HKEY\_CURRENT\_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definida como **1** automaticamente no VDA. O Microsoft Teams lê a chave a ser carregada no modo VDI.

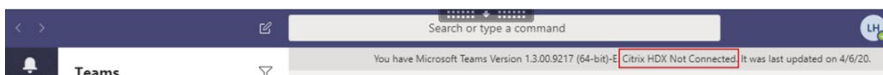
**Nota:**

Se você estiver usando VDAs da versão 1906.2 ou posterior com versões mais antigas do controlador (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda poderá ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

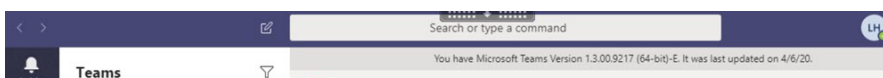
Se você clicar em **About > Version**, a legenda **Citrix HDX Optimized** exibirá:



Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro em partes posteriores da pilha. O erro é mais provável nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, isso indica que o Microsoft Teams não conseguiu carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito no ícone da área de notificação e reinicie. Certifique-se de que a política Gerenciar console não esteja definida como **Proibido** e que a versão do aplicativo Citrix Workspace seja suportada.



### **Importante: a sessão se reconecta**

- Talvez seja necessário reiniciar o Microsoft Teams para obter uma sessão otimizada para HDX quando sua conectividade mudar. Por exemplo, se você estiver fazendo o roaming de um ponto de extremidade não compatível (aplicativo Workspace para iOS, Android ou versões antigas do Windows/Linux/Mac) para um ponto de extremidade compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou o oposto.
- A reinicialização do Microsoft Teams também é necessária se você tiver instalado o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações de VDI persistentes. Nesses casos, o Microsoft Teams pode atualizar automaticamente enquanto a sessão HDX está no estado desconectado. Portanto, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado em um estado otimizado.
- Ao fazer o roaming de uma sessão local para uma sessão HDX, você precisa reiniciar o Microsoft Teams para otimizar com o HDX. Essa ação é necessária em um cenário de acesso remoto ao PC.

### **Requisitos de rede**

O Microsoft Teams conta com servidores de Processador de Mídia no Microsoft 365 para reuniões ou chamadas multipartes. O Microsoft Teams usa retransmissões de transporte do Microsoft 365 para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Portanto, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Consulte os [Princípios de conectividade de rede do Microsoft 365](#) para obter diretrizes detalhadas sobre o planejamento de rede.

Recomendamos avaliar seu ambiente para identificar os riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem.

Use a [Ferramenta de avaliação de rede do Skype for Business](#) para testar se sua rede está pronta para o Microsoft Teams. Para obter informações sobre suporte, consulte [Suporte](#).

### **Resumo das principais recomendações de rede para o tráfego RTP (Real Time Protocol)**

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir da filial.
- Planeje e forneça largura de banda suficiente na filial.
- Verifique se há conectividade e qualidade de rede em cada filial.

- Se você precisar usar qualquer um dos itens a seguir na filial, certifique-se de que o tráfego RTP/UDP (manipulado pelo HdxRtcEngine.exe no aplicativo Citrix Workspace) esteja desimpedido.
  - Ignorar servidores proxy
  - Interceptação SSL de rede
  - Dispositivos de inspeção profunda de pacotes
  - VPN hairpin (use tunelamento dividido, se possível)

#### **Importante: configuração de túnel dividido de VPN**

O tráfego do HdxRtcEngine.exe deve ser desviado do túnel VPN e ter a permissão de usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira pela qual isso é realizado depende do produto VPN e da plataforma de máquina usada, mas a maioria das soluções VPN permite a configuração simples da política para aplicar essa lógica. Para obter mais informações com orientações de túnel dividido específicas à plataforma VPN, consulte [este artigo da Microsoft](#).

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o SRTP (Secure Real-Time Transport Protocol) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para esse recurso, são usadas chaves simétricas (negociadas com DTLS) para criptografar mídia e controlar mensagens usando a codificação de criptografia AES.

As seguintes métricas são recomendadas para garantir uma experiência positiva do usuário:

Métrica	Ponto de extremidade para Microsoft 365
Latência (um sentido)	< 50 ms
Latência (RTT)	< 100 ms
Perda de pacote	< 1% durante um intervalo de 15s
Jitter entre chegada de pacotes	<30ms durante um intervalo de 15s

Para obter mais informações, consulte [Preparar a rede da sua organização para o Microsoft Teams](#).

Em termos de requisitos de largura de banda, a otimização para o Microsoft Teams pode usar uma grande variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam estes codecs durante o processo do estabelecimento de chamada usando a oferta/resposta do Session Description Protocol (SDP).

As recomendações mínimas da Citrix são:

---

Tipo	Largura de banda	Codec
Áudio (em cada sentido)	~ 90 kbps	G.722
Áudio (em cada sentido)	~ 60 kbps	Opus*
Vídeo (em cada sentido)	~ 700 kbps	H264 360p a 30 fps 16:9
Compartilhamento de tela	~ 300 kbps	H264 1080p a 15 fps

---

\* O Opus suporta codificação de taxa de bits constante e variável de 6 kbps até 510 kbps.

Opus e H264 são os codecs preferidos para chamadas ponto a ponto e em conferência.

#### Importante:

Quanto ao desempenho, a codificação é mais cara do que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix Workspace para Linux e Windows. Consulte [Encoder performance estimator](#) e [Otimização para Microsoft Teams](#).

## Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

Se você configurar um servidor proxy explícito no VDA e encaminhar conexões para localhost por meio de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Bypass proxy servers for local address** em **Internet Options > Connections > LAN Settings > Proxy Servers** e ignorar 127.0.0.1:9002.

Se você usar um arquivo PAC, o script de configuração do proxy VDA do arquivo PAC deverá retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

Se a filial estiver configurada para acessar a Internet por meio de um proxy, esses aplicativos suportam servidores proxy:

- Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos [Pac](#) também têm suporte)
- Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos [Pac](#) também têm suporte)

- Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
- Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler configurações de proxy. Esses dispositivos enviam tráfego diretamente para servidores do Microsoft 365 TURN.

**Importante:**

- Verifique se o dispositivo cliente pode se conectar ao servidor DNS para executar resoluções de DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor Microsoft Teams Relay:
  - [worldaz.relay.teams.microsoft.com](https://worldaz.relay.teams.microsoft.com)
  - [inaz.relay.teams.microsoft.com](https://inaz.relay.teams.microsoft.com)
  - [uaeaz.relay.teams.microsoft.com](https://uaeaz.relay.teams.microsoft.com)
  - [euaz.relay.teams.microsoft.com](https://euaz.relay.teams.microsoft.com)
  - [usaz.relay.teams.microsoft.com](https://usaz.relay.teams.microsoft.com)
  - [turn.dod.teams.microsoft.us](https://turn.dod.teams.microsoft.us)
  - [turn.gov.teams.microsoft.us](https://turn.gov.teams.microsoft.us)

Se as solicitações de DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e chamadas de 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 no cliente).

## **Estabelecimento de chamadas e caminhos de fluxo de mídia**

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão SRTP (Secure Real-Time Transport Protocol) de rede direta via User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia recorre ao TCP/TLS 443.

O mecanismo de mídia HDX dá suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal usando retransmissões em torno de NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Este suporte significa que o ponto de extremidade deve poder executar resoluções DNS.

Considere um cenário em que não há caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está ingressando em uma chamada ou reunião com vários participantes. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP da sub-rede do Microsoft 365 e

quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver bloqueado). Para obter mais informações, consulte o diagrama de arquitetura na Configuração de chamada e [URLs do Office 365 e intervalos de endereços IP ID 11](#).

ID	Categoria	Endereços	Portas de destino
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	<b>UDP:</b> 3478, 3479, 3480, 3481, <b>TCP:</b> 443 (fallback)

Esses intervalos incluem retransmissões de transporte e processadores de mídia, com front-end por um Azure Load Balancer.

As retransmissões de transporte do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são pontos de extremidade ICE. Além disso, as retransmissões de transporte do Microsoft Teams não terminam a mídia, o TLS, nem realizam nenhuma transcodificação. Elas podem fazer a ponte TCP (se HdxRtcEngine.exe usar TCP) para o UDP quando encaminham o tráfego para outros pares ou processadores de mídia.

O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com a retransmissão de transporte do Microsoft Teams mais próxima na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e porta 3478—3481 UDP (portas UDP diferentes por carga de trabalho, embora possa haver multiplexação) ou 443 TCP/TLS para fallbacks. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado por TCP, aconselhamos você a projetar suas redes para acomodar o tráfego UDP na filial.

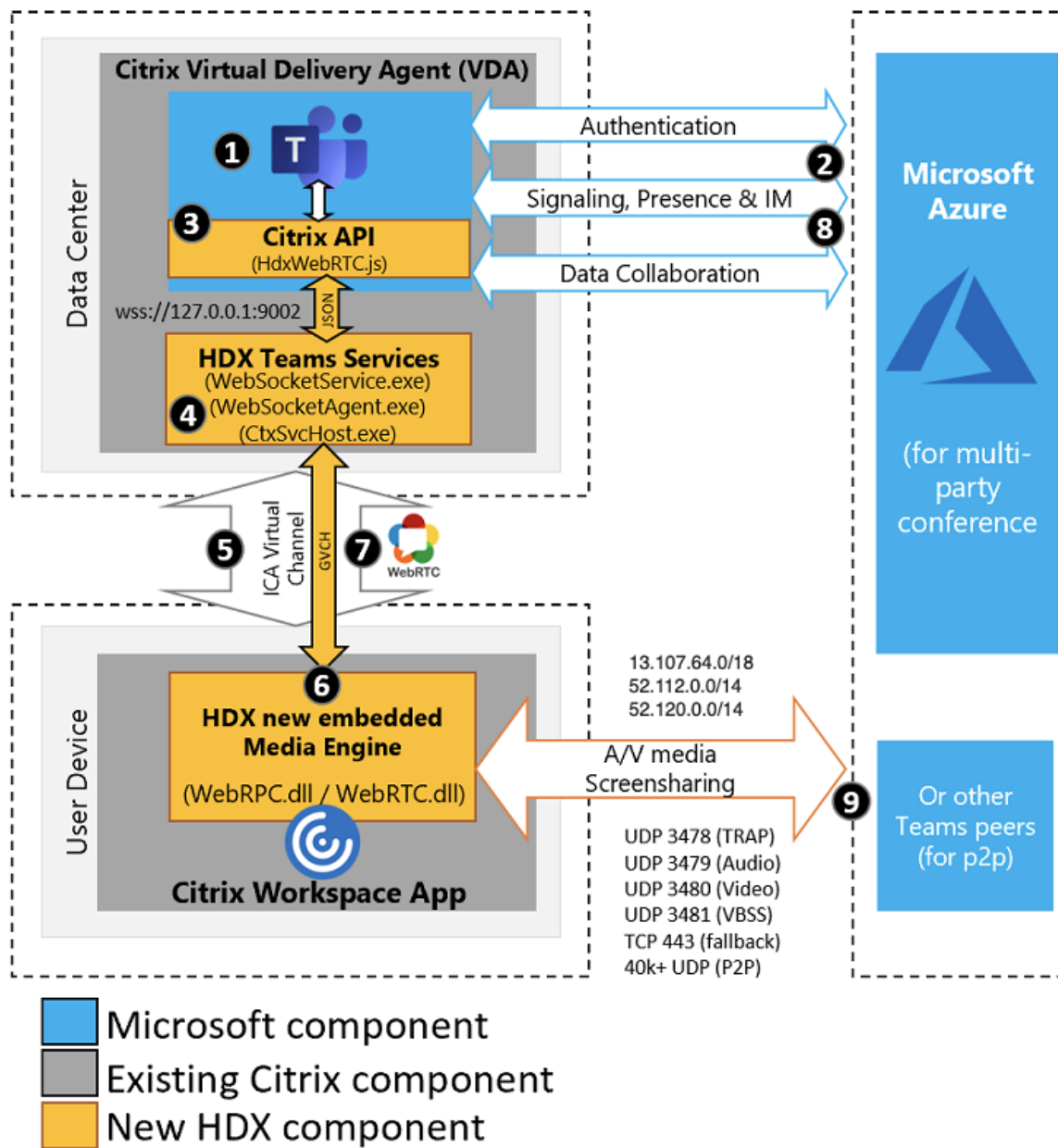
Se o Microsoft Teams for carregado no modo otimizado e o HdxRtcEngine.exe estiver sendo executado no ponto de extremidade, as falhas do ICE podem causar uma falha na configuração da chamada ou áudio/vídeo somente unidirecional. Quando um atendimento não pode ser concluído ou os fluxos de mídia não forem full duplex, verifique primeiramente o **rastreamento Wireshark** no ponto de extremidade. Para obter mais informações sobre o processo de coleta do candidato ICE, consulte “Coletando logs” na seção [Suporte](#).

**Nota:**

Se os pontos de extremidade não tiverem acesso à Internet, os usuários talvez ainda possam fazer uma chamada ponto a ponto somente se os dois estiverem na mesma LAN. As reuniões não ocorrem. Neste caso, há um intervalo de 30 segundos antes que a configuração de chamada comece.

### Configuração de chamada

Use este diagrama de arquitetura como uma referência visual para a sequência de fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.



### Arquitetura

1. Inicie o Microsoft Teams.
2. O Microsoft Teams é autenticado no O365. As políticas de locatário são enviadas para o cliente Microsoft Teams e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.



3. O Microsoft Teams detecta que ele está sendo executado em um VDA e faz chamadas de API para a API JavaScript Citrix.
4. O Citrix JavaScript no Microsoft Teams abre uma conexão segura do WebSocket ao WebSocket-Service.exe em execução no VDA, que gera WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico ligando para o Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe).
6. O wfica32.exe (mecanismo HDX) do aplicativo Citrix Workspace gera um novo processo chamado HdxRtcEngine.exe, que é o novo mecanismo WebRTC usado para a otimização do Microsoft Teams.
7. O mecanismo de mídia Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem iniciar o processamento de solicitações de multimídia.

—Chamadas do usuário—

8. O **par A** clica no botão de **chamada**. Teams.exe se comunica com os serviços do Microsoft Teams no Microsoft 365 estabelecendo um caminho de sinalização de ponta a ponta com o **par B**. O Microsoft Teams solicita ao HdxRtcEngine uma série de parâmetros de chamada compatíveis (codecs, resoluções e assim por diante, que é conhecida como oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e daí para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização e quando são concluídas as verificações de conectividade ICE (travessia de NAT e firewall por meio de solicitações de ligação STUN). Então, a mídia Secure Real-Time Transport Protocol (SRTP) flui diretamente entre HdxRtcEngine.exe e o outro par (ou Microsoft 365, se for uma reunião).

## Sistema de Telefonia da Microsoft

O Sistema de Telefonia é a tecnologia da Microsoft que permite o controle de chamadas e PBX na nuvem do Microsoft 365 com o Microsoft Teams. A Otimização para Microsoft Teams oferece suporte ao sistema de telefonia com planos de chamadas do Microsoft 365 ou roteamento direto. Com o roteamento direto, você pode conectar seu próprio controlador de borda de sessão suportado ao sistema de telefonia Microsoft diretamente sem nenhum software local adicional.

Há suporte para filas de chamadas, transferência, encaminhamento, espera, silenciar e retomar uma chamada.

## **DTMF**

O recurso de tons duplos de multifrequência (DTMF) são compatíveis com estas versões do aplicativo Citrix Workspace (ou posterior):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para ChromeOS versão 2111.1

## **Suporte para e911 dinâmico**

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado no Microsoft Calling Plans, Operator Connect e Direct Routing, ele permite a você:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace em execução no ponto de extremidade, em vez do cliente Microsoft Teams em execução no VDA.

A lei de Ray Baum exige que o local despachável do chamador de 911 seja transmitido para o Ponto de Atendimento Público Seguro (PSAP) apropriado. O Microsoft Teams Optimization with HDX está em conformidade com a lei de Ray Baum quando usado com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posteriores
- Aplicativo Citrix Workspace para Linux versão 2112 e posteriores
- Aplicativo Citrix Workspace para Mac versão 2112 e posteriores
- Aplicativo Citrix Workspace para ChromeOS versão 2112 e posteriores

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de localização de rede ou emergência:

- Configurações de rede
- Serviço de Informações de Local (LIS)

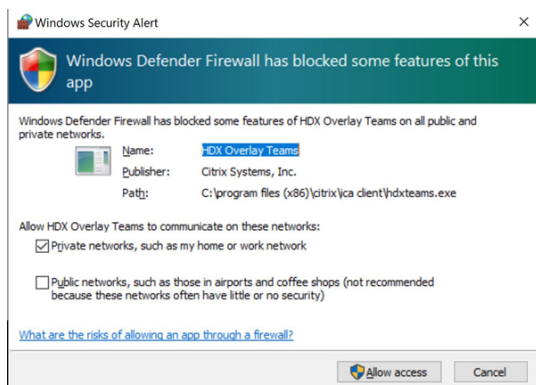
Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a [documentação da Microsoft](#).

As informações de local despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

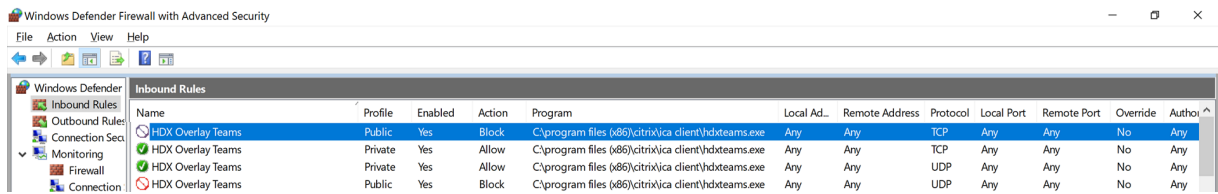
- ID do chassi/ID da porta usando o Link Layer Discovery Protocol (LLDP) para conexões Ethernet/Switch. O Ethernet/Switch (LLDP) é suportado em:
  - Versões 8.1 e 10 do Windows
  - macOS, que requer software de ativação LLDP Para baixar o software de ativação LLDP, acesse [www.microsoft.com](http://www.microsoft.com) e pesquise o software de ativação LLDP.
  - Linux, que exige que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do cliente fino.
- WLAN BSSID e {IPv4-IPv6; Sub-rede; Endereço MAC} do ponto de extremidade em que o aplicativo Citrix Workspace está instalado.
  - Locais baseados em sub-rede e WiFi são compatíveis com o aplicativo Workspace para Windows, Linux e Mac.
- Latitude e Longitude, se a permissão do usuário for concedida no nível do sistema operacional em que o aplicativo Citrix Workspace está instalado (a permissão é definida como HDX RTC Engine)
  - Compatível com todas as plataformas de aplicativos do Workspace. No entanto, no caso do Citrix Workspace para Linux, você deve incluir a biblioteca [libgps](#) na distribuição do SO do cliente fino (>sudo apt-get install libgps23 gpsd lldpd).

## Considerações sobre o firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso com as configurações de **firewall do Windows**. O aviso pede aos usuários para permitir a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Firewall do Windows Defender > Segurança Avançada**. Você pode aplicar regras mais restritivas, se desejar.



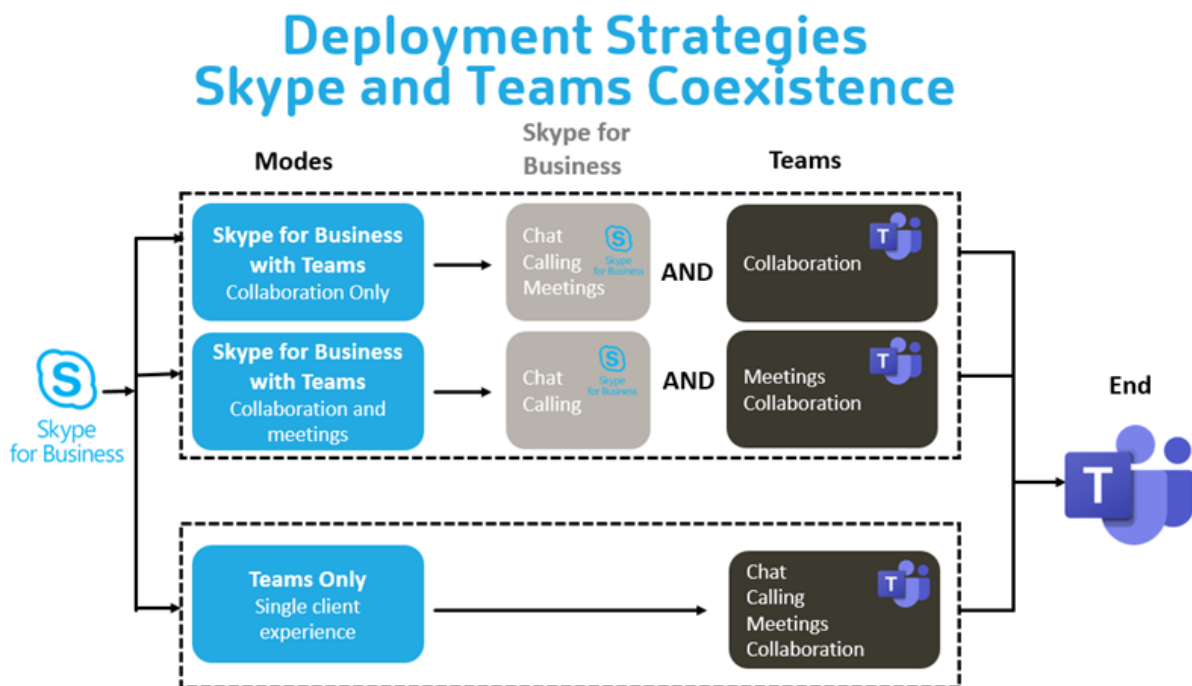
## Coexistência do Microsoft Teams e Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado, como duas soluções separadas com recursos sobrepostos.

Para obter mais informações, consulte [Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business](#).

O Citrix RealTime Optimization Pack e a otimização HDX para os mecanismos multimídia do Microsoft Teams, em seguida, honram o conjunto de configurações Alguns exemplos são modos de ilha e colaboração do Skype for Business com o Microsoft Teams. Além disso, colaboração e reuniões do Skype for Business com Microsoft Teams.

O acesso periférico só pode ser concedido a um único aplicativo no momento. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



## **Citrix SD-WAN: conectividade de rede otimizada para Microsoft Teams**

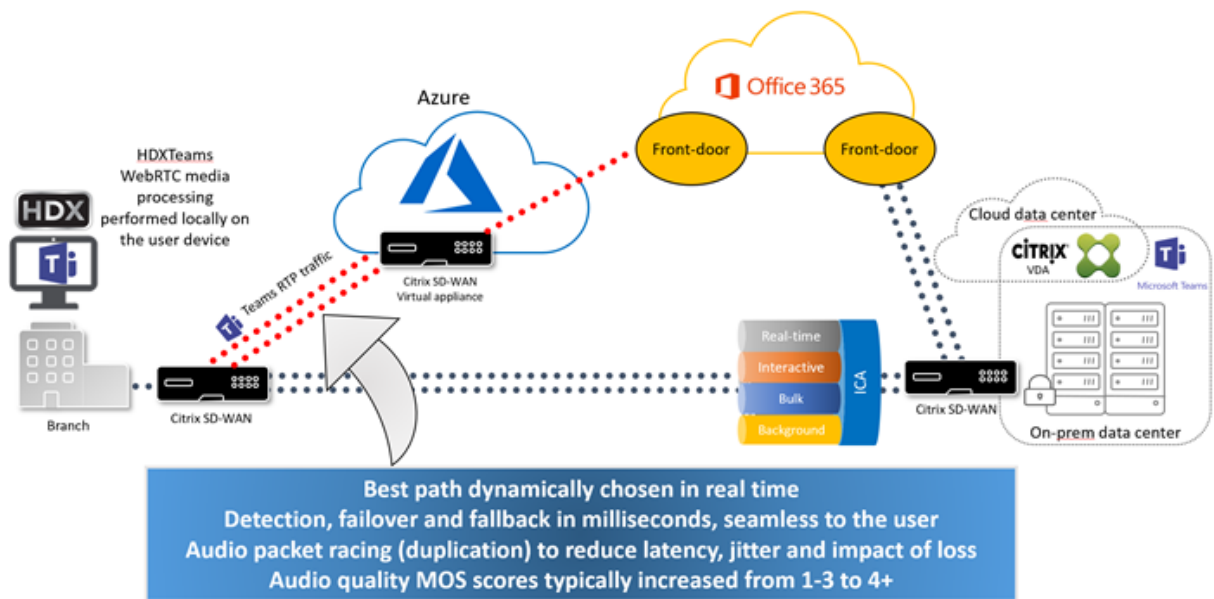
A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio-vídeo do Microsoft Teams dos usuários do aplicativo Citrix Workspace em locais de filiais para um data center antes de ir à Internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço Web do Microsoft 365 baseados em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

As conexões de internet de banda larga de negócios em muitas áreas sofrem de perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio-vídeo do Microsoft Teams quando a integridade da rede é variável ou está degradada.

- Se você usar o Microsoft Azure, um Appliance Virtual (VPX) Citrix SD-WAN implantado no Azure VNET fornece otimizações avançadas de conectividade. Essas otimizações incluem failover de link integrado e corridas de pacotes de áudio.
- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud Direct. Este serviço fornece entrega confiável e segura para todo o tráfego direcionado à Internet.

Se a qualidade da conexão com a Internet da filial não for uma preocupação, pode ser suficiente para minimizar a latência. Desvie o tráfego do Microsoft Teams diretamente do dispositivo de filial Citrix SD-WAN para a porta da frente do Microsoft 365 mais próxima para minimizar a latência. Para obter mais informações, consulte [Otimização do Citrix SD-WAN Office 365](#).



## Reuniões e bate-papo com várias janelas

Você pode usar várias janelas de reuniões ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte [Microsoft Teams Pop-Out Windows for Chats and Meetings](#) no site do Microsoft 365.

### Nota:

Esse recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Ele requer VDA 2112 ou superior e foi retroportado para 1912 CU6+ LTSR.

## Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 suporta desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas ajudando a conversa a manter o foco na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas em conferência ou P2P.

### Nota:

Esse recurso está integrado à interface do usuário/botões do Microsoft Teams. O suporte a Mul-

tiWindow é um pré-requisito que requer uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte [Reuniões e bate-papo com várias janelas](#).

Os controles de interface do usuário do Microsoft Teams de desfoque e efeitos de fundo exigem as seguintes versões mínimas:

- Aplicativo Citrix Workspace para Windows 2207
- Aplicativo Citrix Workspace para Mac 2301
- Aplicativo Citrix Workspace para Linux 2307
- Aplicativo Citrix Workspace para ChromeOS 2303

#### **Limitações:**

- O cliente deve estar conectado à Internet durante a substituição da imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição da imagem de fundo definida pelo administrador e pelo usuário não é compatível com a interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser definidas usando parâmetros de configuração no cliente, se a imagem também estiver armazenada no cliente.

#### **Configurar uma imagem de fundo personalizada**

As chaves de registro a seguir só são necessárias se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso ou se um administrador quiser substituir os comportamentos padrão. Por exemplo, desativar o desfoque da tela de fundo porque o ponto de extremidade não é poderoso o suficiente.

**No Windows** Para definir uma imagem de fundo personalizada, os administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou ponto de extremidade:

Localização: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição da imagem de fundo)

Um valor definido como 1 desfoca o fundo. O usuário final ou o administrador podem definir esse valor.

O valor definido como 2 também requer que a chave **VideoBackgroundImage** esteja presente também. Somente o administrador pode definir esse valor. A seguinte chave é necessária somente se você quiser substituir a imagem de fundo, não para desfocar:

- Nome: VideoBackgroundImage
- Tipo: REG\_SZ
- Valor: my\_image\_name.jpeg

A imagem de fundo do vídeo deve estar presente no diretório `C:\Program Files (x86)\Citrix\ICA Client`.

Essa configuração do registro também pode ser usada para habilitar o desfoque em segundo plano ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de interface do usuário do Microsoft Teams. Em outras palavras, se o seu ambiente ou VDA não suportar várias janelas, você ainda poderá aplicar a solução alternativa do registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações da chave do Registro só entram em vigor quando a sessão HDX se conecta.

**No Mac** Localização da imagem baixada pelo usuário: `/Users/username/Downloads/any_image.png`

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

**No Linux** Localização da imagem baixada pelo usuário: `/home/username/Downloads/any_image.jpg`

Crie o arquivo `/var/.config/citrix/hdx_rtc_engine/config.json` e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,

```
1 {
2
3
4 "VideoBackgroundEffect":2,
5
6 "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
7
8 }
```

## Em HTML5

1. Navegue até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
1 'features' : {
2
```



```
3     'msTeamsOptimization' :  
4     {  
5  
6         'backgroundEffects' : true  
7     }  
8  
9 }
```

3. Salve as alterações.

### Considerações sobre o consumo de CPU cliente

Embora o recurso de desfoque seja econômico em termos de uso de CPU, você pode esperar um aumento no consumo. Por exemplo, em um cliente fino com um chip Intel® Pentium® Silver de 4 núcleos e 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

### Exibição de galeria e alto-falantes ativos no Microsoft Teams

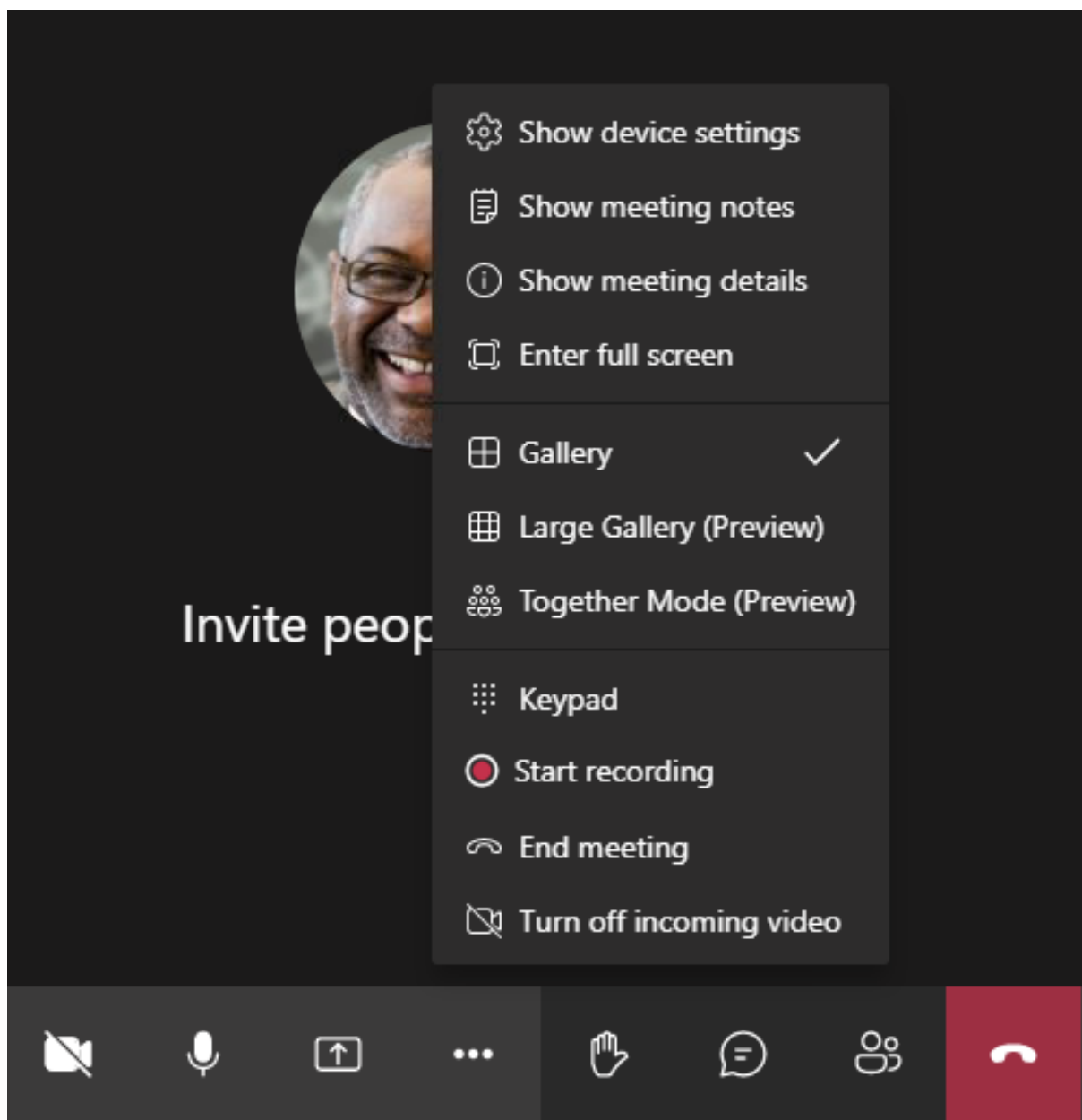
O Microsoft Teams oferece suporte a layouts de **Gallery**, **Large gallery** e **Together mode**.

O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecidos como **Gallery**). Nesse caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham um vídeo, apenas os últimos quatro alto-falantes mais ativos aparecem na tela.

O Microsoft Teams também fornece a grande visualização da galeria com uma grade de até 7x7. Como resultado, o servidor de conferência Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Esse feed único, em estilo de matriz, também pode incluir os vídeos de pré-visualização automática dos usuários.

Por fim, o Microsoft Teams suporta o **Together mode**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para colocar digitalmente os participantes em um histórico compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada em conferência selecionando layouts de **Gallery**, **Large gallery** ou **Together mode** no menu de reticências.



Suporte para restrições de proporção de vídeo (aplicativo Citrix Workspace para Windows 2102, aplicativo Citrix Workspace para Linux 2106, aplicativo Citrix Workspace para MAC 2106 e posterior):

- A opção **Preencher a moldura** está disponível em Gallery/Large Gallery View. Essa opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts Gallery e Large Gallery:

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Layout/Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro últimos palestrantes mais ativos aparecem na tela e os outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.
Técnica mista	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central combina e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Esta ação introduz um pouco de latência adicional.
Alto-falante ativo	O novo alto-falante ativo substitui o alto-falante menos ativo na grade.	Exibe todos os participantes, independentemente de estarem ativos ou inativos.
Codificação no ponto de extremidade	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no ponto de extremidade	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no ponto de extremidade pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo de áudio e vídeo. Isso reduz o consumo de CPU no ponto de extremidade.

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo poderá ser maior.	720p para o layout composto ou misto. Não há necessidade de um stream de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente reduz a resolução ou a taxa de bits de upload.
Problema de “usuário lento”	O remetente modifica a qualidade de cada modalidade (áudio/vídeo/compartilhamento de tela) para a menor qualidade de rede comum entre os participantes. Esse fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com más condições de rede afeta a qualidade de todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência fornece qualidades diferentes com base nas condições de rede de participantes individuais.
Autovisualização	Mostra você em uma pequena miniatura em tempo real.	Mostra você em uma miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout do vídeo principal com algum atraso adicional.

## Compartilhamento de tela no Microsoft Teams

O Microsoft Teams conta com o compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho que está sendo compartilhada com codecs de vídeo como o H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do aplicativo Citrix Workspace 2109 ou superior, para Windows, Linux e Mac, e do aplicativo Citrix Workspace 2303, para ChromeOS, os usuários podem compartilhar suas telas e câmeras de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera é pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O par deve então retomar manualmente o compartilhamento da câmera.

#### **Nota sobre o PowerPoint Live**

Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros colegas ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para ver outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar uma apresentação de slides do PowerPoint Live, clique no botão da “Bandeja de compartilhamento” e selecione um dos slides sugeridos do PowerPoint, ou clique em “Procurar” e localize um arquivo do PowerPoint no seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Aplicativos locais sobrepostos ao Desktop Viewer não são capturados.

#### **Nota**

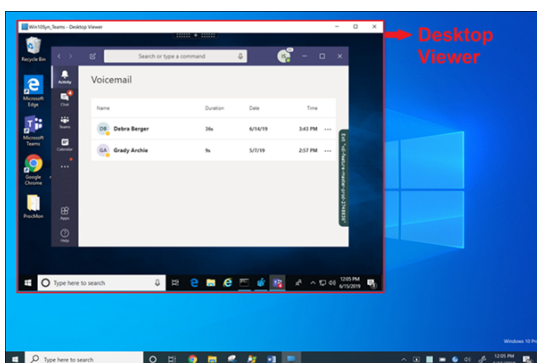
Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte [Requisitos do sistema](#).

#### **Limitação conhecida:**

- Se o Desktop Viewer estiver desativado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desativado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela com vários monitores.
- Nas versões do aplicativo Workspace anteriores à 2106, somente o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor primário para que os outros pares na chamada possam vê-lo.
- O compartilhamento de tela com vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout do monitor virtual (partição lógica de um único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.
- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento só

é possível se o aplicativo local está sobreposto no Desktop Viewer. Esse comportamento foi removido na versão 2009.6 ou posterior, e 1912 CU5 ou posterior.

- Durante o compartilhamento de tela, se você mudar do modo de janela para tela cheia, o compartilhamento de tela é interrompido. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.
- 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 a partir de um aplicativo integrado:**

Se você estiver publicando o Microsoft Teams como um aplicativo integrado independente, o compartilhamento de tela capturará a área de trabalho local do seu ponto de extremidade físico. É necessário o aplicativo Citrix Workspace versão mínima 1909.

### **Compartilhamento de aplicativos**

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

Começando com o aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Você também pode compartilhar aplicativos internos personalizados, como Java, usando o Microsoft Teams otimizado. Para compartilhar um aplicativo específico:

1. Navegue até o aplicativo Microsoft Teams em sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo que você selecionou e os colegas na chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desativar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`:

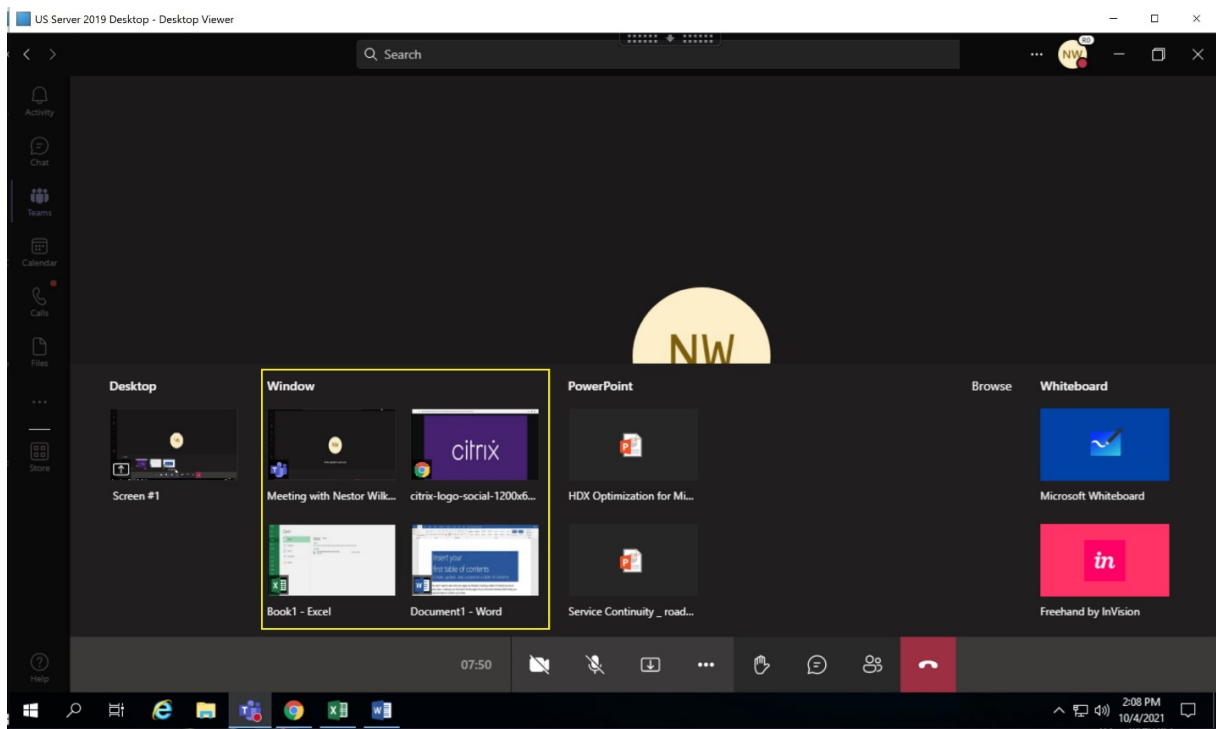
Nome: `UseWsProvider`

Tipo: `DWORD`

Valor: `0`

### Nota:

- Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
- O compartilhamento de tela depende da captura do lado do VDA da janela. O conteúdo é retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para o servidor de conferência ou um par no mesmo nível.



### Limitações conhecidas com o compartilhamento de tela de um aplicativo específico:

- O ponteiro do mouse não fica visível quando você está compartilhando a tela de um aplicativo.
- Se você minimizar um aplicativo ao compartilhá-lo, somente o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até você maximizar o aplicativo.
- Os aplicativos LAA (acesso a aplicativos locais) mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de área de trabalho no Microsoft Teams otimizado no VDA. No entanto, quando você seleciona o aplicativo na lista, o resultado pode não ser o esperado.

### Compatibilidade com o App Protection

O compartilhamento de tela de um aplicativo específico é compatível com o recurso App Protection no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico, se tiver iniciado o aplicativo ou a área de trabalho a partir de um grupo de entrega que tenha o App Protection ativado.

Quando você clica em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Área de trabalho**. Você só pode selecionar a opção **Janela** para compartilhar um aplicativo aberto.

#### Nota:

Quando você inicia aplicativos ou áreas de trabalho de um grupo de entrega com o App Protection ativado, não é possível ver o vídeo recebido ou o compartilhamento de tela 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 posteriores

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de obter o controle, você pode fazer seleções, edições ou outras atividades usando o teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela está sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar a sua solicitação.

Enquanto você tem controle, você pode fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar um teclado e um mouse. Quando terminar, clique em **Solicitar controle**.

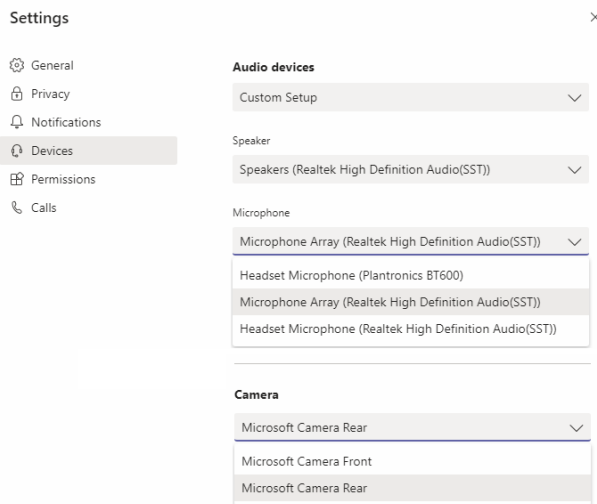
#### Limitações:

- Conceder e solicitar controle não estarão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como compartilhamento de aplicativo). A área de trabalho ou o monitor completo devem ser compartilhados.
- O recurso para fixar a barra de controle em um local específico não está disponível.



## Periféricos no Microsoft Teams

Quando a otimização do Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fone de ouvidos, microfones, câmeras, alto-falantes e assim por diante). Em seguida, os periféricos são listados devidamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele usa o mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações > Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão a partir do mesmo ponto de extremidade.

### Recomendações:

- Headsets certificados pelo Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde o microfone e o alto-falante estão em dispositivos separados, pode haver um eco. Um exemplo disso é uma webcam com um microfone embutido e um monitor com alto-falantes. Ao usar alto-falantes externos, coloque-os o mais longe possível do microfone. Além disso, coloque-os longe de qualquer superfície que possa refratar o som para o microfone. Para obter mais informações, acesse [www.microsoft.com](http://www.microsoft.com) e pesquise fones de ouvido certificados pelo Microsoft Teams.
- Câmeras certificadas pelo Microsoft Teams, embora os periféricos certificados pelo Skype for Business sejam compatíveis com o Microsoft Teams. Para obter mais informações, acesse e pesquise câmeras certificadas pelo Microsoft Teams e periféricos certificados pelo Skype for

Business.

- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento de CPU com webcams que executam codificação H.264 integrada - UVC 1.1 e 1.5.

**Nota:**

O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio com 24 bits ou com frequências acima de 96 kHz.

O HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou mais antigo) suporta apenas esses formatos de dispositivo de áudio específicos (canais, profundidade de bits e taxa de amostragem):

- Dispositivos de reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
- Dispositivos de gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz

Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.

**Webrpc** apresenta logs em **HdxTeams.exe** que mostram este tipo de informação:

```
Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing  
...
```

```
Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't  
create audio module!
```

Como solução alternativa, desative o dispositivo específico ou:

1. Abra o **Painel de controle de som** (mmsys.cpl).
2. Selecione o dispositivo de reprodução ou gravação.
3. Vá para **Propriedades > Avançado** e altere as configurações para um modo suportado.

## Modo de fallback

Se o Microsoft Teams não carregar no modo VDI otimizado (“Citrix HDX não conectado” em Microsoft Teams>About/Version), o VDA retornará às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento da webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando um sistema operacional de versão/plataforma do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não serão aplicadas.

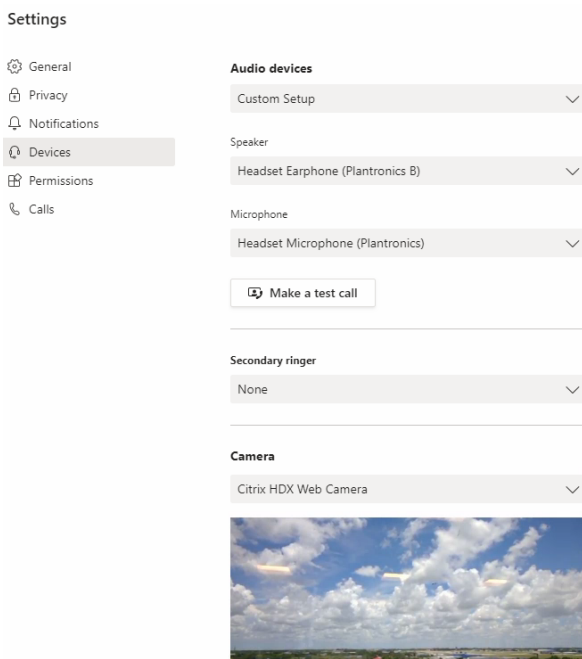
No modo de reserva, os periféricos são traçados ao VDA. Os periféricos aparecem no aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no

VDA. Para obter mais informações, consulte [Modo de fallback do Microsoft Teams](#) na lista de recursos gerenciados pelo registro.

Esse recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior.

Para determinar se você está no modo otimizado ou não otimizado ao observar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX herdadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX** como mostrado no gráfico a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) quando comparados com o modo otimizado.



Quando são usadas as tecnologias HDX herdadas, o Microsoft Teams não descarrega o processamento de compartilhamento de áudio, vídeo e tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do ponto de extremidade. Em vez disso, as tecnologias HDX usam renderização no lado do servidor. Espere alto consumo de CPU no VDA quando você liga o vídeo. O desempenho de áudio em tempo real pode não ser otimizado.

## Limitações conhecidas

### Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e terminar chamadas não têm suporte. Aumentar e diminuir volume têm suporte.

- As configurações de QoS no Admin Center for Microsoft Teams não se aplicam a usuários de VDI.
- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.

#### Limitação no VDA:

- Quando você configura a configuração de **DPI alto do aplicativo Citrix Workspace** como **Yes**, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum valor acima de 100%.

#### Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume no computador cliente, não no VDA.

## Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams em Windows e Mac. Para Linux, consulte seu fornecedor de cliente fino.

Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes terminais são aprimoradas com a adaptação à resolução adequada para a melhor experiência de chamada para todos os chamadores.

Com essa experiência aprimorada, cada usuário pode enviar vários fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p e assim por diante), dependendo de vários fatores, incluindo capacidade do ponto de extremidade, condições da rede e outros. Depois, o ponto de extremidade receptor solicita a resolução de qualidade máxima que pode suportar, proporcionando a todos os usuários a melhor experiência de vídeo.

#### Nota:

Esse recurso está disponível somente após o lançamento da atualização do Microsoft Teams. Para obter informações sobre o ETA, acesse <https://www.microsoft.com/> e pesquise o roadmap do Microsoft 365. Quando a atualização for lançada pela Microsoft, você poderá verificar o [CTX253754](#) para obter a atualização da documentação e o anúncio.

## Limitação da Microsoft

- Uma visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams —entre em contato com a Microsoft para saber para quando esperar a grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.

- A resolução máxima de fluxo de vídeo de entrada e saída é de 720p.
- O toque de retorno de chamada PSTN não é suportado
- O desvio de mídia para roteamento direto não tem suporte.
- As funções de produtor e apresentador de eventos de transmissão e ao vivo não têm suporte. A função de participante tem suporte, mas não é otimizada (renderiza no VDA).
- A função de aumentar zoom e diminuir zoom no Microsoft Teams não é suportada.
- Não há suporte para roteamento baseado na localização e bypass de mídia.
- A mesclagem de chamadas não é suportada (opção não exibida na interface do usuário).

### Limitação da Citrix e Microsoft

- Ao fazer o compartilhamento de tela, a opção **incluir áudio do sistema** não está disponível.
- O Simulcast não é compatível com o ChromeOS.

### Fim da vida útil (EOL) da janela única do Microsoft Teams

Em 31 de janeiro de 2024, a Microsoft retirará o suporte do Microsoft Teams para interface de usuário de janela única ao usar a otimização de VDI do Microsoft Teams e oferecerá suporte somente à experiência de várias janelas. A Microsoft notificou sobre essa descontinuação em 8/9/2023 no Centro de Administração do M365 (ID da publicação: MC674419).

Detalhes públicos sobre o recurso de várias janelas podem ser encontrados no artigo da Tech Community: [New Meeting and Calling Experience in Microsoft Teams](#).

#### Nota:

A Citrix recomenda que você atualize seu VDA e o aplicativo Citrix Workspace para as versões com suporte para continuar usando o Microsoft Teams no modo otimizado para compartilhamento de vídeo e tela. Se você não atualizar sua infraestrutura e seus endpoints para oferecer suporte a várias janelas, suas chamadas, videochamadas e compartilhamento de tela não serão otimizados. Isso pode resultar em problemas de qualidade da chamada, aumento da latência e aumento da carga no servidor.

A tabela a seguir ilustra as versões mínimas, LTSR e recomendadas do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams no Citrix VDI:

Componente	Versão mínima (1)	Versão compatível com LTSR (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+

Componente	Versão mínima (1)	Versão compatível com LTSR (2)	Versão recomendada (3)
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: essa é a versão em que a opção Várias janelas foi introduzida pela primeira vez. Algumas versões mínimas listadas aqui podem estar em fim de vida útil.
2. Versão compatível com LTSR: essa é a versão LTSR com suporte pela Citrix para várias janelas. As versões mais antigas dessas versões LTSR podem funcionar, mas o suporte não estará mais disponível para essas versões quando uma nova versão LTSR CU for lançada. Para obter mais informações sobre as políticas de suporte a 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: essa é a versão do software que a Citrix recomendará se o usuário/cliente optar por atualizar seu software. Todas essas são versões CR.
4. A versão 2203 LTSR para as versões base VDA e CWA inclui a funcionalidade de várias janelas. Essas versões foram substituídas pela CU mais recente, que é a versão oficialmente compatível. Os clientes podem continuar usando essas versões sem suporte a seu critério. A Citrix incentiva os clientes da versão LTSR a atualizarem para a CU mais recente.

**Anúncio de descontinuação do formato SDP (Plan B) do WebRTC**

A Citrix planeja descontinuar o suporte ao formato SDP (Plan B) do WebRTC atual em versões futuras. Você deve usar o Unified Plan no WebRTC para ter suporte às funcionalidades otimizadas do Microsoft Teams.

## Produtos afetados

Em uma das futuras versões do aplicativo Citrix Workspace, chamadas entre pontos de extremidade com a próxima versão do aplicativo Citrix Workspace e pontos de extremidade com o aplicativo Citrix Workspace 2108 ou versões anteriores não serão suportadas. Essa incompatibilidade de chamadas inclui clientes do aplicativo Citrix Workspace (CWA) 1912 LTSR. Os seguintes clientes do CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

## Substituição do Plan B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior à 2109, deverá atualizar para uma versão compatível (de preferência a versão CR mais recente). Caso contrário, chamadas com uma versão futura ou com pontos de extremidade mais recentes apresentarão falha na conexão. As chamadas entre versões futuras e seus parceiros de comunicação federados também podem não ser concluídas se o parceiro federado não tiver atualizado o seu Citrix Workspace.

O aplicativo Citrix Workspace encerrou a data de suporte à versão 2108 em março de 2023, devendo ser atualizado para uma versão mais recente. Para obter mais informações, consulte [Workspace App](#) para obter detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plan B, consulte a documentação do [WebRTC](#).

## Informações adicionais

- [Monitoramento, resolução de problemas e suporte ao Microsoft Teams](#)
- [Implantar o Microsoft Teams da área de trabalho na VM](#)
- [Instalar o Microsoft Teams usando o MSI \(seção Instalação da VDI\)](#)
- [Clientes finos](#)
- [Ferramenta de avaliação de rede do Skype for Business](#)
- [Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.](#)

## Tempo limite de sessão dinâmica

November 5, 2024

Esse recurso permite configurar tempos limite de sessão desconectada e ociosa para os horários de uso de pico e fora de pico para obter um esvaziamento mais rápido da máquina e economia de custos. Este recurso se aplica a:

- Máquinas com SO de sessão única e multissessão.
- Todas as máquinas no Grupo de Entrega, independentemente de estarem marcadas para dimensionamento automático.

Um VDA relata tempos ociosos para sessões que ficaram ociosas por mais de 10 minutos, portanto, tempos limite de sessão dinâmicos não conseguem desconectar sessões ociosas dentro de 10 minutos de ociosidade. Um valor menor remove as sessões prolongadas mais cedo, reduzindo assim os custos.



## Manage Autoscale

CYAZinfo1027

Enabled

×

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Force User Logoff

Autoscaling Tagged Machines

### Dynamic Session Timeout

Configure dynamic timeouts for your peak and off-peak usage times to achieve faster VM draining and cost savings. Larger values can improve user experience and smaller values can achieve faster draining. [Learn more](#)

	During peak times	During off-peak times
Idle session timeout: <span style="font-size: 14px;">?</span>	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block;">Disable ▾</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block; margin-left: 5px;">min ▾</div>	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block;">3 ▾</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block; margin-left: 5px;">min ▾</div>
Disconnected session timeout: <span style="font-size: 14px;">?</span>	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block;">4 ▾</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block; margin-left: 5px;">min ▾</div>	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block;">5 ▾</div> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; display: inline-block; margin-left: 5px;">min ▾</div>

⚠ Autoscale dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Studio policies. When a conflict occurs, the shorter timeout prevails. ↗

Save

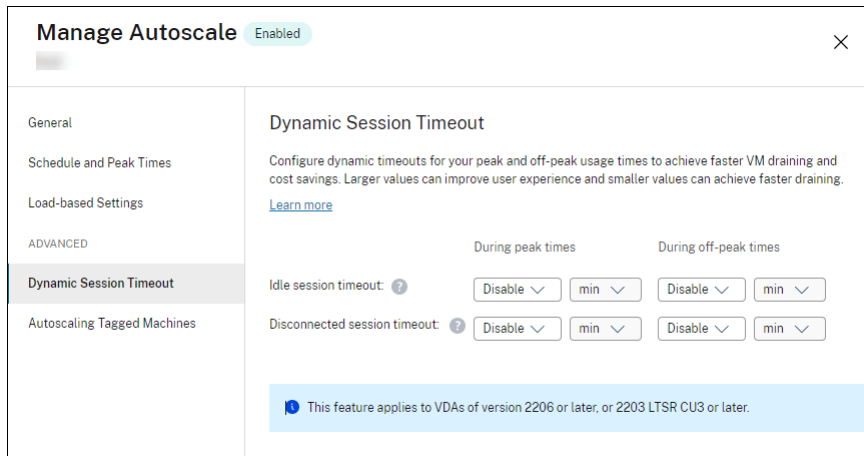
Apply

Cancel

↶

**Observação:**

- Esse recurso está sempre disponível para grupos de entrega com SO multissessão.
- Para grupos de entrega de SO de sessão única, esse recurso se aplica aos VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Certifique-se de que os VDAs tenham se registrado no Citrix Cloud pelo menos uma vez. Quando não estiver disponível, a seguinte interface de usuário é exibida:



- Os tempos limite dinâmicos de AutoScale são para economia de custos. Se usado para fins de segurança, os tempos limite configurados podem entrar em conflito com seu objeto de política de grupo ou com as políticas do console Manage. Quando ocorre um conflito, o tempo limite mais curto prevalece.

**Tempo limite de sessão ociosa.** Habilita ou desabilita um timer que especifica por quanto tempo uma conexão de usuário ininterrupta é mantida se não houver atividade pelo usuário. Quando o temporizador expira, a sessão é colocada no estado desconectado e o tempo limite de sessão desconectada **\*\* é aplicado. Se o \*\*Tempo limite de sessão desconectada** estiver desabilitado, a sessão não será desconectada.

**Importante:**

- Se você especificar um valor menor ou igual a 10 minutos (600 segundos), AutoScale desconectará as sessões relevantes depois que elas estiverem ociosas por 10 minutos. Isso ocorre porque o AutoScale depende dos tempos ociosos da sessão relatados pelos VDAs. Os VDAs relatam tempos ociosos somente para sessões que ficaram ociosas por mais de 10 minutos.
- Uma sessão ociosa ainda pode ser colocada em um estado desconectado se o usuário interagir com ela nos últimos 5 minutos após atingir o tempo limite da sessão ociosa.

**Tempo limite de sessão desconectada.** Ativa ou desativa um timer que especifica por quanto tempo uma área de trabalho desconectada permanece bloqueada antes que a sessão seja desconectada. Se ativado, a sessão desconectada é desconectada quando o timer expira.

## Perguntas frequentes

### **O recurso de tempo limite de sessão dinâmico se aplica somente a máquinas marcadas para dimensionamento automático?**

O recurso de tempo limite de sessão dinâmico se aplica a todas as máquinas no grupo de entrega, independentemente de estarem marcadas para dimensionamento automático.

### **Quando uma sessão é desconectada devido ao tempo limite dinâmico da sessão, as máquinas não marcadas também são incluídas no destino de dimensionamento automático das máquinas marcadas?**

O recurso de tempo limite de sessão dinâmico não está relacionado ao recurso de marcação de dimensionamento automático. Se os tempos limite de sessão dinâmicos resultarem no encerramento das sessões, as máquinas não marcadas também poderão ser desligadas durante o processo, desde que as máquinas estejam drenando até serem desligadas.

## Configurações

September 11, 2024

### **Nota:**

Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente 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 essas configurações:

- Gerenciar a autenticação
- [Citrix Customer Experience Improvement Program](#)
- [Remover Delivery Controllers](#)
- [Alterar o banco de dados de log](#)
- Definir data e hora
- Centralizar o gerenciamento do site
- [Habilitar a atribuição automática de vários usuários para o acesso ao PC remoto](#)

- Habilitar a resolução de DNS
- [Habilitar a confiança em XML](#)
- [Gerenciar chave de segurança](#)
- Definir o tempo limite de inatividade do console do Studio

## Gerenciar a autenticação

Por padrão, os usuários fazem logon no Web Studio usando o nome de usuário e a senha do domínio. Você também pode escolher um método de autenticação diferente para os usuários, como a autenticação de cartão inteligente ou a autenticação integrada do Windows.

Para escolher um método de autenticação para usuários, siga estas etapas:

1. Entre 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 estiverem instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, habilite Permitir acesso entre origens e adicione o URL do servidor do Web Studio à lista de permissões.

### Importante

A autenticação integrada do Windows não funciona quando o Web Studio está configurado como proxy para Delivery Controllers.

- Autenticação de cartão inteligente.
- Credenciais de domínio ou autenticação de cartão inteligente

Ativar a autenticação de cartão inteligente requer configuração adicional. Para obter mais informações, consulte [Configurar a autenticação de cartão inteligente para o Web Studio](#). Depois de habilitar a opção de **autenticação integrada do Windows**, na próxima vez que seus usuários fizerem logon, eles entrarão automaticamente. Como usuário, se você não conseguir entrar automaticamente, siga estas etapas para configurar seu navegador da Web para permitir a autenticação integrada do Windows.

Para Google Chrome:

1. No Painel de controle, selecione Opções da Internet.
2. Selecione a guia **Avançado**.
3. Selecione **Ativar autenticação integrada do Windows**.
4. Selecione a guia **Segurança**.
5. Selecione **Intranet local > Sites > Avançado**.
6. Na caixa **Add this website to the zone**:
  - Se o Web Studio e o Delivery Controller residem no mesmo servidor, digite a 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 URL.
2. Na caixa **Pesquisar**, digite `network negotiate`.
3. Clique com o botão direito do mouse em **network.negotiate-auth.trusted-uris** e selecione **Modificar**.
4. Na caixa **Enter string value**:
  - Se o Web Studio e o Delivery Controller residem no mesmo servidor, adicione uma lista separada por vírgulas de URLs e/ou aliases referenciando o nome do servidor que hospeda o Web Studio.
  - Caso contrário, adicione as 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 **Windows integrated sign-in** na página de login para tentar novamente.

Quando o Web Studio e o Delivery Controller estão instalados em máquinas diferentes, para que a autenticação integrada do Windows funcione, você precisa habilitar **Allow cross-origin access**.

Siga estas etapas para ativar a opção **Allow cross-origin access**:

1. Marque a caixa de seleção **Allow cross-origin access**.
2. Adicione a URL do servidor do Web Studio à lista de permissão.
3. No campo **Enter URL**, insira a URL. Clique em **Add** para adicionar mais, se necessário.

#### Nota

- A URL deve seguir o formato correto: <scheme>://<hostname>. Certifique-se de que não inclua caminhos ou barras à direita.
- Endereços IP e FQDNS são suportados. Ao adicionar uma URL, confirme que ela corresponde à forma como você acessa o Web Studio. Por exemplo, se estiver acessando o Web Studio usando um endereço IP, adicione a URL baseada no endereço IP à lista.
- Se você usar uma porta não padrão, não se esqueça de incluir o número da porta.

4. Clique em **Add** 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 de acordo com suas preferências, siga estas etapas:

1. Entre no Web Studio e selecione **Settings** no painel esquerdo.
2. Localize o bloco **Date and time** e clique em **Edit** para configurar as seguintes opções:
  - **Time format:**
    - Selecione para exibir a hora usando um relógio de 12 horas (9h da noite, por exemplo) ou um relógio de 24 horas (21h, por exemplo).
  - **Date format:**
    - Configure o formato de data para corresponder às suas preferências, por exemplo, aaaa/MM/dd.
  - **Time zone:**
    - **UTC:** exibe a data e a hora em UTC em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações no seu fuso horário local.
    - **Local time zone:** exiba a data e a hora no seu fuso horário local em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações em UTC.

#### Nota:

Essas configurações são específicas para cada conta de usuário.

## Habilitar a resolução de DNS

Para apresentar nomes de DNS em vez de endereços IP no arquivo ICA, siga estas etapas:

1. Entre no Web Studio e selecione **Settings** no painel esquerdo.
2. Ative a configuração **Enable DNS resolution**.

## Definir o tempo limite de inatividade do console do Studio

Você pode definir a duração da inatividade após a qual os administradores serão automaticamente desconectados do console do Studio.

1. Entre no Web Studio e selecione **Settings** no painel esquerdo.
2. Digite uma duração, que varia de 10 minutos a 24 horas.
3. Para aplicar essa configuração, atualize a página ou saia e entre novamente.

## Centralizar o gerenciamento do site

Esse 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](#).

## Implantação segura do Director

November 5, 2024

Este artigo destaca áreas que podem ter impacto na segurança do sistema ao implantar e configurar o Director.

## Configurar Serviços de Informações da Internet (IIS) da Microsoft

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 solicitação: 4.000.000.000

## Extensões de nome de arquivo

Você pode cancelar a permissão de extensões de nome de arquivo não listadas.

O Director requer estas extensões de nome de arquivo na Filtragem de Solicitações:

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

O Director requer os seguintes verbos HTTP na Filtragem de Solicitações. Você pode cancelar a permissão de 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 .NET global 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 **Log on as a service**



- Privilégios **Adjust memory quotas for a process**, **Generate security audits** e **Replace a process level token**

Os direitos e privilégios mencionados são um comportamento normal 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 IPsec (Internet Protocol security) ou HTTPS para proteger a passagem de dados 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 reprodução. Como o IPsec é um conjunto de protocolos de camada de rede, os protocolos de nível superior podem usá-lo sem modificação. O HTTPS usa os protocolos TLS (Transport Layer Security) para fornecer criptografia de dados forte.

### Observação:

- A Citrix recomenda que você restrinja o acesso ao console do Director na rede intranet.
- A Citrix recomenda que você não ative conexões não seguras ao Director em um ambiente de produção.
- Para a segurança das comunicações do Director, é necessária uma configuração para cada conexão separadamente.
- O protocolo SSL não é recomendado. Em vez disso, use o protocolo TLS mais seguro.
- Proteja suas comunicações com o Citrix ADC usando TLS, não IPsec.

Para proteger as comunicações entre servidores do Citrix Virtual Apps and Desktops e Director (para monitoramento e relatórios), consulte [Data Access Security](#).

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 [Secure the License Administration Console](#).

## Separação de segurança do Director

Você pode implantar qualquer aplicativo Web no mesmo domínio da Web (nome de domínio e porta) que o Director. No entanto, quaisquer riscos de segurança nesses aplicativos Web podem reduzir

potencialmente a segurança da sua implantação do Director. Quando um maior grau de separação de segurança é necessário, a Citrix recomenda que você implante o Director em um domínio da Web separado.

## Matriz de compatibilidade de recursos

November 5, 2024

O Citrix Director 7 2402 é compatível com:

- Citrix Virtual Apps and Desktops 7 2112 e posterior
- Citrix Virtual Apps and 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 estarão disponíveis. A Citrix recomenda que a versão do Director, Delivery Controller e VDAs seja a mesma.

### 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 **Upgrade Sequence** em [Atualizar uma implantação](#).

Na primeira vez que você fizer login após uma atualização do Director, é realizada a verificação de versão nos sites configurados. Se um site estiver executando uma versão do Controller anterior à do Director, o console Director exibe uma mensagem recomendando a atualização do site. Além disso, enquanto a versão do site for mais antiga do que a versão do Director, uma nota permanecerá no Dashboard do Director indicando a incompatibilidade.

### Observação:

Versões anteriores do Citrix Director não exibem políticas aplicadas a sessões de usuário em execução em versões recentes do VDA. O Citrix Director 1912 e versões anteriores não exibem políticas aplicadas a sessões de usuário em execução no VDA versões 2003 e posteriores. Use o Citrix Director versões 2003 e posteriores para ver essas políticas.

Os recursos específicos do Director com a versão mínima do Delivery Controller (DC), VDA e outros componentes dependentes necessários junto com a License Edition estão listados na tabela a seguir:

<b>Versão do Director</b>	<b>Recurso</b>	<b>Dependências – versão mínima necessária</b>	<b>Edição</b>
2311	<a href="#">Reproduza sessões ao vivo e gravadas</a>	VDA 2308 e DDC 2311	Todos
2311	<a href="#">Topologia da sessão</a>	None	Todos
2311	<a href="#">Resolução de tela ideal</a>	None	Todos
2311	<a href="#">Otimização do MS Teams</a>	VDA 2311 e DDC mais recentes	Todos
2311	<a href="#">Aprimoramentos da visão geral das sondas</a>	None	Todos
2311	<a href="#">Visualização renovada da duração do logon da sessão</a>	None	Todos
2308	<a href="#">Resumo e detalhamento das investigações</a>	None	Todos
2308	<a href="#">Suporte do Citrix Probe Agent para autenticação multifator do Citrix Gateway</a>	Citrix Gateway	Todos
2308	<a href="#">Desativar alertas do Hypervisor</a>	None	Todos
2308	<a href="#">Tendências das métricas de experiência de sessão</a>	None	Todos
2305	<a href="#">Suporte a autenticação via Citrix Gateway</a>	None	Todos
2305	<a href="#">Gerenciamento do AutoScale no Director</a>	None	Todos
2303	<a href="#">Alerta de máquinas com falha</a>	DC 7 2303	Premium
2203	<a href="#">Suporte a TLS 1.3</a>	-	Todos

<b>Versão do Director</b>	<b>Recurso</b>	<b>Dependências – versão mínima necessária</b>	<b>Edição</b>
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 habilitado	Todos
2212	Programação avançada de investigação	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 do início da sessão	DC 7 1906 e VDA 1903	Todos
1906	Investigação da área de trabalho	DC 7 1906 e Citrix Probe Agent 1903	Premium
7.9 e posterior	Duração do Citrix Profile Management no carregamento do perfil	VDA 1903	Todos
1811	Análise detalhada de perfil	DC 7 1811 e VDA 1811	Todos
1811	Monitoramento de alertas de hipervisor	DC 7 1811	Premium
1811	Investigação de aplicativo	DC 7 1811 e Citrix Application Probe Agent 1811	Premium
1811	Integridade da licença do Microsoft RDS	DC 7 1811 e VDA 7.16	Todos
1811	Exibição dos principais dados RTOP	DC 7 1811 e VDA 1808	Premium
1808	Exportação de dados de filtros	DC 7 1808	Todos

<b>Versão do Director</b>	<b>Recurso</b>	<b>Dependências – versão mínima necessária</b>	<b>Edição</b>
1808	<a href="#">Análise detalhada da sessão interativa</a>	DC 7 1808 e VDA 1808	Todos
1808	<a href="#">Análise detalhada de GPO</a>	DC 7 1808 e VDA 1808	Todos
1808	<a href="#">Dados históricos da máquina disponíveis usando a API OData</a>	DC 7 1808	Todos
7,18	<a href="#">Investigação de aplicativo</a>	DC 7.18	Premium (anteriormente Platinum)
7,18	<a href="#">Políticas de alertas inteligentes</a>	DC 7.18	Premium (anteriormente Platinum)
7,18	<a href="#">Link do Health Assistant</a>	None	Todos
7,18	<a href="#">Análise detalhada da sessão interativa</a>	None	Todos
7,17	<a href="#">Autenticação por cartão inteligente PIV</a>	None	Todos
7,16	<a href="#">Análise de aplicativos</a>	DC 7.16 e VDA 7.15	Todos
7,16	<a href="#">OData API V.4</a>	DC 7.16	Todos
7,16	<a href="#">Sombrear usuários Linux VDA</a>	VDA 7.16	Todos
7,16	<a href="#">Suporte a grupos locais de domínio</a>	None	Todos
7,16	<a href="#">Acesso ao console da máquina</a>	DC 7.16	Todos
7,15	<a href="#">Monitoramento de falhas de aplicativo</a>	DC 7.15 e VDA 7.15	Todos
7,14	<a href="#">Solução de problemas centrada no aplicativo</a>	DC 7.13 e VDA 7.13	Todos

<b>Versão do Director</b>	<b>Recurso</b>	<b>Dependências – versão mínima necessária</b>	<b>Edição</b>
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 de detalhes da sessão	DC 7.x e VDA 7.13	Todos
7,12	Descrições claras de falhas de máquina e conexão	DC 7.12 e VDA 7.x	Todos
7,12	Maior disponibilidade de dados históricos na edição Enterprise	DC 7.12 e VDA 7.x	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 ICA RTT	DC 7.11 e VDA 7.11	Premium (anteriormente Platinum)
7.11	Melhorias de exportação de relatórios	DC 7.11 e VDA 7.x	Todos
7.11	Integração com o Citrix ADM	DC 7.11, VDA 7.x e MAS versão 11.1 compilação 49.16	Premium (anteriormente Platinum)
7.9	Detalhamento da duração do logon	DC 7.9 e VDA 7.x	Todos
7.7	Monitoramento e alertas proativos	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)

<b>Versão do Director</b>	<b>Recurso</b>	<b>Dependências – versão mínima necessária</b>	<b>Edição</b>
7.7	<a href="#">Integração com autenticação do Windows</a>	DC 7.x e VDA 7.x	Todos
7.7	<a href="#">Uso de SO de sessão única e multissessão</a>	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)
7.6.300	<a href="#">Suporte para canal virtual Framehawk</a>	DC 7.6 e VDA 7.6	Todos
7.6.200	<a href="#">Integração de Session Recording</a>	DC 7.6 e VDA 7.x	Premium (anteriormente Platinum)
7	<a href="#">Integração com HDX Insight</a>	DC 7.6, VDA 7.x e Citrix ADM	Premium (anteriormente Platinum)

## Motivo de falhas e solução de problemas no Citrix Director

November 5, 2024

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 na conexão

Categoria	Motivo	Problema	Ação
N/A	[0] Unknown. Esse código de erro não está mapeado.	O Monitoring Service não pode determinar o motivo da falha de conexão ou inicialização relatada pelas informações compartilhadas pelo Broker Service.	Colete logs de CDF no Controller e entre em contato com o suporte Citrix.
[0] None	[1] None	None	N/A
[2] MachineFailure	[2] SessionPreparation	Solicitação de preparação da sessão do Delivery Controller para o VDA falhou. Possíveis causas: problemas de comunicação entre o Controller e o VDA, problemas enfrentados pelo Broker Service ao criar uma solicitação de preparação ou problemas de rede resultando na não aceitação da solicitação pelo VDA.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, <a href="#">Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops</a> , para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
[2] MachineFailure	[3] RegistrationTimeout	O VDA foi ligado, mas o tempo limite esgotou durante a tentativa de 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. Se interrompido, inicie cada um deles.



Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[4] ConnectionTimeout	O cliente não se conectou ao VDA depois que o VDA foi preparado para o início da sessão. A sessão foi intermediada com sucesso, mas o tempo limite esgotou enquanto aguardava o cliente se conectar ao VDA. Possíveis causas: configurações do firewall, interrupções de rede ou configurações que impedem conexões remotas.	Verifique o console Director para confirmar se o cliente tem uma conexão ativa atualmente, o que significa que nenhum usuário é afetado. Se não existir nenhuma sessão, revise os logs de eventos no cliente e no VDA em busca de erros. Resolva os problemas de conectividade de rede entre o cliente e o VDA.
[4] NoLicensesAvailable	[5] Licensing	A solicitação de licenciamento falhou. Possíveis causas: número insuficiente de licenças ou o servidor de licenças ficou inativo por mais de 30 dias.	Verifique se o servidor de licenças está online e acessível. Resolva os problemas de conectividade de rede com o servidor de licenças ou reinicialize o servidor de licenças se apresentar mau funcionamento. Verifique se há licenças suficientes no ambiente e aloque mais, se necessário.

Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[6] Ticketing	Ocorreu uma falha durante a emissão de tickets, indicando que a conexão do cliente com o VDA não corresponde à solicitação do agente. Um ticket de solicitação de inicialização é preparado pelo Broker e entregue no arquivo ICA. Quando o usuário tenta iniciar uma sessão, o VDA valida o ticket de inicialização no arquivo ICA com o Broker. Possíveis causas: o arquivo ICA está corrompido ou o usuário está tentando estabelecer uma conexão não autorizada.	Verifique se o usuário tem acesso ao aplicativo ou à área de trabalho com base nos grupos de usuários definidos nos grupos de entrega. Instrua o usuário a reiniciar o aplicativo ou a área de trabalho para determinar se o problema já se resolveu. 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 os problemas de registro.
[1] ClientConnection-Failure	[7] Other	Uma sessão foi relatada como encerrada a partir do VDA depois que o cliente entrou em contato com o VDA inicialmente, mas antes de concluir a sequência de conexão.	Verifique se a sessão não foi encerrada pelo usuário antes da inicialização. Tente reiniciar a sessão, se o problema persistir, colete registros de CDF e entre em contato com o suporte Citrix.

Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[8] GeneralFail	A sessão não foi iniciada. Possíveis causas: um início intermediado foi solicitado enquanto o agente ainda estava iniciando ou inicializando, ou erro interno durante a fase de intermediação de um início.	Verifique se o Citrix Broker Service está em execução e tente iniciar a sessão novamente.
[5] Configuration	[9] MaintenanceMode	O VDA, ou o grupo de entrega ao qual o VDA pertence, é 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.
[5] Configuration	[10] ApplicationDisabled	O aplicativo não pode ser acessado por usuários finais porque ele foi desativado pelo administrador.	Se o aplicativo tiver que estar disponível para uso em produção, habilite o aplicativo e instrua o usuário a se reconectar.
[4] NoLicensesAvailable	[11] LicenseFeatureRefused	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 da licença existente do Citrix Virtual Apps and Desktops.

Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[13] SessionLimitReached	Todos os VDAs estão em uso e não há capacidade de hospedar mais sessões. Causas possíveis: todos os VDAs estão em uso (para VDAs com SO de sessão única) ou todos os VDAs atingiram o máximo de sessões simultâneas configuradas permitidas (para VDAs com SO multissessão).	Verifique se há algum VDA no modo de manutenção. Desative o modo de manutenção se não for necessário para liberar mais capacidade. Considere aumentar o valor de <b>Maximum Number of Sessions</b> na configuração de política Citrix para permitir mais sessões por VDA de servidor. Considere adicionar mais VDAs com SO multissessão. Considere adicionar mais VDAs com SO de sessão única.
[5] Configuration	[14] DisallowedProtocol	Os protocolos ICA e RDP não são permitidos.	Execute o comando <b>Get-BrokerAccessPolicyRule</b> do PowerShell no Delivery Controller e verifique se o valor <b>AllowedProtocols</b> tem todos os protocolos desejados listados. Esse problema ocorre somente se houver uma configuração incorreta.

Categoria	Motivo	Problema	Ação
[5] Configuration	[15] ResourceUnavailable	O aplicativo ou a área de trabalho ao qual o usuário está tentando se conectar não está disponível. Esse aplicativo ou área de trabalho pode não existir, ou não há VDAs disponíveis para executá-lo. Possíveis causas: a publicação do aplicativo ou da área de trabalho foi cancelada, ou os VDAs que hospedam o aplicativo ou a área de trabalho atingiram a carga máxima, ou o aplicativo ou a área de trabalho está definida no modo de manutenção.	Verifique se o aplicativo ou a área de trabalho ainda está publicado e se os VDAs não estão no modo de manutenção. Determine se os VDAs com SO multissessão estão em carga total. Em caso afirmativo, provisione mais VDAs com SO multissessão. Verifique se há VDAs com SO de sessão única disponíveis para conexões. Provisione mais VDAs com SO de sessão única, se necessário.
[5] Configuration	[16] ActiveSessionReconnectDisabled	A sessão ICA está ativa e conectada a um ponto de extremidade diferente. No entanto, como <b>Active Session Reconnection</b> está desativada, o cliente não pode se conectar à sessão ativa.	No Delivery Controller, verifique se <b>Active Session Reconnection</b> está ativada. Verifique se o valor de <b>DisableActiveSessionReconnect</b> no registro sob <b>HKEY_LOCAL_MACHINE\Software</b> está definido como 0.
[2] MachineFailure	[17] NoSessionToReconnect	O cliente tentou se reconectar a uma sessão específica, mas a sessão foi encerrada.	Repita a reconexão do controle do espaço de trabalho.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[18] SpinUpFailed	O VDA não pode ser ligado a partir do início da sessão. Este é um problema relatado pelo hipervisor.	Se a máquina ainda estiver desligada, tente iniciar a máquina a partir do Citrix Studio. Se isso falhar, revise a conectividade e as permissões do hipervisor. 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 recebeu um Personal vDisk; faça login no hipervisor para redefinir a VM.
[2] MachineFailure	[19] Refused	O Delivery Controller 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 os problemas de roteamento de rede ou firewall.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[20] ConfigurationSet Failure	O Delivery Controller não enviou os dados de configuração necessários, como configurações de política e informações de sessão, para o VDA durante o início da sessão. Possíveis causas: problemas de comunicação entre o Controller e o VDA, problemas que o Broker Service ao criar uma solicitação de configuração ou problemas de rede resultando não aceitação da solicitação pelo VDA.	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	O número máximo de instâncias de um aplicativo foi atingido. Nenhuma instância adicional do aplicativo pode ser aberta no VDA. Esse problema está relacionado ao recurso de limites de aplicativos.	Considere aumentar a configuração do aplicativo, <b>Limit the number of instances running at the same time</b> , para um valor maior se o licenciamento permitir.

Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	O usuário está tentando abrir mais do que uma instância de um aplicativo, mas o aplicativo está configurado para permitir apenas uma única instância do aplicativo por usuário. Esse problema está relacionado ao recurso de limites de aplicativos.	Por padrão, apenas uma instância do aplicativo é permitida por usuário. Se forem necessárias várias instâncias por usuário, considere limpar a configuração de <b>Limit to one instance per user</b> na configuração do aplicativo.
[1] ClientConnection-Failure	[23] Communication error	O Delivery Controller tentou enviar informações para o VDA, como uma solicitação para se preparar para uma conexão, mas ocorreu um erro durante a tentativa de comunicação. Isso pode ser causado devido a interrupções na rede.	Se já iniciado, reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verificar se o VDA se registra com êxito. Confirme se os Delivery Controllers configurados para o VDA estão precisos por meio dos detalhes no log de eventos do aplicativo.



Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring Service converte [12] NoDesktopAvailable para esse código de erro.	O VDA atribuído para iniciar a sessão está em um estado inválido ou está indisponível. Possíveis causas: o estado de energia do VDA é desconhecido ou indisponível, o VDA não foi reinicializado desde a última sessão do usuário, o compartilhamento de sessão está desativado, mas a sessão atual exige que esteja ativado, 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 no estado pronto para poder iniciar a área de trabalho compartilhada publicada ou o aplicativo solicitado pelo usuário. Verifique se o hipervisor que hospeda o VDA não está no modo de manutenção.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[101] MachineNotFunctional. Monitoring Service converte [12] NoDesktopAvailable para esse código de erro.	O VDA não está operacional. Possíveis causas: o VDA foi removido do grupo de entrega, o VDA não está registrado, o estado de energia do VDA não está disponível ou o VDA está tendo 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 é exibido como ativado no Citrix Studio. Se o estado de energia for desconhecido para várias máquinas, resolva os problemas de conectividade com o hipervisor ou as falhas do host. Verifique se o hipervisor que hospeda o VDA não está no modo de manutenção. Reinicialize o VDA depois que os problemas tiverem sido resolvidos.

### Tipo de falha na máquina

Código de erro	ID do código de erro	Problema	Ação
Unknown	-	-	-
Unregistered	3	-	-

---

Código de erro	ID do código de erro	Problema	Ação
MaxCapacity (representado como carga máxima no Director)	4	A máquina está se reportando na capacidade máxima, ou seja, Índice de carga máxima	Certifique-se de que todos os hipervisores estejam ligados. Adicione mais máquinas aos grupos de entrega afetados adicionando mais capacidade ao hipervisor ou adicionando mais hipervisores.
StuckOnBoot	2	A VM não completou sua sequência de inicialização e não está se comunicando com o hipervisor.	Certifique-se de que a VM seja inicializada com sucesso no hipervisor. Verifique se há outras mensagens na VM, como, por exemplo, problemas do sistema operacional. Certifique-se de que as ferramentas do hipervisor estejam instaladas na VM. Certifique-se de que o VDA esteja instalado na VM.
FailedToStart	1	A VM teve problemas ao tentar iniciar no hipervisor.	Verifique os logs do hipervisor.
None	0	-	-

---

**Motivo do cancelamento do registro da máquina (aplicável quando o tipo de falha for Unregistered ou Unknown)**

Código de erro	ID do código de erro	Problema	Ação
AgentShutdown	0	O VDA desligou no período de tolerância.	Ligue o VDA se você não deseja que ele esteja desligado com base nas políticas de gerenciamento de energia existentes. Revise os erros nos logs de eventos.
AgentSuspended	1	O VDA está em modo de hibernação ou suspensão.	Retire o VDA do modo de hibernação. Considere desativar a hibernação nos VDAs do Citrix Virtual Apps and Desktops usando as configurações de energia.
IncompatibleVersion	100	O VDA não pode se comunicar com o Delivery Controller devido a uma incompatibilidade de versões do protocolo da Citrix.	Alinhe as versões do VDA e do Delivery Controller.

Código de erro	ID do código de erro	Problema	Ação
AgentAddressResolutionFailed		O Delivery Controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão precisos. Caso contrário, corrija-os. Se for generalizado, valide as configurações de DNS nos Delivery Controllers. Verifique a resolução de DNS do controlador executando o comando <code>nslookup</code> .
	101	O Delivery Controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão precisos. 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 ping para verificar se o Delivery Controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva os problemas de firewall ou rede. Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, <a href="#">Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)</a> , para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.

Código de erro	ID do código de erro	Problema	Ação
	102	Ocorreu um problema de comunicação entre o Delivery Controller e o VDA.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, <a href="#">Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)</a> , para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA. Entre em contato com o suporte Citrix.
AgentWrongActiveDirectory	103U	Houve uma configuração incorreta de descoberta do Active Directory. A unidade organizacional específica do site (onde as informações do Controller do site são armazenadas no AD) configurada no registro do VDA é para um site diferente.	Verifique se a configuração do Active Directory está correta ou verifique as configurações do registro.

Código de erro	ID do código de erro	Problema	Ação
EmptyRegistrationRequest	104	A solicitação de registro enviada do VDA para o Delivery Controller estava vazia. Isso pode ser devido a uma instalação de software do VDA corrompida.	Reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verifique se o VDA se registra com êxito através do log de eventos do aplicativo.
MissingRegistrationCapabilities	105	A versão VDA não é compatível com o Delivery Controller.	Atualize o VDA ou remova o VDA e reinstale-o.
MissingAgentVersion	106	A versão VDA não é compatível com o Delivery Controller.	Reinstale o software do VDA se o problema estiver afetando todas as máquinas.
InconsistentRegistrationCapabilities	107	O VDA não pode comunicar seus recursos ao Broker. Isso pode ser devido à incompatibilidade entre as versões do VDA e do Delivery Controller. Os recursos de registro, que mudam a cada versão, são expressos 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 a edição do seu Citrix Licensing ou remova o VDA e reinstale-o.
	108	O recurso que você está tentando usar não está licenciado.	Entre em contato com o suporte Citrix.



Código de erro	ID do código de erro	Problema	Ação
UnsupportedCredentialSecurity version	100	O VDA e o Delivery Controller não estão usando o mesmo mecanismo de criptografia.	Alinhe as versões do VDA e do Delivery Controller.
InvalidRegistrationRequest	110	O VDA fez uma solicitação de registro para o Broker, mas o conteúdo da solicitação está corrompido ou é inválido.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, <a href="#">Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)</a> , para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
SingleMultiSessionMismatch	111	O tipo de sistema operacional do VDA não é compatível com o catálogo de máquinas ou o grupo de entrega.	Adicione o VDA ao tipo de catálogo de máquinas correto ou grupo de entrega contendo máquinas com o mesmo sistema operacional.
FunctionalLevelTooLowForCatalog	112	O catálogo de máquinas é definido a um nível funcional de VDA mais alto do que a versão do VDA instalada.	Verifique se o nível funcional do catálogo de máquinas do VDA corresponde ao do VDA. Faça upgrade ou downgrade do catálogo de máquinas para corresponder ao do VDA.

Código de erro	ID do código de erro	Problema	Ação
FunctionalLevelTooLowForDesktopGroup	100	O grupo de entrega é definido a um nível funcional de VDA mais alto do que a versão do VDA instalada.	Verifique se o nível funcional do grupo de entrega do VDA corresponde ao do VDA. Faça upgrade ou downgrade do catálogo de máquinas para corresponder ao do VDA.
PowerOff	200	O VDA não desligou no período de tolerância.	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 os problemas de inicialização ou registro. Revise os logs de eventos no VDA assim que for feito backup para ajudar a determinar a causa raiz do desligamento.
AgentRejectedSettingsUpdate	100	Configurações como políticas da Citrix foram alteradas ou atualizadas, mas houve um erro ao enviar as atualizações para o VDA. Isso pode ocorrer se as atualizações forem incompatíveis com a versão do VDA instalada.	Atualize o VDA, se necessário. Verifique se as atualizações que foram aplicadas são suportadas com a versão do VDA.

Código de erro	ID do código de erro	Problema	Ação
SessionPrepareFailure	206	O Broker não concluiu a auditoria das sessões que estão em execução no VDA.	Se for generalizado, reinicie o Citrix Broker Service no Delivery Controller.
	206	O Broker não concluiu a auditoria das sessões que estão em execução no VDA.	Entre em contato com o suporte Citrix.
ContactLost	207	O Delivery Controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções na rede.	Verifique se o Citrix Broker Service está em execução no Delivery Controller e se o Desktop Service está em execução no VDA. Se interrompido, inicie cada um deles. Se já iniciado, reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verificar se o VDA se registra com êxito. Confirme se os Delivery Controllers configurados para o VDA estão precisos por meio dos detalhes no log de eventos do aplicativo. Use ping para verificar se o Delivery Controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva os problemas de firewall ou rede.

Código de erro	ID do código de erro	Problema	Ação
	207	O Delivery Controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções na rede.	Verifique se o Desktop Service está em execução no VDA. Se interrompido, inicie.
BrokerRegistrationLimitReached	301	O Delivery Controller atingiu o número máximo configurado de VDAs que têm permissão para se registrar simultaneamente. Por padrão, o Delivery Controller permite 10.000 registros simultâneos de VDA.	<p>Considere adicionar Delivery Controllers ao Site ou criar um Site. Você também pode aumentar o número de VDAs autorizados a se registrar simultaneamente no Delivery Controller por meio da chave de registro</p> <p><b>HKEY_LOCAL_MACHINE\Software</b></p> <p>Consulte o artigo do Knowledge Center, <a href="#">Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446)</a>, para obter mais informações.</p> <p>Aumentar esse número pode exigir mais recursos de CPU e memória para o Controller.</p>

Código de erro	ID do código de erro	Problema	Ação
SettingsCreationFailure	208	O Broker não construiu um conjunto de definições e configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falha, resultando em um VDA sem registro.	Verifique os logs de eventos no Delivery Controller em busca de erros. Reinicie o Broker Service se um problema específico não estiver evidente nos registros. Depois que o Broker Service for reiniciado, reinicie o Desktop Service nos VDAs afetados e verifique se eles se registram corretamente.
	208	O Broker não construiu um conjunto de definições e configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falha, resultando em um VDA sem registro.	Reinicie o Desktop Service nos VDAs afetados e verifique se eles se registram corretamente. Entre em contato com o suporte Citrix.

Código de erro	ID do código de erro	Problema	Ação
SendSettingsFailure	204	O Broker não enviou definições e dados de configuração para o VDA. Se o Broker conseguir coletar os dados, mas não conseguir enviá-los, o registro falha.	Se limitado a um único VDA, reinicialize o Desktop Service no VDA para forçar o novo registro e validar se o VDA se registra com êxito por meio do log de eventos do aplicativo. Solucione os problemas ocorridos. Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, <a href="#">Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)</a> , para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
AgentRequested	2	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
DesktopRestart	201	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
DesktopRemoved	202	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
SessionAuditFailure	205	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
UnknownError	300	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.

Código de erro	ID do código de erro	Problema	Ação
RegistrationStateMismatch	102	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
Unknown	-	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.

## SDKs e APIs

November 5, 2024

Vários SDKs e APIs estão disponíveis nesta versão. Para acessar os SDKs e as APIs, acesse [Build anything with Citrix](#). Selecione **Citrix Workspace** para acessar as informações de programação do Citrix Virtual Apps and Desktops e seus componentes relacionados.

### Observação:

O Citrix Virtual Apps and Desktops SDK e o Citrix Group Policy SDK podem ser instalados como um módulo ou um snap-in. Vários componentes SDK (como Citrix Licensing, Citrix Provisioning e StoreFront) são instalados usando apenas um snap-in.

Este produto oferece suporte ao PowerShell versões 3 a 5.

## Citrix Virtual Apps and Desktops SDK

Esse SDK é instalado automaticamente como um módulo do PowerShell quando você instala um Delivery Controller ou Studio. Isso permite que você use os cmdlets desse SDK sem precisar adicionar snap-ins. (As instruções são fornecidas abaixo se você optar por instalar este SDK como um snap-in.)

### Permissions

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 a 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 usando o cmdlet `Add-PSSnapin` (ou `asnp`).

V1 e V2 indicam a versão do snap-in. Os snap-ins do XenDesktop 5 são da versão 1. O Citrix Virtual Apps and Desktops e snap-ins anteriores à versão XenDesktop 7 são da versão 2 Por exemplo, para instalar o snap-in 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 desse SDK, selecione o produto ou componente na lista [Categories](#) e selecione **Citrix Virtual Apps and Desktops SDK**.
- Para obter orientação sobre o PowerShell, consulte [Windows PowerShell Integrated Scripting Environment \(ISE\)](#).

## Group Policy SDK

O Citrix Group Policy SDK permite exibir e configurar os filtros e as configurações da política de grupo. Esse SDK usa um provedor do PowerShell para criar uma unidade virtual que corresponde a configurações e filtros de máquina e usuário. O provedor aparece como uma extensão a `New-PSDrive`.

Para usar o Group Policy SDK, o Studio ou o Citrix Virtual Apps and Desktops SDK devem estar instalados.

O provedor do Citrix Group Policy PowerShell está disponível como um módulo ou um snap-in.

- Para usar o módulo, não é necessário nenhum trabalho adicional.
- 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 as configurações, digite `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`, onde a string 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 estão marcadas de acordo. Siga as orientações fornecidas para configurar o acesso ao serviço de API e usar as APIs para gerenciar e otimizar seus recursos.

## **Monitor Service OData**

A API Monitor permite o acesso aos dados do Monitor Service usando a versão 3 ou 4 da API OData. Você pode criar painéis personalizados de monitoramento e relatórios com base nos dados consultados a partir dos dados do Monitor Service. O OData V.4 é baseado na [ASP.NET Web API](#) e oferece suporte a consultas de agregação.

Para obter mais informações, consulte [Monitor Service OData API](#).



© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.